Trakya Üniversitesi
Mühendislik Bilimleri Dergisi

Cilt: 18 **Sayı: 1** **Haziran** **2017**

Trakya University
Journal of Engineering Sciences

Volume: 18 **Issue: 1** **June** **2017**

Trakya Univ J Eng Sci

http://dergipark.gov.tr/tujes
tujes@trakya.edu.tr

ISSN 2147-0308

Dergi Sahibi / Owner
Trakya Üniversitesi Rektörlüğü, Fen Bilimleri Enstitüsü Adına
On behalf of Trakya University Rectorship, Graduate School of Natural and Applied Sciences
Prof. Dr. Murat YURTCAN

Baş Editör / Editor-in-Chief
Doç. Dr. Hacı Ali GÜLEÇ

Dizgi / Design
Doç. Dr. Hacı Ali GÜLEÇ
Yrd. Doç. Dr. Altan MESUT
Hayriye KAHVECİOĞLU

İletişim Bilgisi / Contact Information
Address : Trakya Üniversitesi, Enstitüler Binası, Fen Bilimleri Enstitüsü,
Balkan Yerleşkesi, 22030, Edirne / TÜRKİYE
Web site : http://dergipark.gov.tr/tujes
E-mail : tujes@trakya.edu.tr
Tel : +90 284 2358230
Fax : +90 284 2358237

Baskı / Publisher
Trakya Üniversitesi Matbaa Tesisleri
Trakya University Publishing Centre

ISSN 2147-0308

İÇİNDEKİLER / CONTENTS

ISSN 2147-0308

http://dergipark.gov.tr/tujes
Trakya University Journal of Engineering Sciences, 18(1): 1-16, 2017
ISSN 2147–0308
Araştırma Makalesi / Research Article

YER ALTI METRO İSTASYONLARINDA MEKAN TASARIMI ÜZERİNE BİR ARAŞTIRMA

Didem AKTOP MADEN[1], Erkan AVLAR[2]

[1] *İstanbul Büyükşehir Belediyesi, Raylı Sistem Daire Başkanlığı, Anadolu Yakası Raylı Sistem Müdürlüğü, İstanbul*

[2] *Yıldız Teknik Üniversitesi, Mimarlık Fakültesi, Mimarlık Bölümü, İstanbul*

Özet: Toplu taşıma sistemlerinden kent içi raylı sistemler, özellikle metropol niteliği kazanmış büyük kentlerde tercih edilmektedir. Yer üstündeki yoğun yapılaşma, kamulaştırma sorunları ve yetersiz ulaşım ağı, raylı sistemlerin yer altına alınmasına neden olmuştur. Metropollerin ulaşımdaki en büyük sorunu olan zaman ve mekan yetersizliğine çözüm sunan metrolar, özel bir güzergah üzerinde hareket etmekte ve bu sistemde özel istasyon yapıları kullanılmaktadır. Yer altı metro istasyonları, belirli noktalarda bulunan giriş yapıları dışında yüzeyle ilişkisi olmayan kapalı yapılardır. Yolculuk sırasında kullanıcıların kentle ilişkisi kopmaktadır. İstasyon yapılarının planları çoğu zaman karışıktır, metroya ulaşıp yolculuk yapmak, uzun ve karmaşık dolaşım alanlarında yürümeyi gerektirir. Bu mekansal kurguda rahat ve güvenli bir kullanım ortamı sağlanmadığında, ortam koşulları yolcularda fiziksel ve psikolojik olumsuzluklara neden olabilmektedir. Bu olumsuz etkiler, mekansal tasarım kurallarına bağlı etkin tasarım ile engellenebilir ya da azaltılabilir. Çalışmada öncelikle, yer altı metro istasyonları için öncü tasarım kuralları mercek altına alınmakta, daha sonra tasarım sürecine katkı sağlamak için yer altı metro istasyonlarında yer alan istasyon girişi, yatay dolaşım alanları, bilet holü, peron ve yardımcı mekanların tasarım kuralları geniş bir perspektifte örnekleri ile değerlendirilmektedir.

Anahtar Kelimeler: metro; yer altı metro istasyonu; yolculu alanlar; mekan tasarım kuralları

A RESEARH ON SPACE DESIGN IN UNDERGROUND SUBWAY STATIONS

Abstract: Urban rail systems from public transport systems are preferred especially in metropolitan cities. Intensive construction on the ground, problems of expropriation and inadequate transportation network caused the rail systems to be taken underground. Subways, that provide solutions to time and space insufficiency, metropolis's biggest problem in transportation, moves on a special route and special structures are used in this system. Underground subway stations are closed structures that are not related to the surface apart from the entrance at certain points. During the journey, users are disconnected from the city. Plans of subway stations are often complicated, reaching the subway and travelling requires walking in long and complicated circulation spaces. If a comfortable and safe environment is not provided for this space design, the environmental conditions can cause physical and psychological disadvantages on the journey passengers. These disadvantages can be prevented or reduced by effective design based on spatial design rules. In the study, firstly, preliminary design rules for underground subway stations are examined, then the design rules of station entrance, vertical circulation elements, ticket hall, platform and auxiliary spaces are evaluated with examples from a wide perspective to contribute to the design process.

Keywords: subway; underground subway station; passenger areas; space design rules

*Corresponding Author: Didem AKTOP MADEN

Tel: +90 (216) 499 44 60, e-mail: didem.maden@ibb.gov.tr

GİRİŞ

Metropollerde artan nüfusun meydana getirdiği büyüme, yoğun yapılaşma ve motorlu araç sayısının artması ile ulaşım sorunu ortaya çıkmış, bu alanlarda yaşayan insanların bir yerden bir yere ulaşımı zorlaşmış ve bunun sonucunda toplu taşıma sistemlerinin önemi artmıştır. Toplu taşıma sistemlerinden kent içi raylı sistemler, özellikle metropol niteliği kazanmış büyük kentlerde tercih edilmektedir. Kent içi raylı sistemler yolcu taşıma kapasitelerine göre; tramvay, hafif raylı sistem ve metro olmak üzere farklı şekilde tesis edilebilmektedir. Metrolar, kent içi ulaşımda yüksek hızı, yüksek yolcu kapasitesi, sık sefer aralığı ve güvenli sistemleriyle öne çıkmaktadır.

Metropollerin ulaşımdaki en büyük sorunu olan zaman ve mekan yetersizliğine çözüm sunan metrolar, tam korumalı yol kullanımına sahip olduklarından özel bir güzergah üzerinde hareket etmekte ve bu sistemde özel istasyon yapıları kullanılmaktadır. Metrolar için ayrılmış bu güzergah, yer üstünde olabileceği gibi nüfus yoğunluğu fazla olan kentlerde, kente paralel olarak yer altında ilerlemekte, yolculuk sırasında hızlı ve kesintisiz hareket sağlanmakta, kentle sadece giriş noktalarında kesişerek, yüzeydeki mekan sıkışıklığını ortadan kaldırmaktadır. Böylelikle yoğun ve hareketli bir yaşantının olduğu, çeşitli kültürel, etnik, sosyal ve ekonomik grupların beraber bulunduğu, sanayi, ticaret ve konut merkezlerine sahip büyük kentler olan metropollerde, yer altı da metropolün bir parçası haline gelmektedir.

Yer altı metro istasyonları yüzeyin altında, belirli noktalarda bulunan giriş yapıları dışında yüzeyle ilişkisi olmayan kapalı yapılardır. Bu sistemde kent içi ulaşım, yer altındaki istasyonlar ve istasyonları birbirine bağlayan karanlık tünellerde sağlanmaktadır. Yolculuk sırasında kullanıcıların kentle ilişkisi kopmaktadır. İstasyon yapılarının planları çoğu zaman karışıktır, metroya ulaşıp yolculuk yapmak, uzun ve karmaşık dolaşım alanlarında yürümeyi gerektirir. Yer altı metrosu ile seyahat eden yolcular; istasyon girişlerini, yatay dolaşım alanlarını (yolcu koridorları, yürüyen bantlar), düşey dolaşım elemanlarını (asansörler, yürüyen ve sabit merdivenler, rampalar), bilet holünü (kontrollü ve kontrolsüz alanlar) ve peronu (platform) kullanarak metroya ulaşmakta ve yine aynı mekanları kullanarak yolculuğunu sonlandırmaktadır. Bu mekansal kurguda rahat ve güvenli bir kullanım ortamı sağlanamadığında, ortam koşulları yolcularda fiziksel ve psikolojik olumsuzluklara neden olabilmektedir. Bu olumsuz etkiler, kurallara bağlı etkin tasarım ile azaltılabilir ya da engellenebilir.

MATERYAL VE METOD

Bu çalışmada amaç, yer altı metrosu kullanıcılarının sağlık ve güvenliğini tehlikeye atabilecek etkenler içermeyen keyifli ve konforlu yapılar tasarlanmasıdır. Bu amaç doğrultusunda çalışmada, yer altı metro istasyonlarının mekan tasarım kuralları açısından değerlendirilmesi hedeflenmiştir. Bunun yanı sıra tasarım kuralları yönünde bir farkındalık oluşturulması çalışmanın hedefleri arasındadır. Bugün İstanbul'da çok sayıda metro inşaatı devam etmekte ve ileriye yönelik metro hatları planlanmaktadır. Türkiye'nin bir çok diğer kentinde de metro çalışması vardır. Bu bağlamda araştırmanın yararlı olacağı ve katkı sağlayacağı düşünülmektedir.

Bu çalışma, mekan tasarımı odaklı bir araştırmadır ve kent içi raylı sistemlerden metro ile sınırlandırılmıştır. Çalışma kapsamında yer altı metrosu istasyon yapıları ele alınmış ve istasyon tasarımında yer alan düşey dolaşım elemanları kapsam dışı bırakılmıştır. Araştırmanın yöntemi; konuya ilişkin literatür taraması, mekan tasarımına ilişkin kuralların ve ayrıntıların gözden geçirilmesi, tasarımı yönlendirecek etkenlerin belirlenmesi ve bu etkenler bağlamında öncü tasarım kurallarının verilmesi, yer altı metro istasyonlarında yer alan mekanların işlev etkinlik sırasına göre ele alınarak mekan özelliği, tasarım ölçütleri ve donanımlar dizini içinde örnekler üzerinden geniş bir perspektifte değerlendirilmesi aşamalarından oluşmaktadır.

Yer altı metro istasyonlarında mekansal tasarım kuralları ile ilgili literatür araştırmasında uluslararası çalışmalara rastlanmıştır. John Carmody ve Raymond Streling (1993) yer altı mekanlarının tasarımını ele almıştır. Jürgen Rauch (1996) metro istasyonlarının mimarisini anlatmış, Brain Edwards (1997) raylı sistem mimarisine yeni yaklaşımlar önermiş, Julien Ross (2000) metro istasyonlarının planlaması, tasarımı ve yönetimi konusunda çalışma hazırlamıştır. Türkiye'de bu konuda tez çalışmaları olduğu görülmektedir. Nurbin Paker (1992), Aysimin Sevdin (1992), Melda Horoz (2001) ve Burak Çetindağ (2003) metro istasyonlarının tasarım kriterleri, Huriye Tunç (2007) yer altı metro istasyonlarında algısal faktörler, Esra Özbek (2007) metrolarda yön bulma, H. Ozan Avcı (2008) metropol kentlerde oluşan zamansız mekanlar olarak metrolar, Emine Demir (2007) ve Büşra Selen Keskiner (2015) ise yer altı metro istasyonlarına ait giriş-çıkış yapıları, Pınar Önal (2014) metro dolaşım alanları iç mekan atmosferi konusunda tez hazırlamıştır.

Türkiye'de yer altı metro istasyonlarının mekan tasarımında DLH (Demiryollar, Limanlar ve Hava Meydanları) ve TS (Türk Standardı)'nda yer alan tasarım kuralları kullanılmaktadır. DLH Demiryolları Planlama ve Tasarım Teknik Esasları (2007), DLH Metro Tasarım Kriterleri (2010) yanı sıra, TS 12127 (1997), TS 12460 (1998), TS 12461 (1998), TS 12511 (1998), TS 12525 (1999), TS 15527 (1999), TS 12574 (1999), TS 12575 (1999) kullanılan standartlardır. Bu standartlarla birlikte, uluslararası standartlara da yer verilmektedir. İstasyonların yangından korunması ve yangın güvenlikli tasarım konusunda NFPA (National Fire Protection Association, 2010), asansörler, yürüyen merdivenler ve yürüyen bantlar konularında EN (European Norm) standartlarından yaralanılmaktadır. Yurtdışındaki metro hatlarının tasarımında farklı standartlar kullanıldığı tespit edilmiş ve bu standartların kent ya da bölge ölçeğinde farklılaşabildiği gözlenmiştir.

YER ALTI METRO İSTASYONLARINDA ÖNCÜ TASARIM KURALLARI

Yer altı metro istasyonunun boyutlandırılmasında en önemli etken yolcu sayısıdır. İstasyon yapısı, istasyondan yararlanacak yolcu sayısının tahmini kapasitesine göre boyutlandırılmaktadır. Boyutlandırma yapılırken en önemli ölçüt, normal işletme koşulları ve acil durum tahliye koşullarıdır. Bununla birlikte yer altı metro istasyonu tasarımında, normal işletme, doruk (pik) saat işletmesi, hizmet kesintisinde işletme ve acil durum tahliyesi olmak üzere dört farklı işletme periyodu da dikkate alınmalıdır. Normal işletme koşulları esas alınarak yapılan istasyon boyutlandırmasında amaç, günlük işletme esnasında yer altı istasyonu yolculu alanlarında ortalama bir düzey sağlamaktır. Hedef ise, doruk (pik) saatlerde, istasyon içerisindeki yolcu hareketinin aksamasını önlemektir (Şekil 1).

Şekil 1: Taipei'de Metro Istasyonu (https://temporarilylostdotcom.files.wordpress.com/2013/02/taipei-1-crowded-subway-station.jpg)

Acil durum tahliye koşulları, yolcuların 4 dakikada perondan, 6 dakikada ise istasyondan tahliyesini ya da güvenli alana ulaşmasını gerektirmektedir (NFPA 130, 2010). Peronda en az iki adet çıkış yolu bulunmalıdır (TS 12127, 1997). Acil bir durumda tünelde ya da istasyonda bulunan yolcuların tahliyesi için gerekli acil kaçış hesapları yapılmalı, istasyon tasarımı bu hesaplara göre şekillenmelidir.

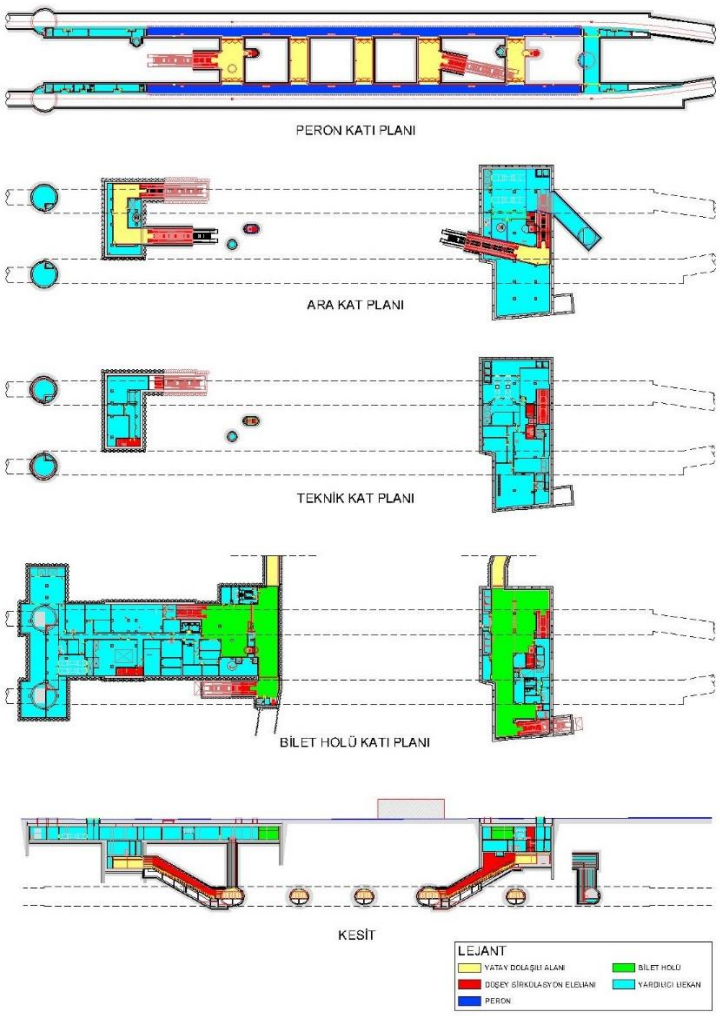
Metro hattının güzergahı ve yer altı metro istasyonlarının yeri, yapılan fizibilite çalışmaları sonucunda bölgenin nüfusuna ve gereksinimine göre

belirlenmektedir. Yer altı metro istasyonlarının mimari olarak biçimlenişinde, çeşitli etkenler rol oynamaktadır. Bu etkenler; istasyon yapısının konumu, yapının yer alacağı zeminin jeolojik yapısı, istasyonu kullanacak yolcu sayısı, yapının boyutu ve istasyonun yapım yöntemidir. Yer altı metro istasyonunun konumu, yüzeydeki yapılaşma ile bağlantılı olarak mimari biçimlenişi de etkilemektedir. İstasyon yapısı; içerisinde yer aldığı kamusal alan sınırlarına, istasyon giriş yapıları ile istasyona ait hava kanallarının yüzeydeki konumlarına ve çevredeki yapıların durumlarına göre tasarlanmaktadır. Bu yapının bulunduğu zeminin jeolojik durumuna göre, metro hattı güzergahı ve tünellerin seviyesi belirlenmekte, bu parametrelerle ilişkili olarak da istasyon yapısı biçimlenmektedir.

Yer altı metro istasyonlarındaki mekanların tasarımında; birikmelere olanak verilmemesi (normal işletim), tren seferinin aksaması ya da ani talep karşısında kullanıcı sayısı artışını karşılayabilmesi (sıkışık işletim) ve acil kaçış için yeterli kapasiteye ulaşması (acil durum işletimi) olmak üzere üç önemli işletim hedefi vardır. Bu hedefler ile istasyonların işlevleri, servis ömürleri boyunca etkin bir biçimde devam ettirilmektedir. İşletim hedeflerinde istasyonların güvenli ve konforlu olması yanı sıra, alan kullanımı en üst düzeyde olmalı, yolcu dolaşımı düşünülerek tüm mekanların ve donanımların çevresinde birikme alanları bırakılmalı, yolcular yapması gereken aktiviteye yönlendirilmeli, yürüyüş doğrultusu açık, düz ve en kısa mesafede olmalı, yürüme yollarının genişliği olabildiğince tek tip olmalı, yol boyunca engel ve daralmalardan kaçınılmalı, iyi bir görüş alanı sağlanmalı, uzun koridorlar ve işlevsiz alanlar bulunmamalı ve eğer gelecekte istasyon yolcu kapasitesinin artması olası ise istasyon tasarımı yapılırken bu öngörü hesaba katılmalıdır (Ross 2000, 111).

YER ALTI METRO İSTASYONLARINDA MEKAN TASARIMI

Yer altı metro istasyonlarındaki mekanların işlev etkinlik sırası; istasyona giriş, bilet holüne iniş, istasyon ve işletme hizmetlerine ulaşım (bilet verme makinesi, telefon vb.), turnikelerden geçiş, yatay dolaşım alanlarında ilerleme, perona iniş, tren bekleme, trene binme / inme ve çıkış şeklinde gerçekleşmektedir. Buna göre, yer altı metro istasyonlarının yolculu alanları; istasyon girişi, yatay dolaşım alanları, bilet holü (konkors), peron (platform) ve yardımcı mekanlardan oluşmaktadır (Şekil 2). Bu mekanlar çalışma kapsamında tek tek ele alınarak değerlendirilmektedir.



Şekil 2: İstanbul Kadıköy Yer Altı Metro İstasyonu Kat Planları

- **İstasyon Girişi**

Yer altı metrolarında yolculuk yapan kişiler, yer altında karanlık tünellerde kenti deneyimleyemez, algılayamaz. İnsanların kentle ilişki kurduğu tek nokta, metroyu kentle buluşturan, "kent kapıları" niteliğindeki istasyon girişleridir (Şekil 3, 4, 5). Yer altı metro istasyonlarına erişim için en az bir, tercihen iki adet giriş/çıkış ve bir adet te dışarı açılan acil çıkış kapısı bulunmalıdır (TS 12127, 1997).

Şekil 3: Londra Canary Wharf Metro İstasyonu Girişi (https://upload.wikimedia.org/wikipedia/commons/8/8e/Canary_Wharf_Tube_Station_-_July_2009.jpg)

Şekil 4: Baltimore Metro İstasyonu Girişi (https://s-media-cache-ak0.pinimg.com/564x/5c/06/cb/5c06cb806cb4a4b9fb474038aba7e46c.jpg)

Şekil 5: Dubai Metro İstasyonu Girişi (http://photos.wikimapia.org/p/00/04/53/46/54_big.jpg)

İstasyon girişleri, çevresinde yeni kentsel alanlar yaratarak, fiziksel ve sosyal yönden kentin mekansal dönüşümüne neden olmaktadır. Girişler, toplanma ve dağılma merkezi olma görevini üstlendiklerinden kentin çekim noktaları haline gelmektedir. İstasyon girişi çevresinde yaya akımı yoğunlaşmakta, bunun sonucunda istasyon çevresine yeni işlevler ve donanımlar gelmektedir. Yer altı ile kentin buluştuğu bu noktada, istasyon girişleri ön plana çıkmakta ve kent imajının oluşturulmasına katkıda bulunmaktadır (Demir, 2007). Bu nedenle giriş yapıları estetik açıdan çevresiyle uyumlu, çekici ve kimliği ile kolay algılanabilir olmalıdır.

Kent içinde birer kamusal mekan olan metro giriş yapıları yaya ile taşıt ilişkisi düşünüldüğünde, erişilebilirlik, işlevsellik ve kentsel algı çerçevesinde değerlendirilmelidir. Kentlerde erişilebilirlik, yaya hareketleri ve toplu taşıma ile sağlandığından, giriş yapılarının yürümeye uygun merkezi noktalarda bulunması, diğer yaya akslarına ve toplu taşıma araçlarına aktarma yapmaya uygun olması gerekmektedir. İşlevsellik, kent ile insan arasındaki bağlantıyı kurarak, mekanları canlı ve kullanılır kılmaktır. Metro istasyonlarından beklenen ana işlev ulaşım olmakla birlikte, farklı aktivite alanları tasarlanarak daha nitelikli mekanlar yaratılabilmektedir. Kent meydanları, kamusal alanların en etkin kullanılan alanlarıdır. Günümüzde kent meydanı olarak kullanılmaya başlayan metro giriş yapıları kentsel imgelerden biri olmakta ve kentin odak noktası haline gelmektedir (Keskiner, 2015).

Yer altı metro istasyonlarında giriş yapılarının biçimlenmesi, yüzeyle bağlantının sağlandığı tek nokta olduğu için algı açısından çok önemlidir. İstasyon girişi tasarımındaki problem, yüzey ile istasyon arasında bağlantı olmamasıdır. Bu nedenle istasyon girişleri okunaklı, ilgi çekici, açıkça tanınabilir olmalıdır. Girişlerde kullanılan semboller, istasyonların belli bir mesafeden algılanmasını sağlar. Bu semboller ülkeden ülkeye farklılık gösterseler de, genelde metroyu kullanan yabancı yolcuların da anlayabileceği ifadeler kullanılmaktadır (Rauch, 1996). Ulaşım sembolü, çok renkli ve karmaşık olmamalıdır. Sembol sade bir resim, harf ya da şekilden meydana gelmeli, sembolün rengi zemin rengine zıt olmalı, sembol kolay ayırt edilebilmelidir (TS 12511, 1998).

- **Yatay Dolaşım Alanları**

Yatay dolaşım alanları, istasyon girişi ile bilet holü, bilet holü ile peron gibi ana fonksiyon alanları arasındaki erişimi sağlayan yatay bağlantılardır (Şekil 6, 7, 8). Bu bağlantılar, yer üstündeki çeşitli noktalardan biraraya gelen insanları metroya ulaştıran yaya koridorları ya da yürüyen bantlar şeklinde olabilmektedir.

Şekil 6: Münih Marienplatz Metro İstasyonu Yatay Dolaşım Alanı (http://www.sumit4allphotography.com/wp-content/uploads/2015/05/munich4-015.jpg)

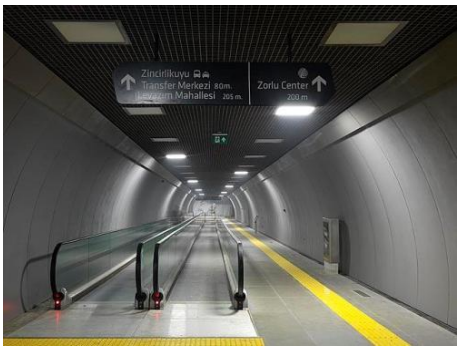
Şekil 7: Rotterdam Wilhelminaplein Metro İstasyonu Yatay Dolaşım Alanı (http://www.e-architect.co.uk/images/jpgs/rotterdam/wilhelminatunnel_zj060209_2.jpg)

Şekil 8: Rio de Janeiro Copacabana Metro İstasyonu Yatay Dolaşım Alanı (https://c2.staticflickr.com/6/5550/10711119366_2976a8853c_b.jpg)

Yatay dolaşım alanları; belirgin yollardan oluşmalı, istasyona girildiği andan itibaren yol güzergahının kolayca seçilebileceği işaretlerle donatılmış olmalı, yolcunun vermesi gereken kararları en aza indirmeli ve keskin dönüşler içermemelidir. Dönemeç yapılması gereken zorunlu hallerde, dönemeç istasyon giriş ve çıkışına yerleştirilmemeli, sağ yön dolaşımı esas kabul edilmelidir. Keskin dönemeçlerde iç köşeler yuvarlatılmalıdır, ters yöndeki yolcu akımının birbirini engellemesini önlemek için dış köşelerde tedbirler (ayna konulması gibi) alınmalıdır. Bu alanlar, 1 metre genişlikteki bir yatay dolaşım alanını (yaya koridoru) dakikada 80 yolcunun kullandığı düşünülerek boyutlandırılmalıdır (TS 12127, 1997). Network Rail İstasyon Kapasitesi Belirleme Rehberi'ne göre; çift yönlü yaya yolları için 40 yolcu dakika/metre oranına göre net genişlik hesaplanmakta ve çıkan sonuca her iki kenar için 30'ar cm eklenmektedir. Eklenen mesafe (toplam 60 cm) yolcuların katı nesnelere yaklaştıkça yavaşlama eğiliminden dolayı hesaba katılan kenar etkisi olarak belirtilmektedir. Her durumda yaya yolarındaki en az net genişliğin 2.00 m olması önerilmektedir (Network Rail, 2011).

Daha uzun ve trafiği yoğun olan yatay dolaşım alanları için bir seçenek de yürüyen bantlardır (Şekil 9, 10). Bu sayede yolcular sadece ayakta durarak ulaşım sağlayabilir ya da aynı zamanda bant üzerinde yürüyerek zaman kazanabilir (Özbek, 2007). Bu bantlar düz ya da eğimli olabilir. Yürüyen bantlarda eğim, %5 - %7 aralığında olmalıdır. 5 m/sn hızla hareket eden bir yürüyen bandın taşıma kapasitesi saatte 8000 kişi olarak düşünülmelidir (TS 12127, 1997). Network Rail İstasyon Kapasitesi Belirleme Rehberi'ne göre, yürüyen bant genişliği en az 1.20 m olmalıdır. Bant taşıma kapasitesi 100 yolcu dakika/metre oranına göre hesaplanmalıdır. Yürüyen bantın uzunluğu en az 50.00 m, en fazla 100.00 m olmalıdır (Network Rail, 2011).

Şekil 9: St Petersburg Metro İstasyonu Yürüyen Bant Uygulaması (https://commons.wikimedia.org/wiki/Main_Page)



Şekil 10: İstanbul Gayrettepe Metro İstasyonu Yürüyen Bant Uygulaması (http://www.ibb.gov.tr/tr-TR/HaberResim/21403/_t/2_JPG.JPG)

Yolcu akışının fazla olduğu yatay dolaşım alanlarında, tek yönlü güzergahlar kullanılarak daha yüksek kapasitelere ulaşılmaktadır. Bir istasyon tam kapasitesine yakın bir kapasiteyle çalışıyorsa karşı yönden gelen akışları, ana akıştan ayırarak tek yönlü bir sisteme geçilmesi (bazen farklı giriş ve çıkışlarla) önerilmektedir. Çok az sayıdaki "kurallara aykırı" karşı yönlü akışlar bile ana akışı ciddi biçimde yavaşlatabileceğinden tek yönlü sistemler ancak aktif olarak (personel denetimiyle veya tek yönlü geçiş olanağı veren bariyerlerle) etkin biçimde uygulanabilecekleri yerlerde kullanılmalıdır. Yatay dolaşım alanlarında genişlik, yolcuların yan yana rahatça yürümelerine olanak verecek ölçüde olmalıdır. Bu ölçü en az 2.00 metre olarak düşünülmelidir (Özbek, 2007).

- **Bilet Holü (Konkors)**

Bilet holü, metro istasyonlarında yolcunun bilgi aldığı, beklediği, bilet verme makinesi ve telefonları kullandığı, turnikeleri kullanarak kontrolsüz (ücretsiz) alandan kontrollü (ücretli) alana geçiş yaptığı ve perona yöneldiği mekandır (Şekil 11, 12). Perondan gelen diğer yolcular ise yine bilet holünü ve turnikeleri kullanarak istasyondan çıkmaktadır. Bilet holü yolcuların toplandığı ve dağıldığı mekanlar olduğundan istasyon yapısının merkezidir. Bu katta genellikle danışma, güvenlik, bilet gişesi, tuvaletler, ticari alanlar ile yolcu kullanımından ayrılmış teknik mekanlar yer almaktadır.

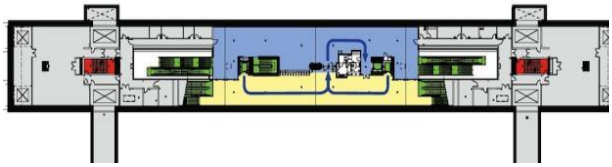
Şekil 11: Moskova Sretensky Boulevard İstasyonu Bilet Holü (http://img-fotki.yandex.ru/get/4429/109481923.68/0_7928b_868806db_orig)

Şekil 12: İstanbul Kadıköy İstasyonu Bilet Holü (Kişisel Arşiv)

Bilet holü alanı, kişi başına en az 1.00 m² yer ayrılarak hesaplanmalıdır. Birden fazla bilet holü sağlandığında, en az alan gereksinimi bilet holleri arasında bölünmelidir (Network Rail, 2011). Bilet holünün net yüksekliği 3.50 m, tavana monte edilmiş cihaz ve diğer askılı elemanlarla bitmiş döşeme arası en az 2.50 m olmalıdır (DLH, 2007). Konkors olarak ta adlandırılan bu hol, istasyondaki giriş yapılarının ve istasyon yapısının mimarisine göre birden fazla da olabilmektedir. Bilet holü katı, istasyon yapısının yüzeye yakın en üst katında yer alabildiği gibi, ara katta ya da peronun hemen üstündeki katta da düzenlenebilmektedir. Bu katın engelli kullanımı açısından yüzeye çıkan ve perona inen asansör olmak üzere mutlaka en az iki adet asansör erişimi olmalıdır. Bilet holü, yolcuların giriş, bilet verme makinesi ya da turnike gibi farklı aktivite alanları arasında rahat dolaşımına olanak vermeli, dönüşler genellikle sağa doğru olmalı ve yolcu akışa engel olmadan nereye gitmesi gerektiğine karar verebilmeli, işlevler birbiriyle

çakışmamalı (örneğin; bilet kuyruğu ya da varsa satış alanları kuyruğu akışa engel olmamalı), bilet satış doruk zamanda yolculara bilet sağlamak için yeterli olmalı, bilet satışı için yeterli sayıda pencere ve personele sahip bilet gişesi ile yolcunun kendi biletini kendisinin aldığı yeterli sayıda bilet verme makinesi bulunmalı, yolcunun yoğun olduğu zamanda, arkaya doğru devam eden ve sıkışıklıkla sonuçlanan yolcu akımları oluşmamalıdır (Ross, 2000).

Geçiş turnikeleri, bilet holünü kontrollü ve kontrolsüz alan olarak ikiye ayırmaktadır (Şekil 13). Turnikelerin adedi, bir turnikeden girişte dakikada 30 yolcu, çıkışta dakikada 40 yolcu geçebileceği düşünülerek belirlenmelidir. Turnike genişliği 0.45-0.50 m, yüksekliği ise 0.90-1.00 m olmalıdır (TS 12127, 1997). Engelli geçişi için, genişliği minimum 80 cm olan özel turnike yapılmalıdır (TS 12460, 1997).



Şekil 13: Toronto Downsview Park Metro İstasyonu Bilet Holü (http://urbantoronto.ca/sites/default/files/imagecache/display-slideshow/images/articles/2011/03/524/524-2054.jpg)

Yolculuk yapacak kişi istasyona girişten itibaren bilet holüne rahatça ulaşabilmeli, yol basit ve kısa olmalıdır. Turnikelerden önceki kontrolsüz alanda, ticari alanlar sınırlı olmalı, yolcu olmayan insan trafiği azaltılmalıdır. Turnikeler, uzaktan görülebilecek şekilde yerleştirilmelidir. Bilet holünün tasarımı yapılırken merdiven, yürüyen merdiven, asansör, bilet gişesi, turnikeler, bilet verme makinesi ve telefonların önlerinde oluşabilecek birikme alanları düşünülmelidir.

- **Peron (Platform)**

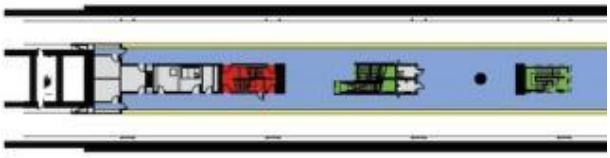
Peron, istasyondaki yolcuların, trene inip bindiği ya da treni beklediği, ray üst kotundan 0.90-1.00 m kadar yüksekte bulunan bölümdür. Ray üst kotuyla olan mesafesi, seçilen aracın vagon kapılarının yüksekliğine göre düzenlenmektedir. Zorunlu haller dışında düz tasarlanmaktadır. Eğrisel olmasının zorunlu olduğu durumlarda, en az 600.00 m yarıçaplı bir eğri şeklinde düzenlenmektedir (DLH, 2010) (Şekil 14, 15).

Şekil 14: Müenchen Candidplatz Metro İstasyonu Peronu (Eğimli) (https://upload.wikimedia.org/wikipedia/commons/2/28/U-Bahn-Muenchen_Candidplatz_-_2007-CC-BY-SA_SYNTAXYS-Achim-Lammerts.jpg)

Şekil 15: Prag Hradcanska Metro İstasyonu Peronu (Düz) (https://upload.wikimedia.org/wikipedia/commons/f/fa/Metro_Prague_-_Hradcanska_Station.JPG)

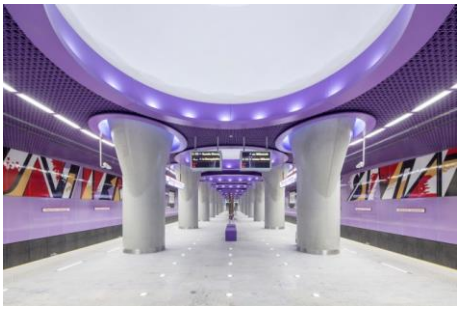
Bir istasyon yapısında peron yerleşimi, yan peron, orta peron, hem yan hem orta peron ya da üst üste peron şeklinde düzenlenebilmektedir. Yan peron, iki ayrı hatta hizmet veren, karşılıklı ve iki adet olarak düzenlenen peronlardır. Yan peronda, düzenlenen peronların her biri, sadece kendi hattına erişim sağlamaktadır. Orta peron ise, iki hattın ortasında olan peronun her iki hatta birden hizmet verdiği düzenlemedir (Şekil 16, 17, 18, 19).

Şekil 16: Lizbon Olaias Metro İstasyonu (Yan Peron) (https://upload.wikimedia.org/wikipedia/commons/7/7e/Metro_de_Lisboa_-_Esta%C3%A7%C3%A3o_Olaias_(8175721609).jpg)



Şekil 17: Toronto Downsview Park Metro İstasyonu'nda Orta Peron Uygulaması (http://urbantoronto.ca/sites/default/files/images/projects/836/836-2059.jpg)

Şekil 18: Münih Georg-Brauchle-Ring Metro İstasyonu (Orta Peron) (https://upload.wikimedia.org/wikipedia/commons/c/cc/Munich_subway_GBR.jpg)



Şekil 19: Varşova Metrosu (Orta Peron) (http://images.adsttc.com/media/images/554a/a083/e58e/ce61/f200/00dc/large_jpg/C12_6(2).jpg?1430954101)

Yer altı metro istasyonlarında hem yan peron hem de orta peronun ya da iki orta peronun kullanıldığı tasarımlar da yapılmaktadır (Şekil 20, 21). Kullanılacak peron tipi ve peron adedi, istasyonun hizmet verdiği hat sayısına ve istasyonu kullanacağı öngörülen yolcu yoğunluğuna göre belirlenmektedir.

Şekil 20: Valencia Alameda Metro İstasyonu (İki Yan ve Bir Orta Peron) (http://www.viajejet.com/wp-content/viajes/Alameda_Station__MetroValencia_by_metromurcia-400x300.jpg)

Şekil 21: Almanya Müncher Freihet Metro İstasyonu (İki Orta Peron) (https://upload.wikimedia.org/wikipedia/commons/0/0f/Munich_subway_station_M%C3%BCnchner_Freiheit_2009-12.jpg)

Yer altı metro istasyonu aktarma istasyonuysa, yani birden fazla metro hattının keşişim ve birleşen noktası ise katlı peron düzenlenmektedir (Şekil 22).

Şekil 22: Sao Paulo Metro İstasyonu (Katlı Peron) (http://fotospublicas.com/paineis-de-led-sao-instalados-na-estacao-se-metro-em-sao-paulo/)

Peron uzunluğu, seçilen trenin uzunluğuna bağlı olarak belirlenmektedir. Ayrıca bu uzunluğa %5-10 oranında fren mesafesi eklenmektedir (Sevdin, 1992). Örneğin dört vagonlu treniçin 100.00 m, altı vagonlu tren için ise 140.00 m uzunlukta peron yapılabilmektedir. Peron genişliği, zirve saatte inen-binen yolcu yoğunluğuna bağlıdır. Gelecek olan trene binmek için bekleyen yolcular, gelecek olan trenden inecek yolcular ve bir önceki treni kaçırmış olan yolcular da hesap edilerek kişi adedi bulunmalı ve kişi başına en az 0.50-0.70 m², tercihen 2.00 m² alan düşecek şekilde peron alanı hesaplanmalıdır. Bu alandan yola çıkılarak, kullanılacak araca göre boyu belirlenmiş olan peronun genişliği tayin edilmelidir. Peron genişliği, uçlardan çıkışlı orta peronda en az 6.70 m, tercihen 7.30 m; ortadan çıkışlı orta peronda en az 3.65 m, tercihen 4.85 m; yan peronda en az 2.50 m, tercihen 3.65 m olmalıdır. Peron kenarında (tren tarafında), peron döşemesinden farklı renk ve dokuda, 0.45-0.50 m genişlikte emniyet bandı bulunmalı ve bu bant peron genişliğine ayrıca eklenmelidir.

Network Rail İstasyon Kapasitesi Belirleme Rehberi'ne göre; yan peron en az 3.00 m, orta peron en az 6.00 m olmalıdır. Peron genişliği hesaplanırken, kişi başına 0.93 m² yer ayrılmalıdır. Peron yolcu yükü hesaplanırken, yolcuların peronda eşit olarak dağılmadığı %35'inin, peronun %25'lik bölümünde yoğunlaştığı düşünülmelidir. Peron genişliğinde bulunan değere, kenar etkisi için 1.00 m mesafe eklenmelidir (Network Rail, 2011).

Peron yüksekliği, en az 3.50 m olmalı, yönlendirme levhası, bilgilendirme levhası, saat gibi tavana asılı elemanların altında en az 2.50 m yükseklik bulunmalıdır. Bu elemanlar, tren tarafından en az 50 cm mesafede olmalıdır. Peron kenarından en yakın engele (merdiven, duvar, pano gibi) olan mesafe, en az 2.50 m olmalıdır. Peron altında en az 60 cm genişlikte ve yaklaşık 90 cm yükseklikte peron boyunca devam eden sığınma nişi olmalıdır. Peronun her iki ucunda, ray kotuna inen merdiven bulunmalıdır. Merdivene inişten önce, peronda kilitli bir kapı bulunmalı ve gerektiğinde personel tarafından açılarak kullanılabilmelidir (TS 12127, 1997).

Peronda en az iki adet çıkış bulunmalıdır. Perondan çıkış için olması gereken en az genişlik peron yükünün 50'ye bölünmesiyle bulunmalıdır. Peron yükünü hesaplamak için ise net peron alanı 0,65'e bölünmelidir. Çıkış için izlenecek yol, kolay kavranabilmeli ve karışık olmamalıdır. Peronda çıkmaz yol, işlevsiz ve karanlık köşeler bulunmamalıdır. Yolcunun istediği çıkışa erişebilmesi için perondan itibaren yol kotuna kadar çıkış işaretleri ve yönlendirme levhaları kullanılmalıdır. Peron ucundan en yakın çıkışa olan mesafe en çok 60.00 m olmalıdır (TS 12127, 1997).

Network Rail İstasyon Kapasitesi Belirleme Rehberi'ne göre; çift yönlü peron giriş-çıkış genişliği bulunurken 1.00 m'den dakikada 40 kişinin geçebileceği düşünülmeli ve çıkan sonuca 0.60 m kenar etkisi mesafesi eklenmelidir. Tek yönlü girişlerde ve tek yönlü çıkışlarda ise kişi sayısı 50 olarak alınarak hesap yapılmalı ve çıkan sonuca kenar etkisi eklenmelidir. Her durumda giriş-çıkış genişliği en az 2.00 m olmalıdır. Peron ucundan en yakın çıkışa olan mesafe en çok 45.00 m olmalıdır (Network Rail, 2011). Peronda, yolcuların güvenliğinin sağlanması için tren tarafında yarım boy ya da tam boy peron ayırıcı kapı sistemi kullanılabilmektedir (Şekil 23, 24, 25). Peron ayırıcı kapı sisteminde bulunan kapılar, yolcular treni beklerken kapalı haldedir, tren geldiğinde açılmaktadır.

Bu sistem; trenin yolcuya çarpması, yolcunun ya da yolcunun taşıdığı herhangi bir şeyin (çocuk arabası, valiz gibi) tren hattına düşmesi, intihar gibi olayların önlenmesinde etkili olmaktadır. Yolcu sayısı çok olan istasyonlarda bu sistemin kullanılması önerilmektedir.

Şekil 23: Hong Kong Heng Fa Chuen Metro İstasyonu (Yarım Boy Kapı Sistemi) (https://upload.wikimedia.org/wikipedia/commons/6/6b/MTR_HFC_%285%29.JPG)

Şekil 24: Londra Webminster Tube Metro İstasyonu (Tam Boy Kapı Sistemi) (https://upload.wikimedia.org/wikipedia/commons/b/b8/Westminster.tube.station.jubilee.arp.jpg)

Şekil 25: Paris Lyon Metro İstasyonu (Tam Boy Kapı Sistemi) (http://img.fotocommunity.com/pariser-metro-linie-14-3922eac6-a0dc-4c3b-8583-a98889e38d18.jpg?width=1000)

- **Yardımcı Mekanlar**

Yer altı metro istasyonlarında istasyon girişleri, yatay dolaşım alanları, düşey dolaşım elemanları, bilet holü ve peron dışında kalan bütün alanlar yardımcı mekanlardır. Yardımcı mekanlar; teknik mekanlar, işletme personeli mekanları ve yolcu hizmet mekanları olmak üzere üç başlıkta toplanabilir.

- **Teknik Mekanlar**

Teknik mekanlar, yer altı metro istasyonlarında bakım ve işletme ile ilgili olan ve sadece işletme personeli tarafından kullanılan alanlardır. Bu alanlar mekanik, elektrik ve elektronik ile ilgili teknik mekanlar olarak üç farklı grupta değerlendirilebilir. Mekanik ile ilgili teknik mekanlar havalandırma, yangın söndürme ve mekanik tesisatı gibi konularla ilgili olan mekanları kapsamaktadır. Bu mekanlar; tünel havalandırma fan odası, istasyon duman atım fan odası, istasyon taze hava besleme fan odası, su deposu, yangın pompa odası, pissu pompa odası, hidrofor odası ve yangın tüp odası olarak sayılabilir.

Elektrik ile ilgili teknik mekanlar ise istasyon içerisinde bulunan mekanların enerji ihtiyaçlarının düzenlenmesi, tren enerjisinin temini ve acil durum enerjisinin planlanması gibi konularla ilgili olan mekanlardır. Bu mekanlar; OG (Orta Gerilim) odası, cer odası, AG (Alçak Gerilim) ana dağıtım pano odası, AG (Alçak Gerilim) tali dağıtım pano odası, yürüyen merdiven pano odası, transformatör odası, katener odası, peron ayırıcı kapı sistemi pano odası, UPS (Uninterruptible Power Supply) odası, akü odası ve kompresör odası olarak sayılabilir.

Elektronik ile ilgili teknik mekanlar; haberleşme ve sinyalizasyon, telsiz, telefon, yolcu erişim ve yolcu bilgilendirme sistemlerinin sağlanması gibi konularla ilgili olan mekanlardır. Bu mekanlar; kontrol merkezi, sinyalizasyon odası, haberleşme odası ve GSM (Global System for Mobile Communications) odası olarak sayılabilir.

Sistem teknolojisi ile bağlantılı teknik mekanlar bir araya toplanmalıdır. Bu yerlere giriş güvenlik altına

alınmalı ve korunmalıdır. Teknik mekanlara istasyon içerisinde yer alan genel mekanlardan veya emniyetli ve kontrollü olarak dışarıdan erişilebilmelidir.

- **İşletme Personeli Mekanları**

İşletme personelinin kullanımındaki mekanlardır. Bu mekanlar; istasyon işletme odası, güvenlik kabini, personel dinlenme odası, personel soyunma odası (erkek ve kadın), personel tuvaleti (erkek ve kadın), temizlik odası, depo ve makinist dinlenme odası olarak sayılabilir.

İstasyon işletme odası, bilet holü kontrollü alanında, yolcu akışını ve turnikeleri doğrudan görebilecek şekilde planlanmalıdır. Bu odanın yolculu bölüme bakan ön cephesi açık bir görüş alanı sağlamak için saydam yapılmalıdır. İşletme odasına erişim doğrudan bilet holünden değil, ara koridor bağlantısından sağlanmalıdır. Çift bilet holü olan istasyon yapılarında, istasyon işletme odasının büyük olan bilet holünde olması tercih edilmelidir.

Güvenlik kabini, turnikelere yakın bir alanda düzenlenen, herhangi bir saldırı anında güvenlik personelinin geçici olarak korunabileceği mekandır. Bu mekanda, güvenlik personelinin gerektiğinde yardım çağırabilmesi için alarm ve haberleşme cihazları bulunmalıdır.

İstasyonlarda işletme personelinin kullanımına yönelik personel dinlenme odası, personel tuvaleti, personel soyunma odası, temizlik odası, güvenlik işaret ve levhaları gibi teknik malzemelerin bulunacağı depo olmalıdır. Hattın ilk ve son istasyonlarında birer makinist odası yer almalıdır.

- **Yolcu Hizmet Mekanları**

İstasyonlarda istasyon giriş ve çıkışları, yatay dolaşım alanları, düşey dolaşım elemanları, bilet holü (konkors) ve peron dışındaki yolcu kullanımına yönelik planlanan mekanlardır. Bu mekanlar; bilet satış gişesi, yolcu tuvaleti (erkek, kadın ve engelli), bebek bakım odası, ilk yardım odası, mescit, kayıp eşya ofisi ve ticari alanlar olarak sayılabilir.

Yolcu hizmet alanlarının yerleşimi, büyüklüğü ve dağılımı istasyonların özeliklerine göre dikkatle seçilmelidir. Yoğun kullanımlı istasyonlarda, işletmenin ihtiyacına göre bilet verme makinelerine ek olarak, bilet satış gişeleri düzenlenebilir. Bilet alma işlemi yolcuların istasyonda en fazla yaptığı aktivitelerden biridir. Bu nedenle bilet satış gişesi kolay görülebilir bir alanda yer almalı ve kullanımı rahat olmalıdır.

Yer altı metro istasyonlarında yolcular için tuvalet ve lavabo tesis edilmelidir. İstasyonlarda yolcu tuvaleti gibi yardımcı mekanlar için çıkmaz yol yapılması gerekirse, bu yolun uzunluğu 30,00 m'yi geçmemelidir (TS 12127, 1997). Yolcu kullanımına yönelik olarak tasarlanan bilet satış gişesi, yolcu tuvaleti (erkek/kadın/engelli), bebek bakım odası, sağlık odası, mescit gibi yolcu hizmet alanları bilet holü katının ücretsiz alanında, yolcuların rahat erişebileceği ve görülebilir noktalarda yer almalıdır.

Yolcu yoğunluğunun fazla olduğu istasyonlarda yolcu kullanımına yönelik ticari alanlar düzenlenebilir. Ticari alanların yerleşiminde öncelikli olan yolcu emniyetidir. Bu alanların önünde oluşabilecek yoğunluk için birikme alanları da düşünülmeli, yolcu dolaşımı engellenmemelidir. Yanıcı, duman üreten veya alev alabilecek maddeler bulunduran mağaza ve dükkanlardan kaçınılmalıdır. Ticari alanlar planlanırken mal girişi, atık yönetimi gibi konular düşünülmeli ve uygun çözümler üretilmelidir. Ticari alanlara ait vitrin, tabela, reklam gibi elemanlar istasyon mimarisiyle uyumlu olmalıdır.

SONUÇ VE DEĞERLENDİRME

Yer altı metro istasyonlarının tasarım aşamasında alınacak bir çok karar, her istasyonun kendisine özeldir ve çok önemlidir. Bu yapılarda hem konforlu, keyifli, güvenli ve estetik mekanlar oluşturmak hem de bu yapıların sorunsuz kullanımı için, mekanlar kurallara uygun olarak tasarlanmalıdır. İyi planlanmış bir istasyon yapısı yolcuların güvenli bir biçimde perona

ulaşımını kolaylaştıracak ve yolculuk süresini kısaltacaktır.

Yer altı metro istasyonu tasarımında, normal işletim ve acil durum tahliye hesapları dikkate alınarak, belirlenen tahmini yolcu kapasitesine göre istasyon içerisindeki yolcu hareketlerinin aksamadan sağlanması esastır. Planlama aşamasında hedef, kurallara bağlı tasarım yaparak yolcu kapasitesi bakımından dengelenmiş mekanlar (istayon girişi, yatay dolaşım alanları, bilet holü, peron) oluşturmaktır. Bu nedenle tasarım aşamasında, gelecekteki yolcu kapasitesi de düşünülmeli ve öngörülere göre tasarım yapılmalıdır. İstasyonu kullanacak yolcu sayısına göre, peron tipi ve peron adedi belirlenmelidir. Yolcu yoğunluğunun ve hat sayısının fazla olduğu istasyonlarda Almanya Müncher Freihet Metro İstasyonu'nda olduğu gibi orta peron sayısı artırılabilir ya da Sao Paulo Metro İstasyonu'nda olduğu gibi katlı çözümlere gidilebilir.

Dünyada, özellikle Türkiye'de birçok uygulamada, istasyon giriş yapıları açık veya yarı açık olarak tasarlanmaktadır. Bu nedenle iç mekanlarda dış hava koşulları ile ilgili sorunlar yaşanmaktadır. Yapıların su alması, merdivenlerde buzlanma gibi sorunların önlenmesi için giriş yapıları kapatılmalıdır. Böylelikle hem dış hava koşullarına karşı önlem alınacak hem de giriş yapılarının kentsel algısı artacaktır. Bu yapılara örnek olarak, Londra Canary Wharf Metro İstasyonu, Baltimore Metro İstasyonu ve Dubai Metro İstasyonu verilebilir. Ayrıca, yer altı metro istasyonları için su basması, özellikle su taşkın kotu yüksek bölgeler için sorun teşkil edebilmektedir. Bu nedenle istasyon girişleri, havalandırma bacaları ve asansörler taşkın kotundan daha üst kotta düzenlenmeli veya riskli bölgelerde taşkın anında devreye giren özel çözümler üretilmelidir.

Bedensel engelli, bebek arabalı ve yaşlı kulllanıcılar düşünüldüğünde istasyon yapılarında asansörlerin gerekliliği tartışılmaz. Bununla birlikte peron derinliği fazla olan veya perona ulaşımın uzun olduğu istasyonlarda asansörler tüm yolcular tarafından da tercih edilmekte ve yer altı metro istasyonu tasarımında önem kazanmaktadır. Ancak, istasyon yapılarında asansör çok az sayıda tesis edilmekte ve bu nedenle perona ulaşım süresi uzamaktadır. Bu tür yapılarda asansör sayısı ve kapasitesi artırılmalıdır.

İstasyonlarda kaza geçirme riskinin en yüksek olduğu mekan perondur. Özellikle yolcu sayısının fazla olduğu istasyonlarda kazalar artmaktadır. Bu nedenle yolcuların kaza geçirme riskini önleyecek yarım veya tam boy peron ayırıcı kapı sistemleri kurulması can ve mal güvenliği açısından önemli görülmektedir. Ayırıcı kapı sistemlerine, Hong Kong Heng Fa Chuen Metro İstasyonu, Londra Webminster Tube Metro İstasyonu ve Paris Lyon Metro İstasyonu'ndaki uygulamalar benzer örnekler olarak verilebilir. Ancak, bu sistemler maliyetleri nedeniyle genelde tercih edilmemektedir.

Peronlarda hem yapım yöntemi hem de asma tavan uygulamaları nedeniyle tavan yüksekliği azalabilmekte ve basık mekanlar oluşabilmektedir. Bu tür mekanlar kullanıcılar üzerinde olumsuz etkiler oluşturmaktadır. Mekan yükseklikleri, Lizbon Olaias Metro İstasyonu ve Münih Georg-Brauchle-Ring Metro İstasyonu örneklerinde olduğu gibi rahat mekan algısı yaratacak biçimde artırılmalıdır.

Yer altı metrolarında her istasyonun bir tasarım temasının, bir kimliğinin olması, kullanıcıların bulundukları mekanı algılaması açısından önemlidir. Varşova Metrosu'ndaki uygulama buna iyi bir örnektir. Bu metro hattının her istasyonu farklı renkte tasarlandığı için, yolcular istasyon rengine bakarak hangi istasyonda olduğunu anlayabilmektedir. Böylelikle her istasyon rengiyle anılmakta ve renkler yolcularda istasyon hafızası oluşturmaktadır.

Yer altı metro istasyonları yapıları gereği soğuk mekanlardır. Özellikle uzunluğundan dolayı merdiven tünelleri ve yaya koridorları kullanıcılar tarafından rahatsız edici bulunmaktadır. Bu mekanlar, kapalı mekanlar olduğundan ferah ve aydınlık ortamlar oluşturulabilmesi için yüzeylerde açık renkler tercih edilmedir. Bu mekanları daha sıcak, canlı ve enerjik

hale getirmek için birkaç renk bir arada kullanılabilir. İnsanları, kent ve kent yaşantısından koparan, doğal ışığın yerini karanlığa bıraktığı istasyon yapıları, doğru bir şekilde aydınlatılmadığında, insanlarda kapalı mekan korkusu oluşturmakta, suç işleme potansiyelini artırarak kente hizmet etmek yerine, kente ve kentliye sorun yaratmaktadır. Bu nedenle istasyonlar iyi aydınlatılmalı ve güvenli dolaşıma olanak sağlanmalıdır. Renk ve aydınlatma konusunda, Münih Marienplatz Metro İstasyonu, Rotterdam Wilhelminaplein Metro İstasyonu ve Rio de Janeiro Copacabana Metro İstasyonu yatay dolaşım alanları doğru tasarımlar olarak örneklenmektedir.

Birçok metro istasyonunda yolcuların günlük ve acil ihtiyaçlarını karşılayacak mekanlar yer almamaktadır. Yoğun kullanımlı istasyonlarda, bebek bakımı için gerekli mobilyaların yer aldığı bebek bakım odası ve sağlık sorunları (kalp krizi, sara nöbeti vb.) veya trende/istasyonda kaza sonucu yaralanmalar gibi acil durumlarda yolcuya ilk müdahalenin yapılabileceği ilk yardım odası düzenlenmelidir. İnsanların metroyu hergün kullandıkları düşünüldüğünde, yolcu dolaşımını aksatmayacak uygun noktalarda büfe, kafeterya, market gibi ticari alanlar da tasarlanabilir.

KAYNAKLAR

1. Demir, E., Metro Duraklarının Mekânsal Özellikleri ve Kent İmajı Üzerindeki Etkileri: Ankara Kızılay-Batıkent Metro Hattı Analizi, Yüksek Lisans Tezi, Gazi Üniversitesi, Fen Bilimleri Enstitüsü, (2007).
2. Demiryolları Planlama ve Tasarım Teknik Esasları, T.C. Ulaştırma Bakanlığı, Demiryollar Limanlar Havameydanları İnşaatı Genel Müdürlüğü, Yüksel Proje, Ankara, (2007).
3. Edwards, B., The Modern Station, New Approaches to Railway Architecture, Aiden Press Oxford, London, (1997).
4. http://fotospublicas.com/paineis-de-led-sao-instalados-na-estacao-se-metro-em-sao-paulo/, Sao Paulo Central Subway Station in Brazil, (Erişim tarihi: 28 Aralık 2016).
5. http://images.adsttc.com/media/images/554a/a083/e58e/ce61/f200/00dc/large_jpg/C12_6(2).jpg?1430954101, Warsaw M2 line, (Erişim tarihi: 10 Ocak 2017).
6. http://img.fotocommunity.com/pariser-metro-linie-14-3922eac6-a0dc-4c3b-8583-a98889e38d18.jpg?width=1000, Parisier metro, linie 14, (Erişim tarihi: 10 Ocak 2017).
7. http://s21.postimg.org/4pfbzmwfb/Wuhan_metro_8.jpg, Wuhan subway metro entrance, (Erişim tarihi : 10 Ocak 2017)
8. http://urbantoronto.ca/sites/default/files/images/projects/836/836-2059.jpg, Downsviwe park station to conncet Spadina subway to go, (Erişim tarihi: 19 Ocak 2017)
9. http://www.e-architect.co.uk/images/jpgs/rotterdam/wilhelminatunnel_zj060209_2.jpg, Wilhelminaplein metro station, (Erişim tarihi: 10 Ocak 2017).
10. http://www.ibb.gov.tr/tr-TR/HaberResim/21403/_t/2_JPG.JPG, Yapımı biten yaya bağlantı tünelleri pazartesi açılıyor, (Erişim tarihi: 11 Ocak 2017).
11. http://www.skyscrapercity.com/showthread.php?t=431156&page=90, Russia urban transport compilation, (Erişim tarihi: 28 Aralık 2016).
12. http://www.sumit4allphotography.com/wp-content/uploads/2015/05/munich4-015.jpg, Metro stations in Münih, (Erişim tarihi: 28 Aralık 2016).
13. http://www.vivireltren.es/2012/03/una-averia-afecta-a-la-circulacion-de-las-lineas-3-y-5-de-metro-valencia/, Metro Valencia, (Erişim tarihi: 28 Aralık 2016).
14. https://c2.staticflickr.com/6/5550/10711119366_2976a8853c_b.jpg, Metro Rio de Janerio Copacabana subway, (Erişim tarihi: 10 Ocak 2017).
15. https://s-media-cache-ak0.pinimg.com/564x/5c/06/cb/5c06cb806cb4a4b9fb474038aba7e46c.jpg, What does a subway entrance say about its city?, (Erişim tarihi: 10 Ocak 2017).
16. https://temporarilylostdotcom.files.wordpress.com/2013/02/taipei-1-crowded-subway-station.jpg, Taipei crowded subway station, (Erişim tarihi: 28 Aralık 2016).
17. https://upload.wikimedia.org/wikipedia/commons/0/0f/Munich_subway_station_M%C3%BCnchner_Freiheit_2009-12.jpg, Munich u-bahn, (Erişim tarihi: 28 Aralık 2016).
18. https://upload.wikimedia.org/wikipedia/commons/2/28/U-Bahn-Muenchen_Candidplatz_-_2007-CC-BY-SA_SYNTAXYS-Achim-Lammerts.jpg, Munich U-bahn, (Erişim tarihi: 28 Aralık 2016).
19. https://upload.wikimedia.org/wikipedia/commons/6/6b/MTR_HFC_%285%29.JPG, Chai Wan transport, (Erişim tarihi: 28 Aralık 2016).

20. https://upload.wikimedia.org/wikipedia/commons/7/7e/Metro_de_Lisboa_-_Esta%C3%A7%C3%A3o_Olaias_(8175721609).jpg, Metro de Lisboa, (Erişim tarihi: 28 Aralık 2016).

21. https://upload.wikimedia.org/wikipedia/commons/7/7e/Metro_de_Lisboa_-_Esta%C3%A7%C3%A3o_Olaias_(8175721609).jpg, Downsviwe park station to conncet Spadina subway to go, (Erişim tarihi: 19 Ocak 2017)

22. https://upload.wikimedia.org/wikipedia/commons/8/8e/Canary_Wharf_Tube_Station_-_July_2009.jpg, Canary Wharf tube station, (Erişim tarihi: 28 Aralık 2016).

23. https://upload.wikimedia.org/wikipedia/commons/8/8e/Metro_SPB_Line5_Sportivnaya_Travelator_Tunnel.jpg, Moving walkway, (Erişim tarihi: 28 Aralık 2016).

24. https://upload.wikimedia.org/wikipedia/commons/b/b8/Westminster.tube.station.jubilee.arp.jpg, Webminister tube station, (Erişim tarihi: 28 Aralık 2016).

25. https://upload.wikimedia.org/wikipedia/commons/c/cc/Munich_subway_GBR.jpg, List of Munich U-bahn stations, (Erişim tarihi: 28 Aralık 2016).

26. https://upload.wikimedia.org/wikipedia/commons/f/fa/Metro_Prague_-_Hradcanska_Station.JPG, Metro Prague: Hradcanska station, (Erişim tarihi: 28 Aralık 2016).

27. Keskiner, B. S., İstanbul Metro Çıkışlarının Yaya-Taşıt İlişkileri Çerçevesinde Değerlendirilmesi: Kadıköy-Kartal Metro Hattı Örneği, Yüksek Lisans Tezi, İsanbul Teknik Üniversitesi, Fen Bilimleri Enstitüsü, (2015).

28. Metro Tasarım Kriterleri, T.C. Ulaştırma Bakanlığı Demiryollar Limanlar Havameydanları İnşaatı Genel Müdürlüğü, Ankara, (2010).

29. NFPA 130., Standart For Fixed Guideway Transit and Passenger Rail Systems, (2010).

30. Özbek, E., Metrolarda Yön Bulma Davranışının Çevresel Stres Bağlamında İrdelenmesi, Yüksek Lisans Tezi, İstanbul Teknik Üniversitesi, Fen Bilimleri Enstitüsü, (2007).

31. Rauch, J., Architektur von U-Bahnhöfen = The architecture of Underground Railway Stations, Stuttgart: K. Kramer, (1996).

32. Ross, J., Railway Stations: Planning, Design, and Management, Architectural Press, Oxford, (2000).

33. Sevdin, A., Mimari Tasarımda Bina Total Performansı Kavramı: Metro İstasyonlarında Değerlendirme, Yüksek Lisans Tezi, İstanbul Teknik Üniversitesi, Fen Bilimleri Enstitüsü, (1992).

34. Station Capacity Assesment Guidance, Netwok Rail, 2011.

35. TS 12127, Şehiriçi Yollar - Raylı Taşıma Sistemleri Bölüm 1: Yeraltı İstasyon Tesisleri Tasarım Kuralları, Türk Standartları Enstitüsü, Ankara, (1997).

36. TS 12460, Şehiriçi Yollar - Raylı Taşıma Sistemleri Bölüm 5: Özürlü ve Yaşlılar İçin Tesislerde Tasarım Kuralları, Türk Standartları Enstitüsü, Ankara, (1998).

37. TS 12511, Şehiriçi Yollar-Raylı Taşıma Sistemleri Bölüm 7: Ulaşım Sistemi Sembolü Tasarım ve Yerleştirme Kuralları, Türk Standartları Enstitüsü, Ankara, (1998).

http://dergipark.gov.tr/tujes
Trakya University Journal of Engineering Sciences, 18(1): 17-30, 2017
ISSN 2147–0308
Araştırma Makalesi / Research Article

NON-LINEAR ANALYSIS OF BRIDGE STRUCTURES

Kubilay KAPTAN[1]

[1]*Beykent Üniversitesi, Mühendislik-Mimarlık Fakültesi, İnşaat Mühendisliği Bölümü, 34396, İstanbul*

Abstract: For the health tracking of civil infrastructures, it is essential to determine the non-linear behaviour connected to structural damage. For the precise assessment of these types of non-linear behaviours, it is essential to evaluation of how these structures will function when exposed to specific earthquake movement. To determine the behaviour, non-linear static or non-linear time history analysis approach can be utilized, but the locally destroyed impact has to be also regarded. With the prominent impact of basic mode of non-linear static approach, non-linear time history evaluation approach is broadly utilized for the evaluation of complex non-linear behaviour with many degrees of freedom and with local damages. In this study, the non-linear time history evaluation method with some restricted higher modes accounting the impact of local damages is suggested. Specifically, some RC piers are presumed to be surpassed the yield capability throughout earthquakes and trigger large inelastic deformations and damage. To identify the seismic response extremely impacted by the hysteretic behaviour of destroyed RC piers, the modified Takeda model is presented. As a confirmation of effectiveness of suggested approach, the non-linear responses of damaged bridge structure are investigated among suggested approaches and above described traditional non-linear analysis approach.

Keywords: Nonlinear Dynamics; hysterical model; modified Takeda model; modal order; substructure

KÖPRÜ YAPILARININ DOĞRUSAL OLMAYAN ANALİZİ

Özet: Altyapı tesislerinin doğru ve sağlık takibi için, yapısal hasarın doğrusal olmayan davranışının belirlenmesi esastır. Bu tür doğrusal olmayan davranışların kesin olarak değerlendirilmesi için, bu yapıların belirli deprem hareketlerine maruz kaldıklarında nasıl işlev görecekleri incelenmelidir. Davranışı belirlemek için, doğrusal olmayan statik veya doğrusal olmayan zaman artımı (time history) yöntemi kullanılabilir, ancak yerel etkiler de göz önüne alınmalıdır. Doğrusal olmayan statik yaklaşımla doğrusal olmayan zaman artımı yöntemi yaklaşımı, birçok serbestlik derecesi ve yerel hasarlar içeren karmaşık ve doğrusal olmayan davranışın değerlendirilmesi için yaygın olarak kullanılmaktadır. Bu makalede, yerel hasarların etkisini dikkate alan sınırlı yüksek modları olan doğrusal olmayan zaman artımı yöntemi önerilmiştir. Özellikle bazı betonarme ayakların, depremler sırasında esneme kapasitelerini aştığı ve bunun da büyük inelastik deformasyonları ve hasarları tetiklediği varsayılmaktadır. Hasar görmüş betonarme ayakların histerik davranışından aşırı derecede tetiklenen sismik etkiyi tanımlamak için değiştirilmiş Takeda modeli sunulmuştur. Önerilen yaklaşımın etkililiğinin doğrulanması için, hasar görmüş köprü yapısının doğrusal olmayan tepkileri, önerilen yaklaşımlar ve yukarıda açıklanan geleneksel doğrusal olmayan analiz yaklaşımı ile incelenmiştir.

Anahtar Kelimeler: Doğrusal olmayan dinamik; histerik model; modifiye Takeda modeli; modal sıralama; alt yapı

INTRODUCTION

The forces induced on a bridge structure with reinforced concrete (RC) piers during major earthquakes may exceed the yield capacity of some piers and cause large inelastic deformations and damages in the piers as depicted in Figure 1.

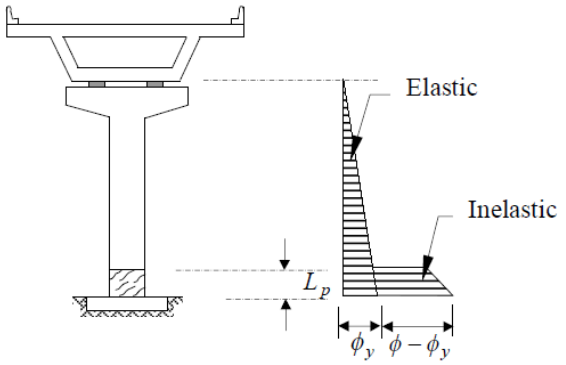


Figure 1. Inelastic behavior of a RC bridge pier

Since the seismic response of bridge piers is highly affected by the hysteretic behavior when they have damaged, reliable model for such behavior is needed. The system of strength deterioration of RC elements is generally construed by concrete spalling and interface bond slip among the concrete and embedded reinforcements. In the celebrated damage model for RC members suggested by Park and Ang (1985), cumulative damage is based on a linear combination of the maximum displacement and the cumulative hysteretic energy dissipation. Nevertheless, only one of the two variables is generally integrated in existing strength deterioration models in the literature, say several models are structured only on the maximum displacement, such as models in Lai et al (1984), Roufaiel and Meyer (1987), Chung et al (1989) and Yousseef and Ghobarah (2001), though others on the cumulative energy dissipation, such as in Kunnath et al (1997), Mork (1991), Rahnama and Krawinkler (1993) and Sucuoglu and Erberik (2004).

The bilinear peak driven hysteretic model as demonstrated in Figure 2 and 3 presents a typical base for all the existing strength deterioration models. The strength deterioration can be indicated either by softening the skeleton curves (Figure 2) or shifting the reloading oriented points (Figure 3). In Figure 2 and 3, F_{yi} relates to the yield strength at the ith loading cycle; Δu_o and ΔF_o refer to the change of displacement and force of the oriented point, correspondingly. Triangles and circles indicate the maximum displacement point and the reloading oriented point in a loading cycle, correspondingly.

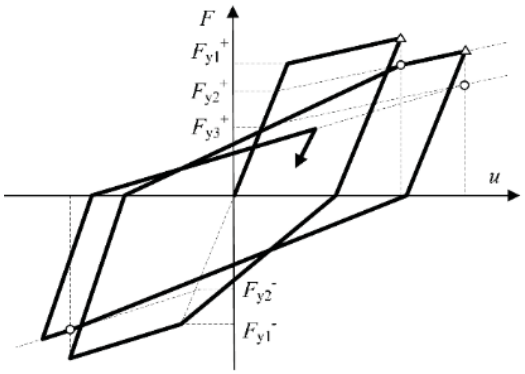


Figure 2. Strength deterioration in peak oriented hysteretic model: Soften the skeleton curve

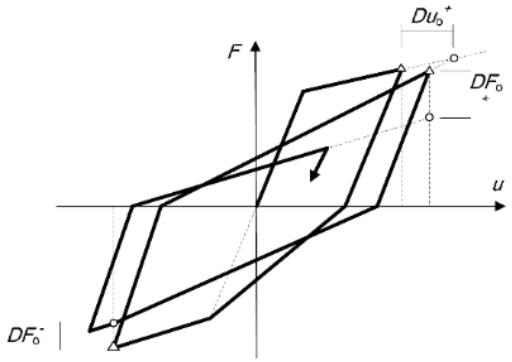


Figure 3. Strength deterioration in peak oriented hysteretic model: Move the reloading oriented point

Amongst different models, stress-strain constitutive models are the most popular as they provide more realistic representation of concrete behaviour such as stress-strain relationship, and non-linear behaviour in cracking and crushing; and they have been used in modelling of the structure based on the computationally

powerful method, the Finite Element Method. In constitutive modelling of concrete materials, it is known that either plasticity-fracture or plasticity-fracture-damage models are required in order to simulate concrete behaviour well (Jefferson 1999, 2002a, 2003a). In literature, however, no one constitutive model is yet able to properly describe all aspects of non-linear concrete behaviour because of the complexity of multiaxial behaviour of concrete. In addition, not many constitutive models have been successfully implemented into engineering practice to deal with both complex RC structures and earthquake loadings. Therefore, another important objective of the research is to employ two of the most recently developed constitutive models, one based on the plasticity-fracture approach, namely Multi-crack model (Jefferson 1999) and the other based on plasticity-fracture-damage approach, namely Craft model (Jefferson 2003a, 2003b), for modelling concrete and RC structures under different types of loading. In spite of the numerical efficiency of these methods, however, enough many modes have to be included or the influence of truncated modes have to be corrected to achieve an approximated result with reasonable accuracy particularly on local behavior (Dikens et al. 1997).

In concrete material, strain-softening problem is a common phenomenon (Hillerborg et al. 1976, Bazant and Oh 1983). This is also considered in the constitutive models used in this study, based on continuum mechanics. Strain-softening can induce localised instabilities in the numerical procedure and consequently, non-unique solutions or mesh-dependency problems for numerical analysis (Crisfield 1982, Zienkiewicz and Taylor 1991, Crisfield 1996), and thus use of classical continuum mechanics in this case has been proved to be inadequate (Comi 2001, Jirasek and Bazant 2002). In an attempt to avoid mesh dependency problem, the fracture energy provisions of crack is used (Hillerborg et al. 1976). In the smeared cracking approach, cracking is assumed to be spread over a 'numerical' fracture process zone which is numerically or mathematically equated the characteristic length of an element. As this characteristic length is related to the adopted finite element size, the spurious mesh dependency can be eliminated (Bazant and Oh 1983, Oliver 1989). Due to these softening-related problems, the identification of model parameters and non-linear procedures play a crucial part in the validation and application of the models.

Seismic design of RC bridge piers is increasingly performed using dynamic analysis in the time domain, where the responses of the structure to appropriately selected time-histories is strongly dependent on the characteristics of the earthquake ground motions. Besides, the dynamic effects that arise from the random ground motions should be taken into account for the characterisation and the modelling of the non-linear and damage behaviour of RC bridge piers through its material models. However, seismic applications of finite element material models have not been widely used for such investigations due to technical challenges in implementing them into non-linear dynamic analysis. As a result, very little work has been done into the non-linear dynamic response and damage behaviour as well as their quantitative measures for RC bridge piers under earthquake time-histories (Kwan and Billington 2003, Hindi and Sexsmith 2004). Therefore, the non-linear dynamic response and damage are also pursued in this study, with the use of nonlinear material models for the analyses of RC bridge piers under artificially generated timehistories.

In this study substructuring method with modal correction vectors and modal sorting method are proposed to analyze reinforced concrete structures having locally damaged properties. The hysteretic behaviors of the damaged concrete structures are reproduced by multi linear hysteretic model with

*

limited nonlinear parameters including the characteristics of stiffness degradation, pinching effect by shear and axial force and strength deterioration (Lee and Yun 2008). Figure 4 shows different hysteresis models.

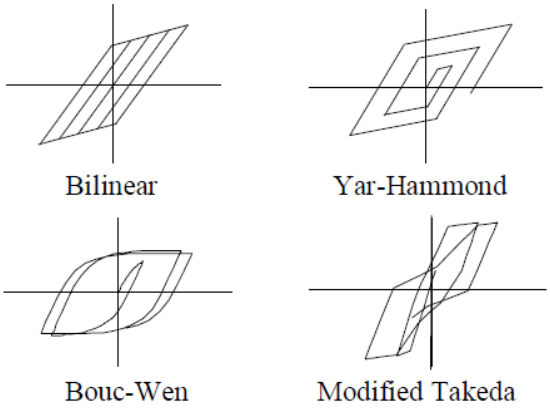


Figure 4. Hysteresis models

SEISMIC RESPONSE ANALYSIS OF RC BRIDGE PIER

It is obvious that under different earthquake time history records, the structure experiences different response and damage. In order to analyse and compare the response and damage behaviour of the structure, a method for quantifying the damage has to be devised and used. One class of methods to quantify damage is the use of a "damage index" to create a single measure that adequately represents the complex seismic behaviour. Damage indices aim to provide a mean of quantifying numerically the damage in reinforced concrete structures sustained under cyclic and earthquake loading (Hindi and Sexsmith 2001, 2004). In earthquake engineering literature, there have been various damage measures proposed and considered in the experimental and theoretical studies to explain damages observed in the structures under artificial ground motions or in actual structures subjected to real earthquake motions such as Park and Ang (1985), Chung et al. (1989), Chai et al. (1995), Fajfar and Gaspersic (1996), Ghobarah et al. (1999), and Hindi and Sexsmith (2001).

Many studies have been performed in the analysis or characterisation of seismically-induced damage to reinforced concrete members and, in particular, RC bridge piers (Banon et al. 1981, Park and Ang 1985, Roufaiel and Meyer 1987, Stephens and Yao 1987, Jeong and Iwan 1988, Chung et al. 1989, Williams and Sexsmith 1995, William et al. 1997, Ghobarah et al. 1999, Hindi and Sexsmith 2001, and Erberik and Sucuoglu 2004, Kim et al. 2005). However, the majority of these studies are based on data from static cyclic tests in both numerical and experimental areas.

NONLINEAR HYSTERIC BEHAVIOR

Roufaiel and Meyer (1987) proposed an extension of the spread plasticity model developed earlier by Meyer et al. (1996). The new model includes the effect of shear and axial forces on the flexural hysteretic behavior based on a set of empirical rules.

The hysteretic moment-curvature relation is described by Takeda's model. The variation of axial loads due to overturning moments is not accounted for. The analytical results are compared with available experimental data and show very good agreement. A set of new damage parameters is proposed which correlate well with the residual strength and stiffness of specimens tested in the laboratory. In the modified Takeda model, four different kinds of braches may exist in the hysteresis of the moment-curvature (M -ϕ) relationship as in Figure 5. Basically, The Takeda model (Takeda et al. 1970) includes the phenomenon of stiffness degradation in reinforced concrete members subject to cyclic loading. Roufaiel and Meyer (1987) introduced a model that accounts for the pinching effects due to shear force and strength degradation after yielding.

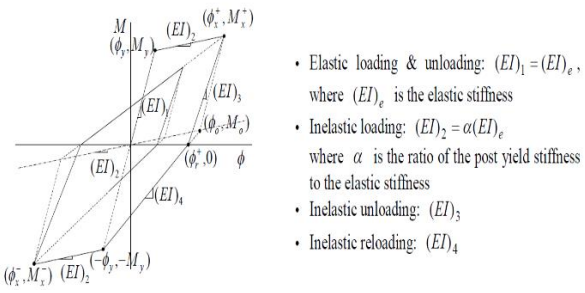


Figure 5. Hysteretic moment - curvature behavior of the modified Takeda model

Park and Ang (1985) formulated and suggested a hysteretic model utilizing damage index to define the gradual strength degradation and softening perform in reinforced concrete structural members caused by repetitive increase of the maximum deformation maintained by the member. Nevertheless, few of them contain all the factors of the deterioration of strength, stiffness, and ductility features in a comprehensive hysteretic design to get the inelastic behavior of reinforced concrete members under big reversal cycles loading. The hysteretic designs for modeling the phenomena of stiffness degradation, pinching effect, and strength deterioration and softening are in short, described here. When a reinforced concrete structural member is subjected to repeated cyclic loading above its elastic limit, the evolvement of concrete cracking and plastic behavior of the reinforcing steel with linked anchorage slip would head to the deterioration of the stiffness of the reinforced concrete member at each cyclic loop. A Q-HYST degrading stiffness hysteretic model proposed by Saiidi and Sozen (1979), improved from the Takeda model (Takeda et al. 1970), can efficiently account the unloading stiffness. Laboratory assessments performed on reinforced concrete specimens by Popov et al. (1972) and Ma et al. (1976) have identified that there is a strong correlation among the degree of pinching and the magnitude of shear at the section, and that pinching effect minimizes the load resistance of the member during reloading.

In this study, the concrete bridge pier is assumed to be locally damaged at the bottom of the pier due to severe earthquake ground motion and the dominant nonlinear hysteretic behaviors can be effectively represented by four parameters like as yield moment(M_y), stiffness degradation(α), pinching (β) and stiffness deterioration(γ). Figure 6 shows typical hysteretic behavior of a RC members subjected to cyclic loadings for several cases of these parameters.

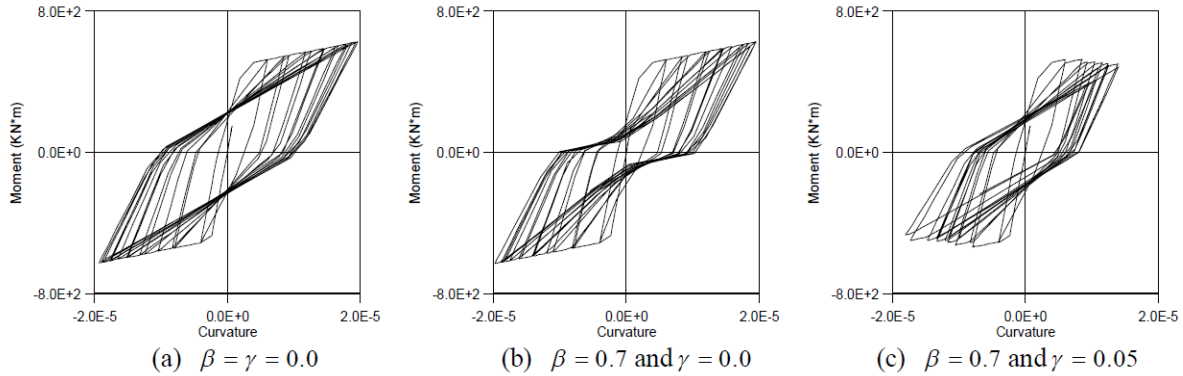


Figure 6. Moment vs. curvature in a RC bridge pier (M_y = 500KN.m y M = × , and α = 0.03)

NONLINEAR DYNAMIC ANALYSIS

In this approach, the seismic response of the framework is examined utilizing step-by-step time history analysis. The major methodology of this process is nearly identical to the static method of analysis. Nevertheless, this technique varies in the principle that the design displacements are not set up utilizing the targeted displacement; yet, are estimated through dynamic an

*

adanalysis by submitting the building model to an ensemble of the ground motions. The determined seismic response is very sensitive to the ground motion characteristics, and the examination is performed for more than one ground motion record.

To execute the non-linear dynamic analysis, the equation recommended by the Newmark's method (Chopra 1995) may be properly prolonged. Structured on review of analytical techniques, the non-linear dynamic analysis method is implemented for the analytical study because of its precision and effectiveness in identifying the inelastic seismic response of a system exposed to the ground motion data. The evaluation of previous research works show that the past research works have adopted static methods in majority for simplicity. However, the present research works in majority have adopted dynamic analysis (especially non-linear dynamic analysis) to accomplish much better precision to estimate the realistic seismic demands. Moreover, different seismic design codes prescribe dynamic analysis for medium and tall structures and it has been applied by recent analysts as well (Karavasilis et al. 2008; Panda and Ramachandra 2010). Therefore, non-linear dynamic analysis method has been implemented in the present study to determine the seismic response of the building models.

Integration Method using Nonlinear Modal Equations

The modal analysis approaches to nonlinear systems have been and continue to be an attractive idea, mainly because of the ability of these approaches to give fairly accurate solutions when only a few modes are considered, and because they provides directly the mode shapes and natural frequencies of the analyzed system, information that, even for nonlinear systems, is usually desirable to have. The equation of motion for a system with nonlinear properties when subjected to an earthquake ground acceleration may be written as

$$M\ddot{X}(t) + C\dot{X}(t) + KX(t) + R(t) = -M\{L\}\ddot{x}_g(t) \quad (1)$$

where *M*, *C* and *K* are the mass, damping and initial stiffness matrix; *X (t)*, $\dot{X}(t)$ and $\ddot{X}(t)$ are the displacement, velocity and acceleration vectors;$\{L\}$ is the influence vector accounting the direction of the earthquake excitation; $\ddot{X}_g(t)$ the ground acceleration, and *R(t)* is the nonlinear residual force vector. If the physical coordinates of Eqn. 1 are transformed to modal coordinates assuming the diagonal modal damping, the typical modal equation of the motion can be obtained as

$$\ddot{q}_n(t) + 2\varsigma_n\omega_n\dot{q}_n(t) + \omega_n^2 q_n(t) = \bar{f}_n(t) \qquad (n = 1, 2, \cdots, l) \quad (2)$$

where $q_n(t)$, $\dot{q}_n(t)$ and $\ddot{q}_n(t)$ the modal displacement, velocity and acceleration for the n-th mode; ζ_n z and ω_n are the corresponding damping ratio and natural frequency; and $\bar{f}_n(t)$is the modal load which includes the nonlinear residual force which depends on the unknown concurrent structural response. Hence, the above modal equations can be solved iteratively at each time by updating the nonlinear residual force.

Substructuring Method

Nonlinear damage is defined as the case when the initially linear-elastic structure behaves in a nonlinear manner after the damage has been introduced. One example of nonlinear damage is the formation of a fatigue crack that subsequently opens and closes under the normal operating vibration environment.

The substructuring method is probably effective in the model improving of large-scale structures and associated purposes. In these research, the global structure is divided into smaller and more controllable substructures. The substructures are assessed independently to acquire their specified solutions,

which are then built to restore the options to the global structure by imposing constraints at the interfaces.

In this study, to serve as a set of vectors with which to create the coupled system behavior within the sub-structures, the fixed interface normal modes are considered. Figure 7 shows the substructure model of locally damage bridge pier structure.

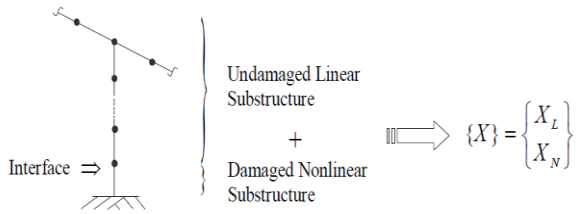


Figure 7. Substructure model of locally damage bridge pier structure

Denoting the properties associated to the linear and nonlinear substructures by the subscripts L and N, respectively, the equation of motion in Eqn. 3.1 can be written as follow:

$$\begin{bmatrix} M_{LL} & M_{LN} \\ M_{NL} & M_{NN} \end{bmatrix} \begin{Bmatrix} \ddot{X}_L \\ \ddot{X}_N \end{Bmatrix} + \begin{bmatrix} C_{LL} & C_{LN} \\ C_{NL} & C_{NN} \end{bmatrix} \begin{Bmatrix} \dot{X}_L \\ \dot{X}_N \end{Bmatrix} + \begin{Bmatrix} R_{LN} \\ R_{NN} \end{Bmatrix} =$$

(3)

In order to reduce the problem size using mode superposition in linear substructure, the following coordinate transformation can be applied:

$$\begin{Bmatrix} X_L \\ X_N \end{Bmatrix} = \begin{bmatrix} \Phi_{LL} & \psi & -K_{LL}^{-1} K_{LN} \\ 0 & 0 & I \end{bmatrix} \begin{Bmatrix} q_L \\ p \\ X_N \end{Bmatrix}$$

(4)

where L q is the linear modal response vector and p is the modal correction vectors to compensate the influence of the truncated modes. The modal correction vectors can be created using a mathematically consistent Rayleigh-Rits approximation where the assumed Ritz basis vectors are derived using the special force truncation vector. The nonlinear behavior of locally damaged structural dynamic systems can be obtained by solving the nonlinear modal equation with transformation of Eqn. 1 using above Eqn. 3.4. Various substructuring methods differ from each other by the determination of the reduction matrix, T.

Modal Sorting Method

When the modal analysis is used for the structural dynamic systems, the truncation of modes may cause significant difficulty in obtaining reasonable dynamic response (D'Aveni, A. and Muscolino, G. 2001), particularly for the locally damaged behavior. In this study, a modal sorting technique is proposed to select the modes with larger contribution to the DOF near the damaged location. The *j*-th modal contribution to the *i*-th DOF Ξ_{ij} under earthquake load nay be evaluated as

$$\Xi_{ij} = \phi_{ij} \Gamma_j S_j$$

(5)

where ϕ_{ij} is the *j*-th eigenvector at the *i*-th DOF, Γ_j is the modal participation factor at the *j*-th mode; S_j is the deformation response spectrum of the ground motion at the *j*-th natural period at $\omega=\omega_j$. The modes are sorted by the order of the magnitudes of those modal contribution values for a specific DOF. With the sorted modal vectors, the global displacement vector can be obtained as

$$X(t) = \tilde{\Phi} Q(t)$$

(6)

where $\overline{\Phi}$ is the matrix of the sorted eigen-vectors matrix, and Q(t) is the corresponding modal displacement vector. Then, as like the substructuring method, by using above Eqn. 6, it is possible to obtain the nonlinear modal equation and to apply the modal integration method to obtain the nonlinear dynamic responses.

*

SAMPLE STUDIES FOR HYSTERIC BEHAVIOR

Simplified Pier Model

This example is a simplified bridge model with a pier in the middle of the deck. It is assumed that the deck is supported by a single bridge piers and earthquake load is applied, so the effect of the deck may be considered as an additional lumped mass on the top of the pier. The pier is fixed the ground level. The earthquake acceleration is applied to the pier in the form of body force so that the relative displacement responses of the pier can be obtained directly. As mentioned above, for simplicity, axial load is not included in this study. The pier is modeled by 10 beam elements. The total number of DOFs is 30. The geometric and sectional properties of the pier are shown in Figure 8(a). The nonlinear hysteretic behavior is assumed to be occurred at the bottom of the pier during the earthquake. Figure 8(b) and (c) show the applied ground acceleration and the relation between the moment and the curvature in the bottom area of this model. To corroborate the possible differences in predictions between the models for a specific earthquake, EL CENTRO 1940 N-S motion (NS, peak ground acceleration (PGA) = 0.139g, 1979) was used as input for the three models and the displacement time history was computed and compared. A scaled El Centro earthquake is used. Figure 9 shows the time-scaled time histories used for simulation: NS 1940 El Centro record,

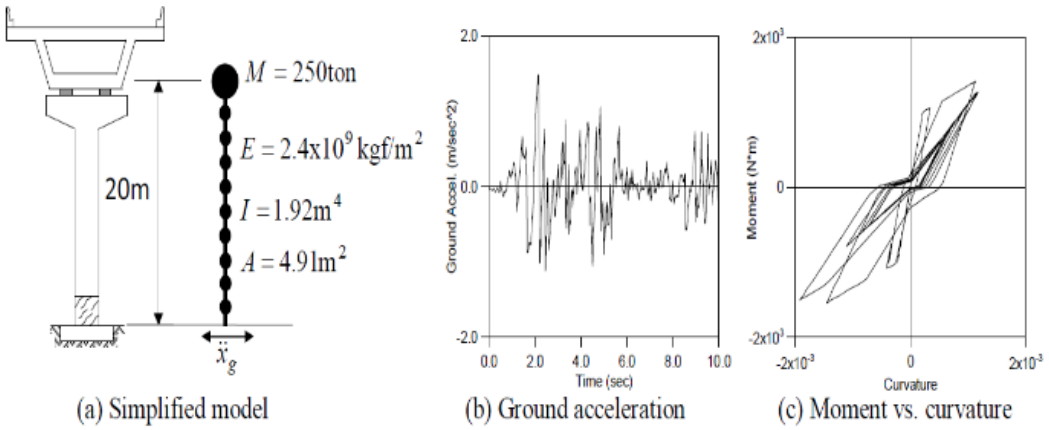


Figure 8. Cantilever model of bridge pier subjected earthquake excitation

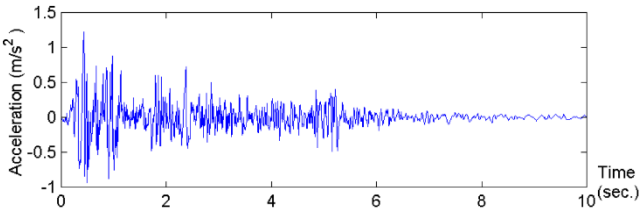


Figure 9. Time-scaled time histories used for simulation: NS 1940 El Centro record

The nonlinear hysteretic responses are obtained by the nonlinear modal integration, substructuring and modal sorting method and are compared with the response by the direct step by step integration method (Wilson-θ, θ=1.4). The first natural frequency is obtained as 0.41 Hz, while the damping ratio is assumed as 5% viscous damping for each mode.

The nonlinear parameters M_y, α, β and γ in this model are assumed to have the values of 1,000(tonf·m), 0.1,

0.7 and 0.02, respectively. As several design codes require at least 90 percent of the modal participating mass is included in the calculation of response for each principal direction, the first mode (96% modal participating mass) and lower 10 modes (100% modal participating mass) are considered to compare the nonlinear behaviors. In using the sorting method, the near node of damaged member is taken as the sorting point. When the first mode is used, three methods give a little different result compared to the result obtained with direct step by step integration method as shown in Figure 10. However, when the lower 10 modes are included and one modal correction mode is included in substructuring method, all of three methods give good results as shown in Figure 11. Especially, the modal sorting and substructuring methods give a better accurate result than the using nonlinear modal integration method. From this example, it is found that the substructuring method with modal correction vectors can effectively applied to the locally damaged structural dynamic systems and improves the accuracy of nonlinear response.

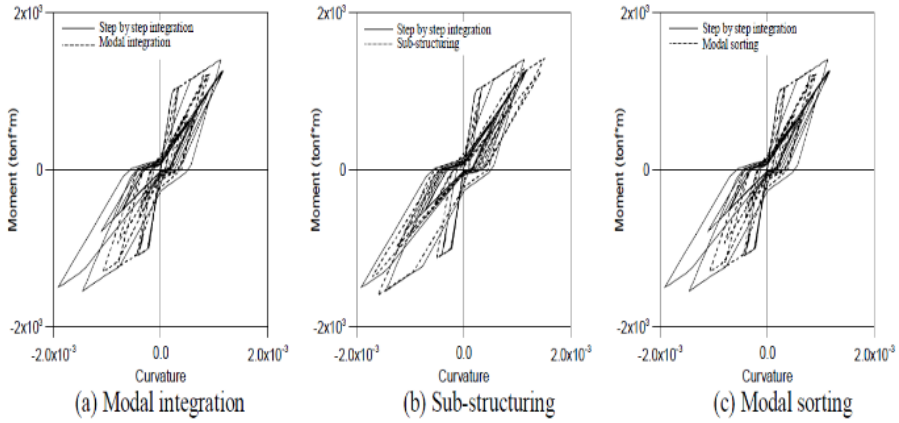


Figure 10. Moment vs. curvature with the first mode

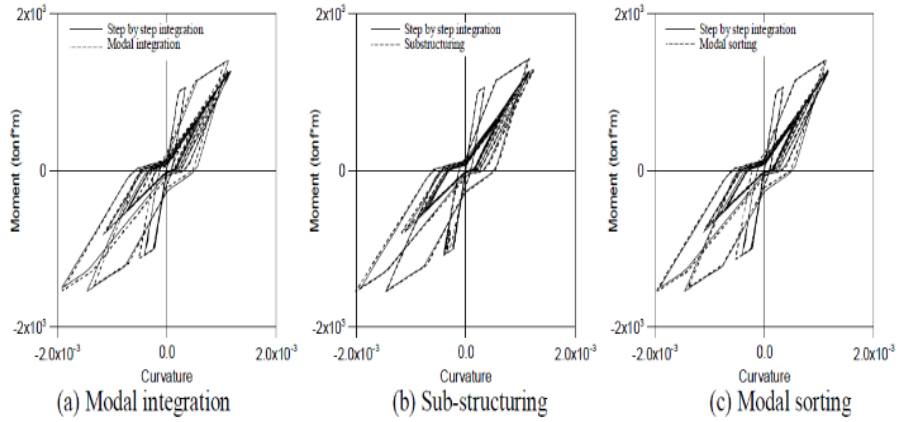


Figure 11. Moment vs. curvature with the lower 10 modes

Continuous Bridge Model

This example is a four span continuous bridge model subjected to an earthquake load. It is assumed that the deck and the pier have uniform cross-sections. The bridge structure is modeled by 3D frame elements as in Figure 12. Table 1 shows the materials properties of specimens. The bottom of the bridge pier is assumed to be damaged by a scaled El Centro earthquake (NS, PGA = 0.4g, 1940) acting in the transverse direction of

*

bridge. Figure 13 shows the displacement and time histories used for simulation: NS 1940 El Centro record and Figure 14 shows the angular velocity responses of the RPS under El Centro Earthquake.

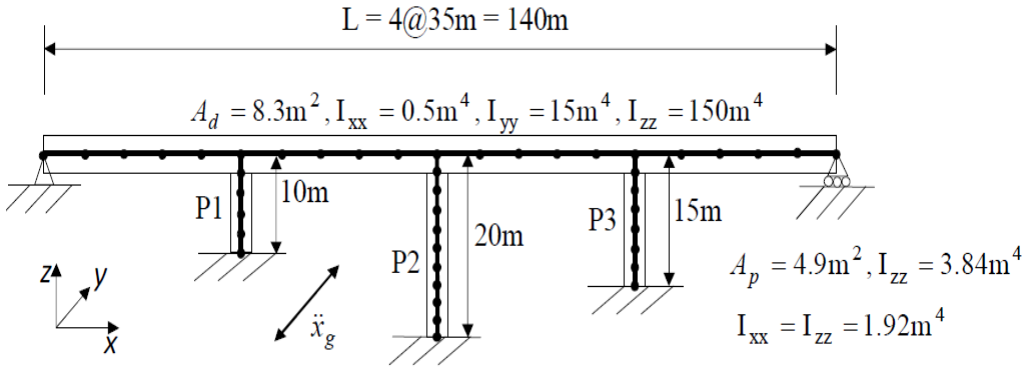


Figure 12. Continuous bridge model

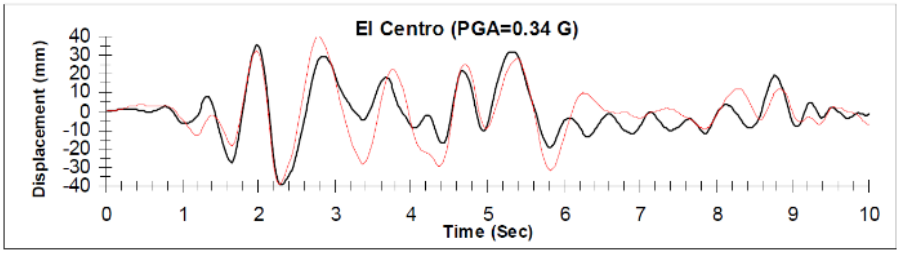


Figure 13. Displacement and time histories used for simulation: NS 1940 El Centro record.

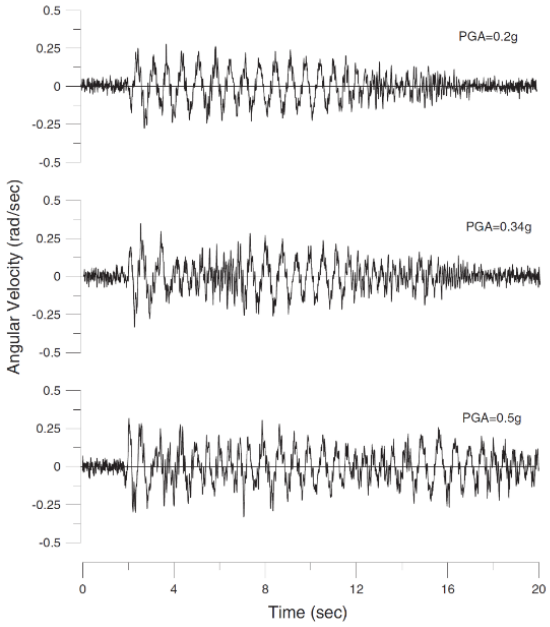


Figure 14. Angular velocity responses of the RPS under El Centro Earthquake.

Table 1. Materials properties of specimens

Concrete	**Piers**
Unit weight, kN/m^3	25
Compressive strength, MPa	27
Elastic modulus, MPa	24,648
Steel reinforcement	Yielding strength, f_y = 400 MPa

The six DOF's are assigned at each node and the total number of DOF's is 231. The nonlinear parameters M_y,

α, β and γ are assumed to have the values 1,000 (tonf·m), 0.1, 0.7 and 0.5, respectively.

The nonlinear hysteretic behaviors in pier 2 and 3 which are obtained by three nonlinear analysis methods and compared with the results obtained by the direct step by step integration method like as above simplified pier model. The fundamental natural frequency of this model is obtained as 2.56 Hz. The viscous damping ratio is assumed as 5% for each mode. At least the lower 25 modes should be included to obtain 90% of the modal participation mass for the appropriate modal analysis. The input ground acceleration is shown in Figure 15(a). Figure 15(b) and (c) are the relationships of moment vs. curvature subject assumed earthquake loading in Pier 2 and Pier 3, respectively.

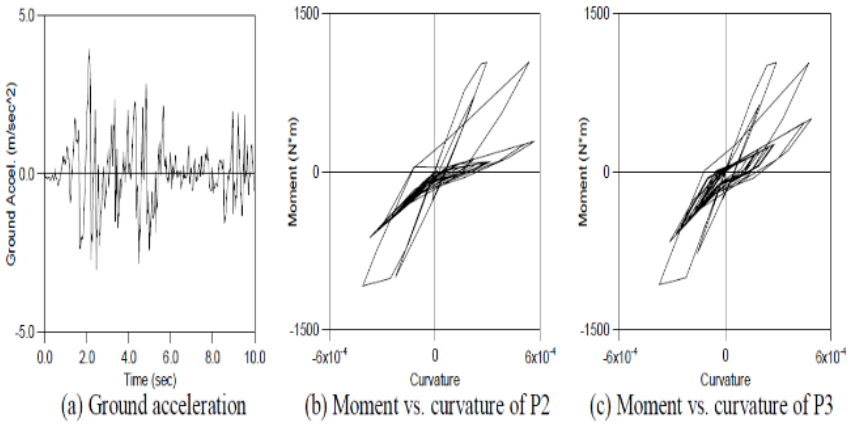


Figure 15. Ground acceleration and Moment vs. curvature of piers

In this example, one modal correction vector is included in substructuring method and the node located in the top of each pier which is assumed to be damaged is taken as the sorting point in sorting method. In the Pier 2, the modal integration method gives less accurate than the results of other two methods as shown in Figure 16. Especially, the more accurate analysis result can be obtained from the analysis using the modal sorting method compared with the other methods.

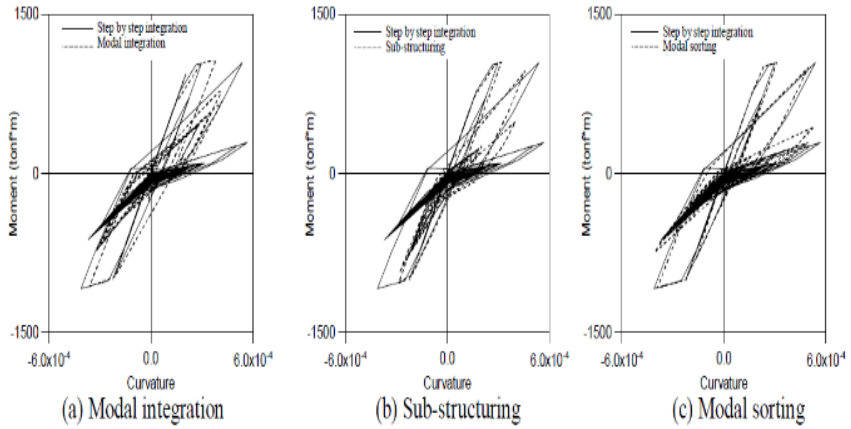


Figure 16. Moment vs. curvature of P2 with 25 modes

*

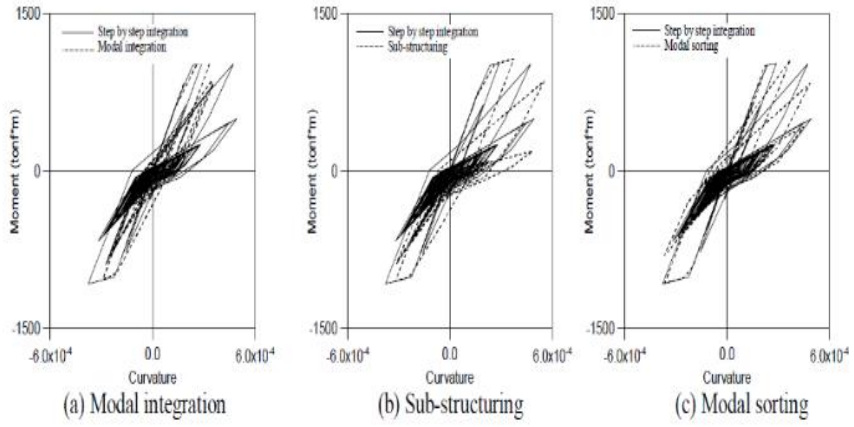


Figure 17. Moment vs. curvature of P3 with 25 modes

However, the analysis results in Pier 3 have a little difference from the result by direct step by step integration method as shown in Figure 17. This may be the result from the restraint by boundary condition and the influence of distortion of higher modes in damage area. As similar to the Pier 2, using the modal integration method also shows insufficient accuracy to describe the hysteretic behavior of locally damaged structure. In spite of somewhat discrepancies in these analysis results, however, it is even expect that the proposed modal sorting method can be used to reduce the problem size effectively and can be applied to the analysis of the locally damaged structural systems together with the substructuring method.

CONCLUSIONS

Some efficient modal methods to analyze the nonlinear hysteretic behavior of locally damaged RC structures are proposed and compared with the time integration schemes which are usually used in the analysis of nonlinear structural dynamic systems having inelastic behavior. The hysteretic model is reproduced using the modified Takeda model, in which important nonlinear characteristics of the damaged RC members, such as stiffness degradation, pinching effect and strength deterioration are included with a limited number of parameters. To verify the efficiency of proposed methods, the bridge structures are assumed to have some damages in the bottom of piers during severe earthquake and modal integration method, substructuring method and modal sorting method have applied to analyze the nonlinear hysteretic behavior and to compare with the result by Wilson θ method.

From the verification, it is found that the modal integration method has less accuracy than the other two methods and the modal sorting and substructuring methods are expected to give reasonable accuracy with limited modes in the analysis of locally damaged structural dynamic systems.

- The utilize of simple designs may generate decent estimations if the appropriate geometry is selected.
- The experimental outcomes of the total scale bridge testing, and the companion element tests, demonstrated that bridge actions is extremely reliant of the degree of displacement.
- When primarily modeling a bridge structure, there is a temptation to presume that the foundation structure is strong and stiff therefore presuming full fixity at the pile cap level. Nevertheless, the inclusion of equal soil springs and masses to be able to design soil-structure the interaction is extremely suggested.

REFERENCES

1. Banon, H., Biggs, J. M., and Irvine, H. M., (1981). Seismic damage in reinforced concrete frames. Journal of Structural Engineering, ASCE, Vol. 107, No. ST9, 1713-1729.
2. Bazant, Z. P., and Oh, B. H., (1983). Crack band theory for fracture of concrete. Materials and Structures (RILEM, Paris), Vol. 16, 155-177.
3. Chai, Y. H., Romstad, K. M., and Bird, S. M., (1995). Energy-based linear damage model for high-intensity seismic loading. Journal of Structural Engineering, Vol. 121, No. 5, 857-864.
4. Chopra, A. K., (1995). Dynamics of structures: theory and applications to earthquake engineering. Prentice Hall, New Jersey.
5. Chung, Y.S., Meyer, C. and Shinozuka, M. (1989), Modeling of Concrete Damage, ACI Structural Journal, 86(3), 259-271.
6. Comi, C., and Perego U., (2001). Fracture energy based bi-dissipative damage model for concrete. International Journal of Solids and Structures, Vol. 38, No. 36-37, 6427-6454.
7. Criesfield, M. A., (1982). Local instabilities in non-linear analysis of reinforced concrete beams and slabs. Proceedings of Institute of Civil Engineers, Part 2, Vol. 73, 135-145.
8. Crisfield, M. A., (1996). Nonlinear analysis of solids and structures, Volume 1: Essentials, Willey & Sons, New York.
9. D'Aveni, A. and Muscolino, G. (2001), Improved dynamic correction method in seismic analysis of both classically and non-classically damped structures, Earthquake Engrg. and Struct. Dynamics, 30, 501-517
10. Dikens, J.M., Nakagawa J.M., and Wittbrodt M.J. (1997), A critique of mode acceleration and modal truncation argumentation methods for modal response analysis, Computer & Structures, 62:6, 985-998
11. Fajfar, P., and Gaspersic, P., (1996). N2 method for the seismic damage analysis of RC buildings. Earthquake Engineering and Structural Dynamics, Vol. 25, No. 1, 31-46.
12. Ghobarah, A., Abou-elfath, H., and Biddah, A., (1999). Response-based damage assessment of structures. Earthquake Engineering and Structural Dynamics, Vol. 28, No.1, 79-104.
13. Hillerborg, A., Modeer, M., and Pertersson, P. E., (1976). Analysis of crack formation and crack growth in concrete by means of fracture mechanics and finite element. Cement and Concrete Research, Vol. 6, 773-782.
14. Hindi, R. A., and Sexsmith, R. G., (2001). A proposed damage model for RC bridge columns under cyclic loading. Earthquake Spectra, Vol. 17, No. 2, 261-290.
15. Hindi, R. A., and Sexsmith, R. G., (2004). Inelastic damage analysis of reinforced concrete bridge columns based on degraded monotonic energy. Journal of Bridge Engineering, ASCE, Vol. 9, No. 4, 326-332.
16. Jefferson, A. D., (1999). A multi-crack model for the finite element analysis of concrete. Proceedings of BCA Concrete Conference, 275-286.
17. Jefferson, A. D., (2002a). Local plastic surfaces for cracking and crushing in concrete. Journal of Materials: Design and Application, Vol. 216(L), 257-266.
18. Jefferson, A. D., (2003a). Craft, a plastic-damage-contact model for concrete. Part I – Model theory and thermodynamics. International Journal of Solids and Structures, Vol. 40, No. 22, 5973-5999.
19. Jefferson, A. D., (2003b). Craft, a plastic-damage-contact model for concrete. Part II – Model implementation with implicit return-mapping algorithm and consistent tangent matrix. International Journal of Solids and Structures, Vol. 40, No. 22, 6001-6022.
20. Jeong, G. D., and Iwan, W. D., (1988). The effect of earthquake duration on the damage of structures. Earthquake Engineering and Structural Dynamics, Vol. 16, No. 8, 1201-1211.
21. Jirasek, M., and Bazant, Z. P., (2002). Inelastic analysis of structures. John Willey & Son, New York.
22. Karavasilis, T. L., Seo, C.-Y., and Ricles, J. (2008). HybridFEM: A Program for Dynamic Time History Analysis of 2D Inelastic Framed Structures and Real-Time Hybrid Simulation. Bethlehem, PA.
23. Kim, T. -H., Lee, K. -M., Chung, Y. -S., and Shin, H. M., (2005). Seismic damage assessment of reinforced concrete bridge columns. Engineering Structures, Vol. 27, No. 4, 576-592.
24. Kunnath, Sashi, K.; El-Bahy, Ashraf; Taylor, Andrew; and Stone, William, Cumulative Seismic Damage of Reinforced Concrete Bridge Piers, Technical Report NCEER-97-0006, National Center for Earthquake Engineering Research, September 1997, 147 pages

*

25. Kwan, W. -P., and Billington, S., L., (2003). Unbonded posttensioned concrete bridge piers. Part II - Seismic analyses. Journal of Bridge Engineering, ASCE, Vol. 8, No. 2, 102-111.

26. Lai, S.S., Will, G.T. and Otani, S. (1984) "Model for inelastic biaxial bending of concrete members", ASCE Journal of Struct. Engrg., V.110, 11, 2563-2584.

27. Lee, K.J. and Yun, C.B. (2008), Parameter identification for nonlinear behavior of RC bridge piers using sequential modified extended Kalman filter, Smart Structures and Systems, 4:3, 319-342.

28. Ma, G., Hao, H., and Lu, Y., (2003). Modelling damage potential of high-frequency ground motions. Earthquake Engineering and Structural Dynamics, Vol. 32, No. 10, 1483-1503.

29. Meyer, B., Armijo, R., De Chabalier, J., Delacourt, C., Ruegg, J., Acache, J., Brioke, P., Papanastassiou, D., 1996. The 1995 Grevena (Northern Greece) earthquake: fault model constrained with tectonic observations and SAR interferometry. Geophys. Res. Lett. 23, 2677 – 2680.

30. Mork, K.J. (1991), "Response Analysis of Reinforced Concrete Structures under Seismic Excitation", Earthquake Engineering and Structural Dynamics, 23(1), 33-48.

31. Oliver, J., (1989). A consistent characteristic length for smeared crack models. International Journal for Numerical Methods in Engineering, Vol. 28, 461-474.

32. Panda S K and Ramachandra L S 2010 Buckling of rectangular plates with various boundary conditions loaded by non-uniform inplane loads. Int. J. Mech. Sci. 52: 819–828

33. Park, J.Y., and Ang, A.H.S., (1985). Mechanistic seismic damage model for reinforced concrete. Journal of Structural Engineering, ASCE, Vol. 111, No. 4, 722-739.

34. Popov, E.P., Bertero, V.V. and Krawinkler, H. (1972), "Cyclic behavior of three reinforced concrete flexural members with high shear", Earthquake Engrg. Research Center Report No. EERC 72-5, Univ. of California, Berkeley, Calif

35. Roufaiel, M.S.L. and Meyer, C. (1987), Analytical modeling of hysteretic behavior of R.C. Frames, J. Struct. Engrg., ASCE, 113:3, 429-443

36. Rahnama, M. and Krawinkler, H. (1993), "Effect of Soft Soils and Hysteresis Models on Seismic Design Spectra", John A. Blume Earthquake Engineering Research Center Report No. 108, Department of Civil Engineering, Stanford University.

37. Saaidi, M. And Sozen, M.A. 1979, "Simple and Complex Models for Nonlinear Seismic Response of reinforced Concrete Structures," SRS No.465, U of Illionis, Urbana.

38. Stephens, J. E., and Yao, J. T. P., (1987). Damage assessment using response measurements. Journal of Structural Engineering, Vol. 113, No. 4, 787-801.

39. Sucuoglu, H. and Erberik, A. (2004), "Energy-based Hysteresis and Damage Models for Deteriorating Systems", Earthquake Engineering and Structural Dynamics, 33(1), 69-88.

40. Takeda, T., Sozen, M. A., and Nielsen, N. N., (1970). Reinforced concrete response to simulated earthquakes. Journal of Structural Engineering, ASCE, Vol. 96, No. 12, 2557-2573.

41. Williams, M. S., and Sexsmith, R. G., (1995). Seismic damage indices for concrete structures: a state-of-the-art review. Earthquake Spectra, Vol. 11, No. 2, 319-349.

42. Williams, M. S., Villemure, I., and Sexsmith, R. G., (1997). Evaluation of seismic damage indices for concrete elements loaded in combined shear and flexure. ACI Structural Journal, Vol. 94, No. 3, 315-322.

43. Youssef, M., and Ghobarah, A., "Modelling of RC Beam-Column Joints and Structural Walls," Journal of Earthquake Engineering, V.5, No. 1, 2001, pp. 93-111.

44. Zienkiewicz, O. C., and Taylor, R. L., (1991). The finite element method. 4th edition. Vols. 1 and 2, Mc.Graw-Hill, London.

http://dergipark.gov.tr/tujes
Trakya University Journal of Engineering Sciences, 18(1): 31-41, 2017
ISSN 2147–0308
Araştırma Makalesi / Research Article

ENTROPY BASED ESTIMATION ALGORITHM USING SPLIT IMAGES TO INCREASE COMPRESSION RATIO

Emir ÖZTÜRK[1*], Altan MESUT[1]

[1] *Department of Computer Engineering, Trakya University, Edirne-TURKEY*

Abstract: Compressing image files after splitting them into certain number of parts can increase compression ratio. Acquired compression ratio can also be increased by compressing each part of the image using different algorithms, because each algorithm gives different compression ratios on different complexity values. In this study, statistical compression results and measured complexity values of split images are obtained, and an estimation algorithm based on these results is presented. Our algorithm splits images into 16 parts, compresses each part with different algorithm and joins the images after compression. Compression results show that using our estimation algorithm acquires higher compression ratios over whole image compression techniques with ratio of 5% on average and 25% on maximum.

Keywords: Estimation algorithm; image compression; image processing; image complexity

SIKIŞTIRMA ORANINI ARTTIRMAK İÇİN BÖLÜNMÜŞ RESİMLERİ KULLANAN ENTROPİ TABANLI BIR TAHMİN ALGORİTMASI

Özet: Resim dosyalarını belirli sayıda parçalara böldükten sonra sıkıştırma işlemi yapmak sıkıştırma oranını arttırabilmektedir. Elde edilen sıkıştırma oranı resmin her parçasının farklı bir algoritmayla sıkıştırılması ile daha da fazla arttırılabilmektedir. Her algoritma farklı karmaşıklık değerlerinde farklı sıkıştırma oranı sağlamaktadır. Bu çalışmada bölünmüş resimlerden sıkıştırma sonuçları istatistikleri ve ölçülen karmaşıklık değerleri elde edilmiş ve bu sonuçları kullanan bir tahmin algoritması önerilmiştir. Algoritmamız resimleri 16 parçaya böler, her parçayı farklı bir algoritmayla sıkıştırır ve bu parçaları en son aşamada birleştirir. Sıkıştırma sonuçlarından görüldüğü üzere algoritmamız resmi tek parça halinde sıkıştırma işlemine göre ortalama %5 ve maksimum %25 daha iyi sıkıştırma performansı sağlamıştır.

Anahtar Kelimeler: Tahmin algoritması; Görüntü sıkıştırma; Görüntü işleme; Görüntü karmaşıklığı

INTRODUCTION

With the evolution of digital photography and cameras, the amount and resolution of photos are increasing gradually. Therefore, there is a storage problem for large amount of images with high resolution. To reduce the size of the photos, lossless or lossy image compression methods can be used. JPEG (CCITT Rec, 1992), JPEG2000 (ISO/IEC 15444-1, 2004; Christopoulos et al., 2000), JPEG XR (ITU-T Rec, 2009) and PNG (ISO/IEC 15948:2004, 2004) can be given as examples to these methods.

JPEG, which is widely used since 1992, gains compression by eliminating high frequency values using DCT (discrete cosine transform) (Ahmed et al., 1974). However, using JPEG with high compression ratios results in blocking effect because of DCT. JPEG2000, which uses DWT (discrete wavelet transform) (Mallat, 1989) instead of DCT, provides better image quality. However, its slower encoding process limits its usage. Because slow encoders are not suitable especially for digital cameras, embedded systems, smartphones and other types of devices that have powerless processors. JPEG XR is proposed in 2009 as an alternative to JPEG2000. JPEG XR uses PCT with integer values with the help of Hadamard matrices. With an additional process, blocking effect could also be reduced.

General purpose lossless data compression algorithms like DEFLATE, LZMA, PPMd or Bzip2 can also be used to compress images. PNG is a lossless still image compression algorithm which is based on DEFLATE. Although lossless compression is not efficient for compressing photographs, it will be better to use a lossless method when compressing low complex images like diagrams, logos, etc.

Our previous work show that, compression ratio can be increased by splitting image into several parts and compressing these parts with the same algorithm individually (Öztürk, 2012). Using different compression algorithms on each part can also increase compression ratio.

In this study, statistical results from image properties are obtained by splitting image files into certain parts. Gain on compression ratio by compressing each part with different algorithm is examined. Finally, an estimation algorithm based on acquired statistical results is developed and performance of the estimation algorithm is measured. In second section, common algorithms used for getting statistical results are given. In third section, statistical method to obtain results is proposed. In fourth section an estimation algorithm is proposed and results of the algorithm is presented. Last section contains conclusions about developed estimation algorithm.

COMMON COMPRESSION ALGORITHMS USED FOR STATISTICAL ANALYSIS

LZMA (LZ77)

LZ77 is a dictionary based compression algorithm which was developed by Abraham Lempel and Jakob Ziv (Lempel and Ziv, 1977). The algorithm works by keeping a history window (known as: sliding window) of the most recently seen data and comparing the current data being encoded with the data in this window. If a matching repeated sequence is found, a reference to the position in the sliding window and the length of the match is encoded. The size of sliding window affects the compression ratio. LZSS is a slightly modified version of LZ77 that provides better compression ratio (Storer and Szymanski, 1982)

The Lempel–Ziv–Markov chain algorithm (LZMA) uses a dictionary compression scheme which is similar to the LZ77 algorithm. However, LZMA uses stream of bits which is encoded using an adaptive binary range coder instead of a generic byte-based model. Implementation of this model is as simple as byte-based model and it gives much better compression ratio. LZMA2 is a simple container format that can include both uncompressed data and LZMA data. LZMA2

supports arbitrarily scalable multithreaded compression and decompression and efficient compression of data which is partially incompressible (Wikipedia, 2017).

DEFLATE & PNG

DEFLATE is a lossless compression algorithm, which was developed by Phil Katz in mid 90's (Deutsch, 1996). The compressed data is considered as set of blocks. Each block is compressed with using LZSS along with Huffman encoding. Huffman tree for each block is independent from previous and next block. Size of the compressible blocks are variable. If the encoder decided that Huffman tree is too big to encode data efficiently, the current block will be ended and a new block will be created. Huffman trees are added to encoded blocks before compressed data and these trees are also encoded with Huffman encoding. To obtain efficient compression ratio, minimum 3 repeated characters will be encoded. 256 different repetition count between 3 and 258 could be represented with one byte. Search buffer which is 32.768 bytes long will be represented with 15 bits and 1 bit is used for uncompressed data flag. If a repetition does not found in sliding window, actual byte values will be encoded with the same Huffman tree. However, the distance information will be encoded with a different Huffman tree (Feldspar, 2011; RFC 1951, 1951).

PNG (Portable Network Graphics) is a lossless image compression method that is based on DEFLATE (…). While GIF format is limited to 8-bit indexed color (256 color), PNG gives a much wider range of color depths and supports alpha channel transparency. Although PNG does not support animation intrinsically like GIF, it is now the most widely used lossless image compression method on the Internet (Gelbmann, 2013).

PPMd (PPM)

PPM (Prediction by Partial Matching) algorithm was published in 1984 by Cleary and Witten (Cleary and Witten, 1984). It tries to predict the next character using some previous encoded characters. In 90s, different variations of PPM showed up. The most used version of PPM was developed by Dmitry Shkarin and known as PPMd (Shkarin, 2002).

Based on the *n*-grams obtained from the previously encoded part of the input being compressed, the probability distributions of all the characters following these *n*-grams are stored. Although these probability distributions are compressed with Huffman or Arithmetic encoder, if $n > 5$ the required memory size will be too large. Generally arithmetic coding is preferred because possibility range could be very wide. If no prediction can be made based on previously encoded n symbols (the currently encoded symbol is not found in the n^{th} context), the algorithm encodes the probability of an escape character and search the symbol in $(n-1)^{th}$ context. This process is repeated until a match is found. If no more symbols remain in context a fixed prediction is made.

Different approaches have been developed to determine the probability of the escape character. PPMd is one of them, which increments the count of the escape character every time it is used. In other words, PPMd estimates the probability of a new symbol as the ratio of the number of unique symbols to the total number of symbols observed.

Although PPM-based compressors often have a high compression ratio, they cannot be used to speed up network traffic due to their slow compression and decompression times.

Bzip2 (BWCA & BWT)

Bzip2 is a free and open-source file compression utility that uses the BWT (Burrows–Wheeler Transform). Although it has a lower compression ratio than PPM-based algorithms, it is widely used because it can perform faster compression and decompression.

BWT (Burrows and Wheeler, 1994) is a block sorting method which rearranges a character string into runs of similar characters. Generally, another transform like MTF (Move-To-Front coding) is used after BWT. BWT and MTF do not acquire compression but

transform data into appropriate form to increase compression ratio of Huffman or Arithmetic encoding. Algorithms based on BWT which are developed lately use different transform techniques to increase compression ratio.

JPEG

JPEG is the most widely used still image compression standard since it was developed by Joint Photographic Experts Group in 1992. Proposed standard defines the compression and decompression stages but not the file format. JPEG is a lossy compression algorithm and the amount of compression could be specified using a quality factor. Lower quality factors provide higher compression ratios and lower image quality.

Compression stages of JPEG is as follows: Color space transformation, chroma subsampling, segmentation, discrete cosine transform, quantization, zig-zag scanning, run length encoding and entropy encoding.

Color space transformation from RGB to YCbCr must be done before downsampling. Downsampling will reduce the chrominance values (Cb and Cr) by averaging four neighboring pixels and storing only one (or two) value for each four pixels. This loss of information is not important since the eye is less sensitive to fine color details than to fine brightness details. After that, the image is split into blocks of 8×8 pixels and each block is transformed into frequency domain using DCT. According to the selected quality factor in the quantization stage, high-frequency components are stored with a lower accuracy than the low-frequency components. Each block is scanned in a zigzag order to create an appropriate entry for run-length encoding (RLE). In the last stage that is entropy encoding, Huffman or Arithmetic coding is used.

JPEG2000

JPEG2000 is another still image compression standard that was developed to overcome some of the disadvantages of JPEG and to achieve high quality images at high compression ratios. As we have mentioned before, it is a wavelet-based method. With using DWT, there will be blurring in the image at high compression ratios instead of blocking effect seen in JPEG compressed images. Compression stages in JPEG2000 can be simplified as follows: Color space transformation, segmentation (tiling), DWT, quantization, MQ encoding.

JPEG2000 has some additional features different from JPEG, like;

- Color space transformation can be done with Reversible Color Transform (RCT) that does not cause quantization errors (because it uses integers instead of floating point numbers).
- It can also perform lossless compression in the same architecture.
- The desired compression ratio can be given before compression. If the encoder predicts that it can compress the image to the specified size or smaller with lossless mode, it will use this mode.
- With the help of ROI (Reigon of Interest), partitions with important data could be compressed with high quality and other parts could be compressed with low quality.
- It supports alpha channel for transparency.
- It supports progressive transmission and multiple resolution representation with the help of its subband coding structure.
- It supports HDR (High Dynamic Range) by using floating point values for pixels.

JPEG XR

JPEG XR (JPEG extended range) is a newer standard and file format for photographic images based on Windows Media Photo (HD Photo). Its purpose is to obtain the speed of JPEG and quality of JPEG2000. If you want to compress an image that uses 16 bits for each channel with JPEG, each channel will lose 8 bits of information because JPEG can only use 8 bits per channel. JPEG XR is developed to support extended information for each channel (it supports bit depths of

up to 32 bits). With the support of extended information, JPEG XR is optimal for compressing high resolution and HDR images.

Coding stages of JPEG XR are similar to JPEG's: Color space transformation, chroma subsampling, segmentation, prefiltering, Photo Core Transform (PCT), quantization, estimation of coefficients and entropy encoding.

Some of the differences between JPEG and JPEG XR are:

- JPEG XR uses lossless color space transformation instead of lossy one in JPEG.
- JPEG XR uses 4 × 4 blocks instead of 8 × 8 (these blocks are grouped into 16 × 16 macroblocks).
- JPEG XR has an optional prefiltering step: Photo Overlap Transform (POT).
- JPEG XR uses PCT, which is a kind of 4 × 4 lossless DCT.
- Entropy coding in JPEG XR is more complex.
- JPEG XR supports lossless compression (like JPEG2000).

STATISTICAL METHOD TO ACQUIRE IMAGE PROPERTIES

Images can have different complexity in their different parts. After splitting image into parts, each part can be processed individually. Using the same algorithm with whole image and partitioned image can have different compression ratios. If each part is compressed with different algorithms, higher compression ratios can be obtained. Because, known compression algorithms will give different compression results on different complexity values (Öztürk and Mesut, 2016). PNG and general lossless compression algorithms obtain high compression ratio especially on low complexity images. Lossless modes of image compression algorithms i.e. JPEG2000 and JPEG XR obtain high compression ratio on high complexity images. For example, in a scanned document, the parts that contain photographs will have more complexity than the other parts that contain texts. Therefore, if we use a known general purpose lossless compression algorithm on low complexity parts instead of compressing them with JPEG2000 or JPEG XR, total compression ratio will be increased.

To obtain statistical results, 24bpp bitmap files were split into 4 and 16 equal parts. After that, 9 different compression algorithms (Deflate, Deflate64, LZMA, LZMA2, PPMd, Bzip2, JPEG2000, JPEG XR and PNG) are used on original image, 4 and 16 parts of the image. After splitting operation, compression ratios over 21 images are obtained. Different complexity values like entropy, different color count, quadrilateral square count are also obtained from original image and each part of the image. We developed an application for obtaining these results. Developed application is shown in Figure 1.

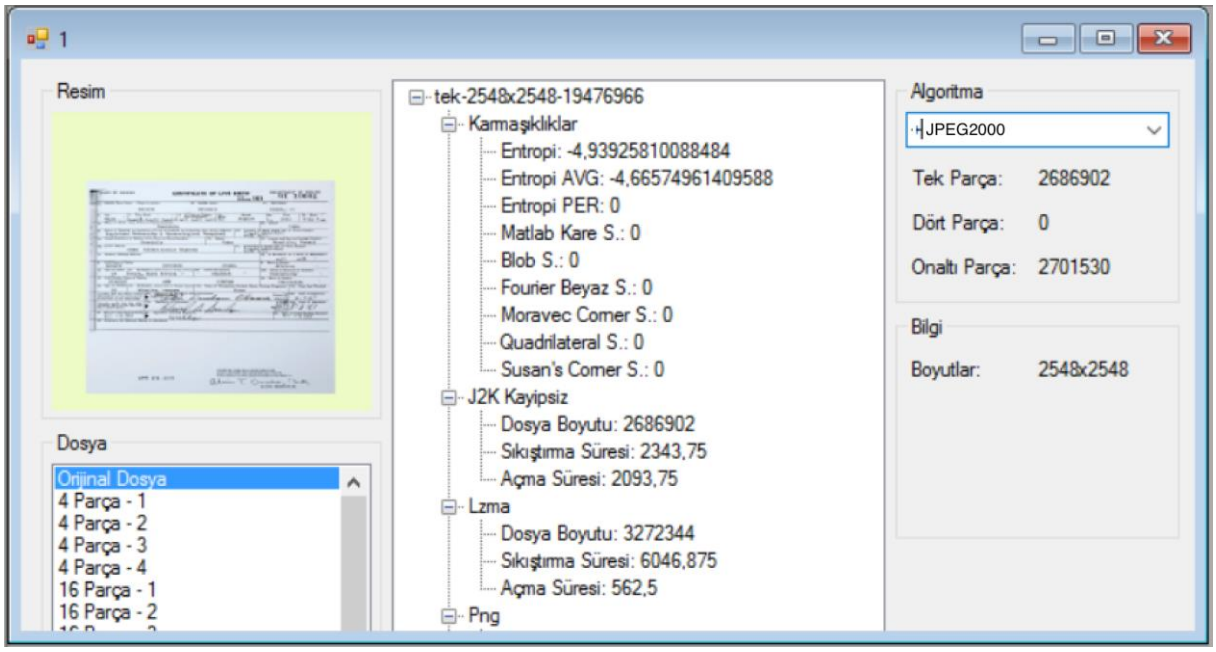


Figure 1. Application for Obtaining Image Properties

As seen in Figure 1, application allows selecting the whole image or its parts. Selected image or a part of it is shown on upper left. After selecting one of the images, main pane will show acquired complexity values and compression ratio of each known lossless compression algorithm. Compression results of the algorithms on whole image and split images could be shown for requested algorithm on the right.

Entropy is calculated on grayscale form of given image. Different color count is obtained for each color channel of the image and average of these values is used. Quadrilateral square count is calculated with splitting image until split part is under a given threshold value. Given image will be split into 4 equal parts and an integrity value for each part is calculated. If calculated integrity of the part is above the threshold value, the part will be split into 4 equal parts again.

Entropy value is directly proportional with complexity (entropy increases with increasing complexity). Analyzing complexity measures show that entropy is the most reliable criterion for complexity. Because of this, only entropy is selected for complexity measurement.

Comparing the compression results of 4 parts and 16 parts of images shows that dividing images into 16 parts gives better results than 4 parts. Therefore, splitting image into 16 parts is selected for proposed estimation algorithm.

The steps of statistical method based on acquired knowledge are given in Figure 2. As seen in Figure 2, the entropy value of whole image and parts of the image are acquired for complexity measurement.

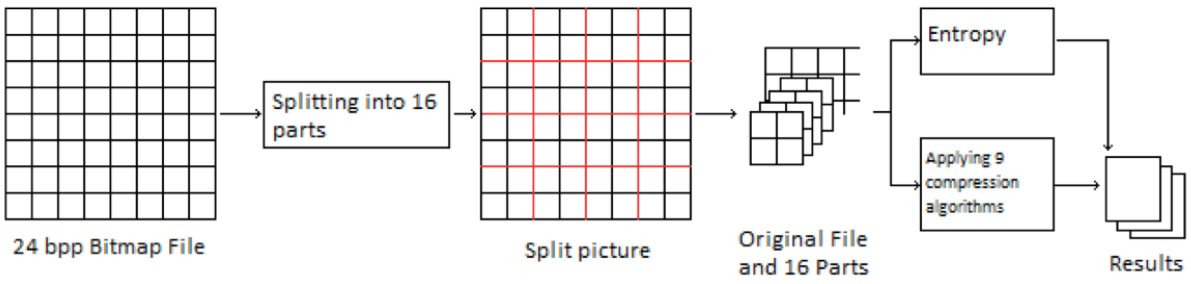


Figure 2. Steps of Obtaining Image Properties

ESTIMATION ALGORITHM

Using obtained statistical data, it can be identified which algorithm gives the most efficient results with given entropy value. Therefore, an estimation could be made to select which algorithm is suitable for compression without compressing the given part.

After analyzing the entropy values of given images, 2 algorithms out of 9 gives correlated results with entropy. Therefore, these 2 algorithms are selected for estimation to obtain proper results. Selected algorithms are LZMA and JPEG2000.

To obtain results for estimation, a corpus consists of 30 images larger than 2MP and 16 parts of these images (510 images in total) is used. Most of these images are scanned documents that have blank spaces, writings and pictures to show compression ratio of different algorithms on different level of complexity.

Figure 3 shows which algorithm is acquired best compression ratio over given entropy value. As seen in Figure 3, LZMA gives better results between 0.25 and 4.25 and JPEG2000 gives better results between 4.25 and 7.75. Especially when the entropy value is larger than 6, JPEG2000 gives better results on all images. Based on these results, an estimation algorithm could be proposed.

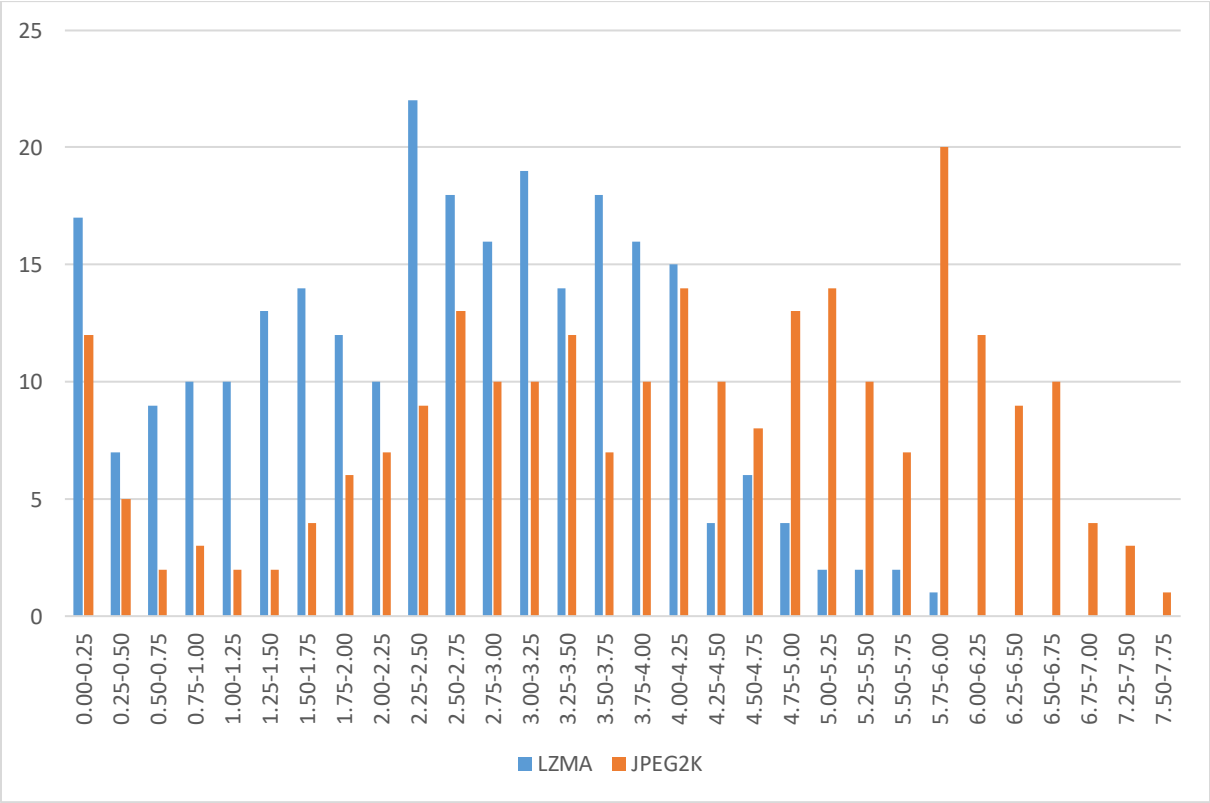


Figure 3. Best Compression Ratio Results at Given Entropy Values

Steps of the estimation algorithm are given in Figure 4. The algorithm splits given image into 16 parts. For each part, the algorithm first calculates the entropy value. Based on entropy value, the algorithm will choose a lossless compression algorithm and compresses that part with that algorithm. After compressing 16 parts with selected algorithms, the image will be joined.

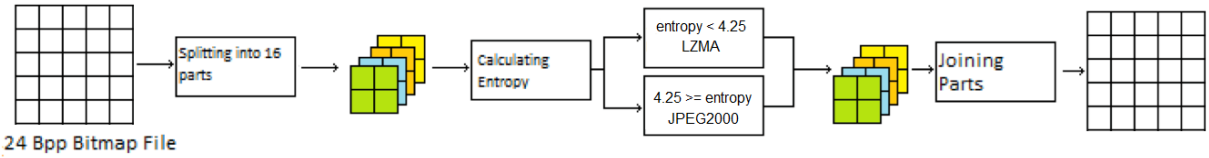


Figure 4. Steps of the Estimation Algorithm

An example of splitting operation is given in Figure 5. After splitting image into 16 parts, each part is compressed with most efficient compression algorithm. As seen on sample image, 6 parts are compressed with LZMA. Other 10 parts are compressed with JPEG2000. LZMA mostly gives better results on white spaces. JPEG2000 gives best results on parts with images or writings. Total size of the split image is smaller than compressing whole file with JPEG2000 or LZMA.

Figure 5. Splitting Operation of Sample Image

Compression ratios of our estimation algorithm and the best compression algorithm on whole image for 30 test images are given in Figure 6. Our estimation algorithm gives better results than compressing whole images with JPEG2000 or LZMA except 28th and 29th images. Figure 7 shows compression gain of our estimation algorithm over whole image compression with the best algorithm. Most of these images acquired gain with using our estimation algorithm. Best gain is obtained on 23rd image file with the ratio of 24.24%.

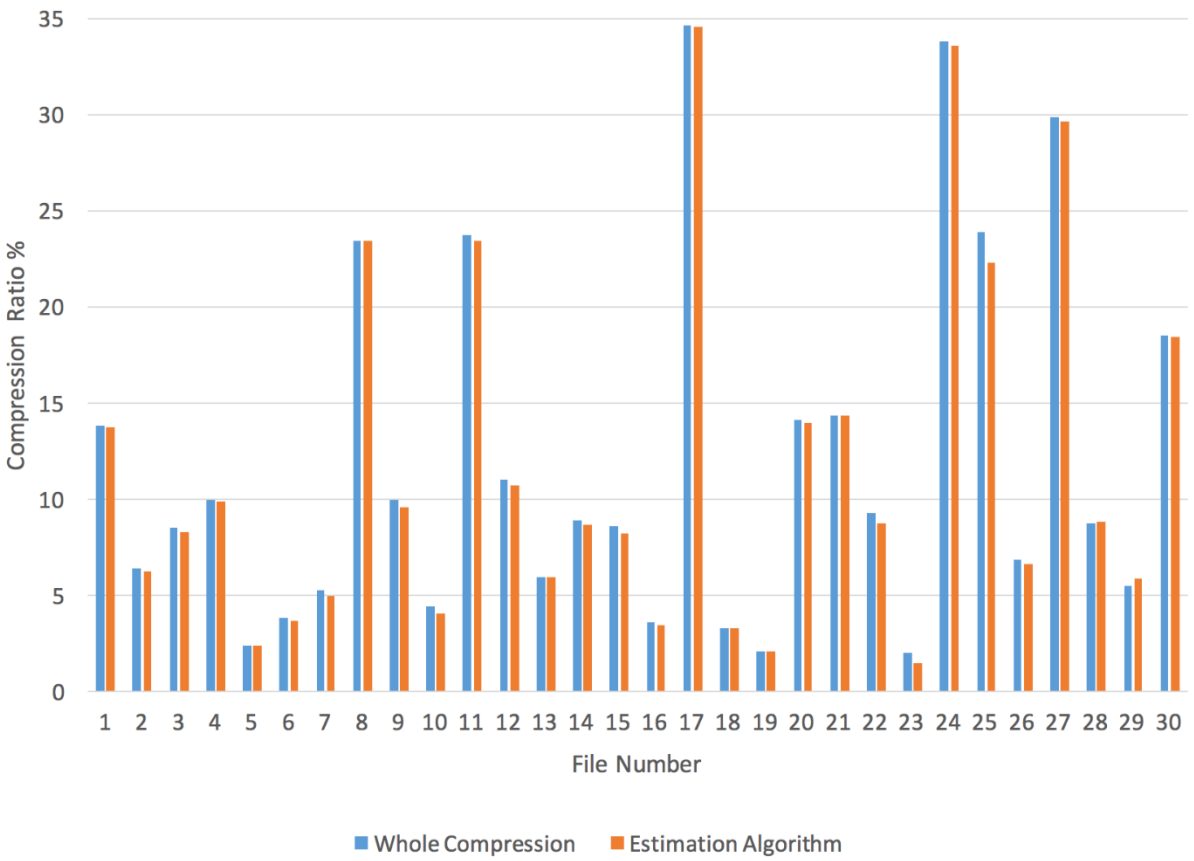


Figure 6. Compression Ratios of 30 Images

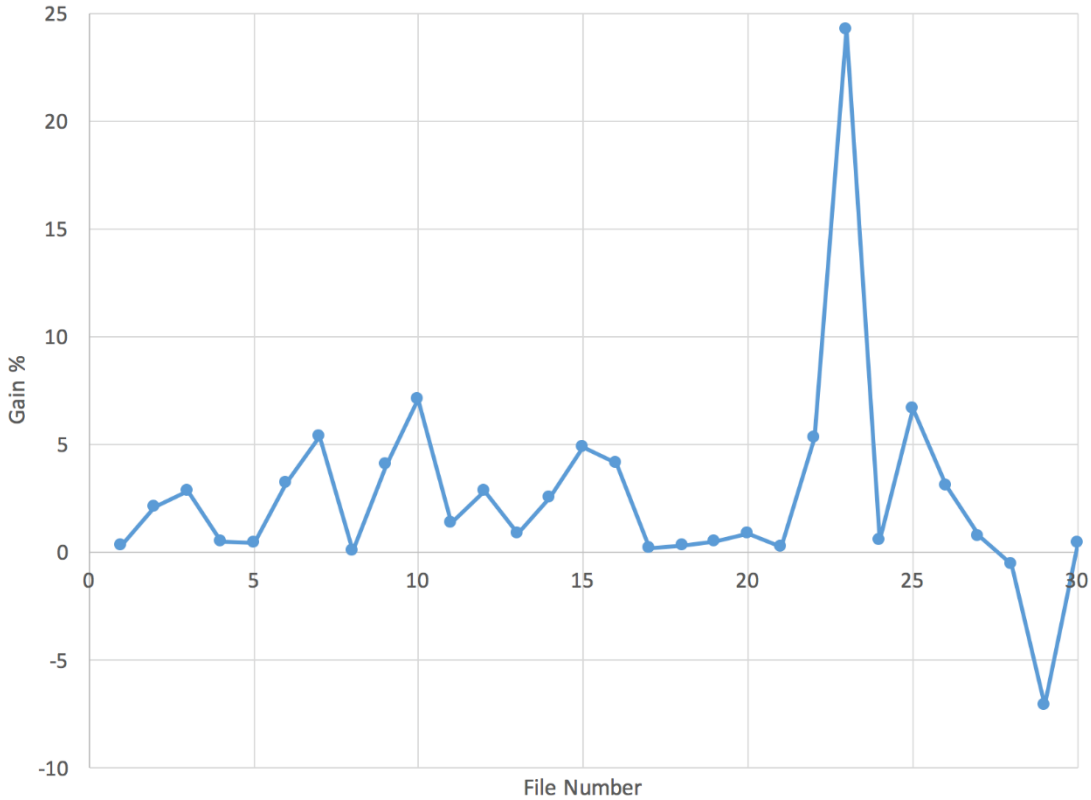


Figure 7. Obtained Compression Ratio Gain Over The Best Compression Algorithm

CONCLUSIONS

Splitting image into several parts is effective for increasing compression ratio. Besides, entropy is a decisive property for choosing the compression algorithm with best compression ratio. Within 9 algorithms, only two algorithms give stable results with the change of entropy. JPEG2000 is efficient mostly on images with high complexity and LZMA is efficient on low complexity images.

Although the gain obtained is small, gain will grow with image resolution. Success rate of the estimation algorithm is based on the amount and quality of statistical data. With the increase of amount and variety of data, algorithm will give more accurate results for different situations. Performance of estimation algorithm is also based on used known algorithms like JPEG2000 or LZMA.

With discovering different complexity methods, eliminated 7 algorithms could be also used in estimation algorithm. Using these algorithms with different situations could produce more efficient compression ratios.

An algorithm with lossy image compression algorithms could also be developed. When a user wants to specify the file size or amount of loss before compression, the algorithm could select proper lossy or lossless algorithm with right compression parameters to obtain desired result.

REFERENCES

1. CCITT Rec. T.81, (ISO/IEC 10918-1, 1994), Digital Compression and Coding of Continuous-Tone Still Images – Requirements And Guidelines (JPEG), 1992.
2. ISO/IEC 15444-1, JPEG 2000 image coding system: Core coding system. 2004.
3. CHRISTOPOULOS C, SKODRAS A, EBRAHIMI T. The JPEG2000 still image coding system: An Overview. *IEEE Transactions on Consumer Electronics*, 46(4), 1103-1127, 2000.
4. ITU-T Rec. T.832, (ISO/IEC 29199-2, 2010), JPEG XR image coding system: Image coding specification. 2009.
5. ISO/IEC 15948:2004, Information technology -- Computer graphics and image processing -- Portable Network Graphics (PNG): Functional specification, 2004.
6. AHMED N, NATARAJAN T, RAO KR. Discrete Cosine Transform. *IEEE Transactions on Computers*, 23(1): 90-93, 1974.
7. MALLAT S. A Theory for Multiresolution Signal Decomposition: The Wavelet Representation. *IEEE Pattern Analysis and Machine Intelligence*. 11(7), 674-693, 1989.
8. DEUTSCH LP. DEFLATE Compressed Data Format Specification version 1.3. *IETF Network Working Group, Request for Comments 1951*, 1996.
9. CLEARY J, WITTEN I. Data Compression Using Adaptive Coding and Partial String Matching, *IEEE Transactions on Communications*. 32 (4): 396–402, 1984.
10. SHKARIN D. PPM: One Step to Practicality, *Proceedings of IEEE Data Compression Conference*. 202-211, 2002, Utah, USA.
11. BURROWS M, WHEELER DJ. A block sorting lossless data compression algorithm, *Technical Report 124, Digital Equipment Corporation*. 1994.
12. ÖZTÜRK E. Transformation and Segmentation Operations on Images for Increasing the Effectiveness of Compression Methods, *MSc Thesis, Trakya University*, 2012.
13. FELDSPAR A. An explanation of the deflate algorithm. http://www.zlib.net/feldspar.html. Retrieved 2017-02-13.
14. ÖZTÜRK E, MESUT A. Finding the Optimal Lossless Compression Method for Images Using Machine Learning Algorithms, International Scientific Conference UNITECH'16, II,345-348 Gabrovo-Bulgaria, 2016.
15. ZIV J, LEMPEL A. A Universal Algorithm for Sequential Data Compression. IEEE Transactions on Information Theory, Vol. 23, 1977, pp. 337-343.
16. ZIV J, LEMPEL A. Compression of Individual Sequences via Variable-Rate Coding. IEEE Transactions on Information Theory, Vol. 24, 1978, pp. 530-536.
17. WELCH TA. A Technique for High-Performance Data Compression. IEEE Computer, Vol. 17, 1984, No. 6, pp. 8-19.
18. STORER JA, Szymanski TG. Data compression via textual substitution. Journal of the ACM, Vol. 29, 1982, pp. 928-951.

19. Wikipedia. Lempel–Ziv–Markov chain algorithm. http://en.wikipedia.org/wiki/LZMA. Retrieved 2017-02-13.

20. Gelbmann M. The PNG image file format is now more popular than GIF. *W3Techs. Q-Success*. 2013-01-31.

http://dergipark.gov.tr/tujes
Trakya University Journal of Engineering Sciences, 18(1): 43-52, 2017
ISSN 2147–0308
Araştırma Makalesi / Research Article

MOBİL CİHAZLARDA RSA ALGORİTMASININ PERFORMANS OPTİMİZASYONU

Tarık YERLİKAYA[1*], Hakan GENÇOĞLU[2]

[1] *Trakya Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümü, Edirne*

[2] *İstanbul Aydın Üniversitesi Fen Edebiyat Fakültesi Matematik-Bilgisayar Bölümü, İstanbul*

Özet: Asimetrik şifreleme algoritmaları, simetrik algoritmalara göre çok yavaş çalışırlar. Fakat anahtar dağıtım problemleri yoktur. Optimize edilmedikleri sürece fazla sayıda işlem yaparak şifreleme işlemini gerçekleştirirler. Ayrıca, örneğin RSA algoritması, tatmin edici bir güvenlik için, çok büyük asal sayılar kullanarak şifreleme yapar. Bu durum da donanım için ekstra işlem yükü demektir. Genel kullanımda asimetrik algoritmalar küçük veri paketlerini şifrelemek için kullanılır. Bu çalışmamızda mobil cihazlar üzerinde RSA algoritmasının çalışması test edilmiştir. Mobil cihazların kısıtları göz önüne alınarak RSA algoritması optimize edilmiş ve algoritmanın hızlı çalışması sağlanmıştır.

Anahtar Kelimeler: Mobil iletişim; RSA; Mobil RSA; Mobil Veri Güvenliği; Biginteger

OPTIMIZATION OF PERFORMANCE OF THE RSA ALGORITHM ON MOBİLE DEVICES

Abstract: Asymmetric encryption algorithms encrypt data very slowly according to symmetric encryption algorithms but there is no key distrubiton problem in asymmetric algorithms. Asymmetric algorithms make a lot of process to encrypt the data unless they are optimized. Besides RSA algorithm uses very big prime numbers for satisfactory security and it means extra process for the hardware. Asymmetric algorithms is usullay used for encryption of very small data packets. In this study we tested the performance of RSA algorithm on mobile devices. Considering boundaries of mobil devices we optimised the RSA algorithm, and fast operation of the algorithm was provided.

Keywords: Mobile communications; RSA; Mobile RSA; Mobile Data Security; Biginteger

[*]Corresponding Author: Tarık YERLİKAYA
e-mail: tarikyer@trakya.edu.tr

GİRİŞ

Teknolojinin gelişmesi, internetin yaygınlaşması, mobil cihazlar ve bilgisayarların hayatımızda vazgeçilemez bir hal almaya başlamasıyla veri güvenliği önem kazanmıştır. Veri güvenliği artık iletişim güvenliği olarak anılmaya başlanmıştır. Bulut teknolojisi platform bağımsız ve kesintisiz iletişimin gerçekleşmesini sağlar. Bununla birlikte verilerimizin herkese açık güvensiz internet ortamında bulunması gerekmektedir. Özel bilgilerimizin herkese açık ortamlarda korunabilmesi için şifreleme tekniklerinden yararlanılabilir. Veriler internet ortamına girmeden önce mobil cihazlar veya bilgisayarlarda şifrelenerek internete verilirse, verileri ele geçirmeye çalışan üçüncü şahıslar için anlamsız veri katarları haline gelecektir.

Kısıtlı kaynakları dolayısıyla mobil cihazlarda şifreleme algoritmalarının doğru bir şekilde kullanılması gerekir. Matematik tabanlı asimetrik şifreleme algoritmalarının içerdiği çözülmesi zor problemler çok fazla işlem ve kaynak gerektirmektedir. Bu algoritmaların mobil cihazlarda kullanılabilmesi için optimize edilmeleri gerekir. Bu çalışmamızda RSA algoritmasının içerdiği üs alma işlemi optimize edilerek mobil cihazlardaki performansı ölçülmüştür. Üs alma işlemi için İkili üs alma (Binary Method), çok büyük asal sayıların depolanabilmesi ve işlemleri için BigInteger sınıfı kullanılmış Windows platformunu içeren masaüstü pcler ile Android platformunu içeren tabletlere yönelik yazılan uygulamalar ile performans testi gerçekleştirilmiştir.

ÖNCEKİ ÇALIŞMALAR

Mobil cihazlarda şifreleme ve veri iletimi üzerine farklı çalışmalar yapılmıştır. “Bluetooth üzerinden güvenli veri iletimi” isimli çalışmada küçük boyutlu verilerin akıllı olmayan mobil cihazlarda bluetooth üzerinden gönderilmesi simetrik algoritma kullanılarak yapılmıştır. [1] Başka bir çalışmada simetrik yapıda bir algoritma düşünülerek bu algoritma için akıllı telefonlara yönelik uygulama yazılmış ve analizi yapılmıştır.[2]

Çalışmamız gücü kanıtlanmış olan yüksek işlem gücü gerektiren RSA algoritmasının optimizasyon sonrasındaki performansını ölçecektir.

ŞİFRELEME ALGORİTMALARI

Simetrik Şifreleme Algoritmaları

Simetrik şifreleme algoritmaları şifreleme ve şifre çözme işlemleri için aynı anahtarı kullanır. Dolayısıyla anahtar gizli olmak zorundadır. Algoritma ne kadar güçlü olursa olsun anahtar bilindiği takdirde şifreli metin hemen çözülebilir. İki tür simetrik algoritmadan söz edilebilir.

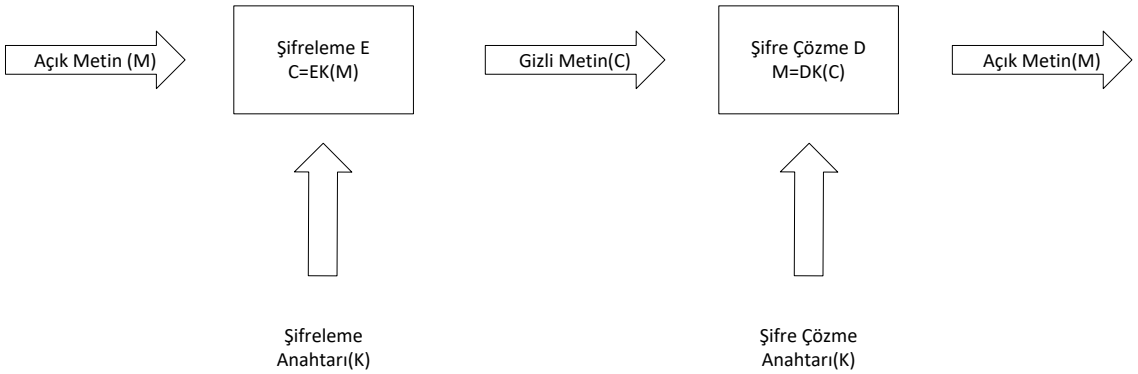
- Blok şifreleme algoritmaları
- Akış şifreleme algoritmaları

Blok şifreler yaygın olarak Feistel Ağı veya Substitution-Permutation Ağı nı kullanır. Feistel mimarisine örnek olarak DES verilebilir, AES-Rijndael algoritması da Sustituon-Permutation Ağı nı kullanır.

Hangi ağı kullanırlarsa kullansınlar simetrik algoritmalar asimetrik algoritmalara göre çok hızlıdırlar. Basit yer değiştirme, xor lama, öteleme gibi işlemlerden oluşurlar.

Akış şifreler ise veri uzunluğuna eşit veya büyük, periyodik olmayan (Bir bölümü kullanılarak anahtarın tahmin edilemeyeceği), rastgele üretilmiş tek kullanımlık anahtarlar ile verinin işleme sokulması ile şifrelenirler. Buradaki en büyük problem tek kullanımlık tamamen rastgele üretilmiş tek kullanımlık anahtarı üretmektir.

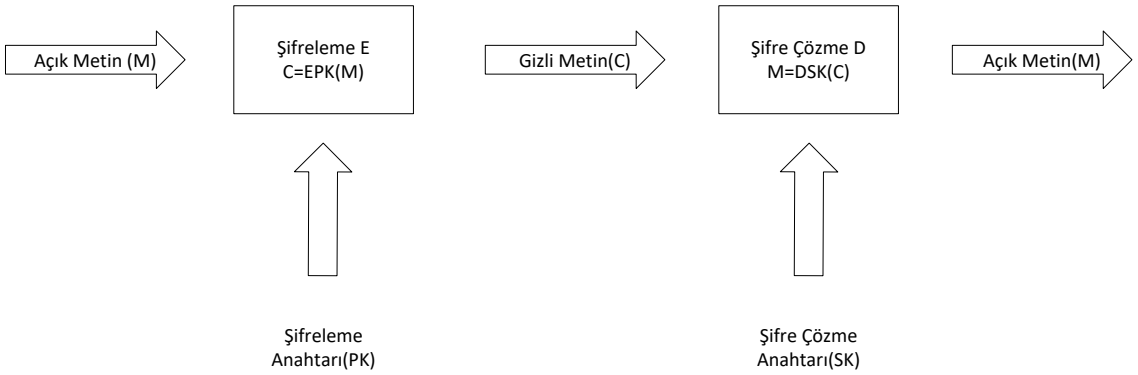
Bu performanslarına rağmen şifreleme ve şifre çözme işlemleri için tek anahtar kullanmaları bu anahtarı alıcıya iletme işleminde büyük problem doğurur. Simetrik algoritmaların bu problemi farklı yöntemlerle çözülmeye çalışılmıştır.



Şekil 1. Simetrik Algoritma Şifreleme – Şifre Çözme Süreci

Asimetrik Şifreleme Algoritmaları

Asimetrik şifreleme algoritmalarında şifreleme için ayrı, şifre çözme için ayrı anahtar kullanılır. Şifreleme için kullanılan anahtar açıktır ve herkes tarafından bilinebilir. Şifre çözmek için kullanılan anahtar sadece şifreli metni çözecek olan alıcı tarafından bilinmelidir ve gizlidir. Bu iki anahtar matematiksel olarak birbirine bağlı olmakla birlikte açık anahtar kullanılarak gizli anahtarı elde etmek imkânsızdır.



Şekil 2. Asimetrik Algoritma Şifreleme – Şifre Çözme Süreci

Rivest-Shamir-Adleman (RSA) Algoritması

1977 yılında duyurulan algoritma ayrık logaritma problemine dayanır. Çok büyük sayıları oluşturma ve işleme zorluğu üzerine kuruludur. Anahtar oluşturma işlemi asal sayılar ile yapılır.

- P ve Q gibi çok büyük iki asal sayı seçilir.
- Bu iki asal sayının ve bir eksiklerinin çarpımı $N = P.Q$, $\varphi(N)=(P-1)(Q-1)$ hesaplanır.
- 1'den büyük $\varphi(N)$'den küçük $\varphi(N)$ ile aralarında asal bir E tamsayısı seçilir.
- Seçilen E tamsayısının mod$\varphi(N)$'de tersi alınır sonuç D gibi bir tamsayıdır.
- E ve N tamsayıları genel anahtarı, D ve N tamsayıları ise özel anahtarı oluşturur. [3]

RSA Sisteminin Güvenliği

RSA algoritmasına yapılabilecek saldırılardan birisi P ve Q sayılarını hesaplamaya çalışmaktır. P ve Q sayılarının tespit edilebilmesi durumunda $\varphi(N)$ sayısı ve dolayısıyla D gizli anahtarı hesaplanabilir. Bu durumda şifrelenmiş metinler kolaylıkla çözülebileceği gibi imzalar da taklit edilebilir. N= PQ olduğundan çarpanlara ayırma yapılarak P ve Q sayıları tahmin edilmeye çalışılır. Büyük sayıların çarpanlara kolayca ayrılabilmesiyle ilgili henüz kesin ve hızlı bir yöntem bulunmadığından P ve Q sayıları çok büyük seçilirse bu işlem imkansızlaşır.[4]

RSA algoritmasında şifreleme işlemi şifrelenmesi düşünülen karakterin ASCII karakter tablosundaki

karşılıklarının belirlenen E anahtarı üssünün N sayısına göre mod alma işlemi ile gerçekleştirilir. İşte bu noktada iki adet problem ortaya çıkmaktadır.

- E ve D anahtarlarının büyüklüğü nedeniyle üs alma işleminin uzun sürmesi
- Seçimler ve işlemler sonucunda ortaya çıkan çok büyük sayıların depolanması

Bu çalışmamızda bu iki probleme yönelik masaüstü pcler için Windows platformu mobil cihazlar için android platformu kullanılarak uygulama geliştirilmiş ve performans tespiti yapılmıştır.

MODÜLER ÜS ALMA

Bilgi teknolojilerinde klasik üs alma işlemleri kullanılacak olursa üs adet çarpma işlemi yapılması gerekir. Örneğin RSA algoritmasında şifrelemek için kullanılacak olan E=230910291 anahtarı 230910291 defa çarpma işlemi yapılacağı anlamına gelir. Bu işlemin şifrelenmesi istenen metnin her bir karakteri için yapıldığı düşünülecek olursa sonucun ne kadar uzun sürdüğü tahmin edilebilir.

Modüler üs alma algoritmaları kullanıldığında ise bu işlem çok daha kısa sürede sonlandırılır. Bu çalışmamızda ikili üs alma metodu (Binary Method) kullanılmıştır. İkili üs alma metodu üs değerini ikili sistemde değerlendirerek her bit değerine göre işlem yapar. Örneğin 230910291 sayısının bit karşılığı 11011100001101101001010010011 ve üs alma işlemi için 15 defa çarpma işlemi yapılacaktır. [3]

Örneğin 3^15 (mod 10) işlemini ele alalım.

3^15=14348907 ve 14348907 (mod 10) =7 olduğundan 3^15 mod 10 = 7 dir. Klasik üs alma mantığında tabanın 15 defa kendisiyle çarpılmasını gerektiren döngü kurulur.. İkili üs alma metodunda 15 sayısının bit karşılığı olan 1111 daki bit karakterleri adedi kadar yani 4 defa işlem yapılır. Algoritma şöyledir:

1. Sonuç=1
2. Eğer son bit 1 ise sonuç = sonuç*taban mod n
3. Değilse taban = taban*taban mod n
4. Üssü bir bit sağa kaydır
5. 2. Adıma git

Bu işlem sonucunda tabanın 4 adımda 15. Kuvveti alınmış olur.

UYGULAMA

Çalışmamızda RSA algoritmasının Android ve Windows platformlarındaki performansı test edilmiştir. Android platformunun doğal dili olan java kullanılarak uygulama geliştirilmiş ve bu uygulama bir emulator tablet de ve gerçek tablet de çalıştırılmıştır. Windows platformu için c# dilinde uygulama yazılmış ve pc de test edilmiştir. Şifrelenecek veri olarak 65 basamaklı ve 260 basamaklı iki adet sayı seçilmiştir.

Uygulamanın PC versiyonu Windows 10 işletim sistemi, AMD Phenom II işlemci 8 GB ram donanımına sahip masaüstü bilgisayarda, mobil versiyonu Android 4.0.4 işletim sistemi NVIDIA Tegra 1Ghz dual core 1GB Ram Motorola Xoom tablet ve Android 4.1 Jelly Bean işletim sistemi Armeabi – v7a tek Çekirdekli İşlemci 1536GB Ram Emulator tablet ile yapılmıştır.

RSA algoritmasının gücü P ve Q sayılarının büyük seçilmesi işlemine dayanır. Çalışmamızda P ve Q sayıları 210 basamaklı sayılar olarak seçilmiştir. Bu sayılar internet kullanılarak bulunmuştur. [7]

P=449417999055441493994709297093108513015373787049558499205492347871729927573118262811508386655998299074566974373711472560655026288668094291699357843464363003144674940345912431129144354948751003607115263071543163

Q=643808006803554439230129854961492699151386107534013432918073439524138264842370630061369715394739134090922937332590384720397133335969549256322620979036686633213903952966175107096769180017646161851573147596390153 [7]

N=P*Q=2893389061935254999093170856551293001773658486700109961034756033503178071108094410504900624339669067240975947894640920418682347794608464677806000131150809116632025487984149797615133484802447858476276955511439647547230142540914027248277018746492731723054391029052435045639900211954700658629784297642678110394919124636699652538653628662441

530779411610353308007986488516578967427848289713639255595384651640941168379276739393

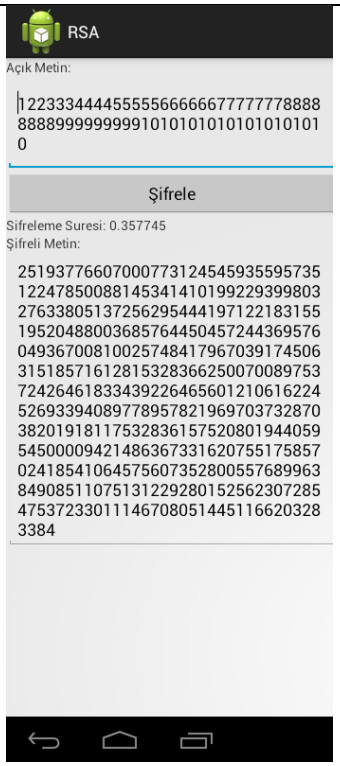
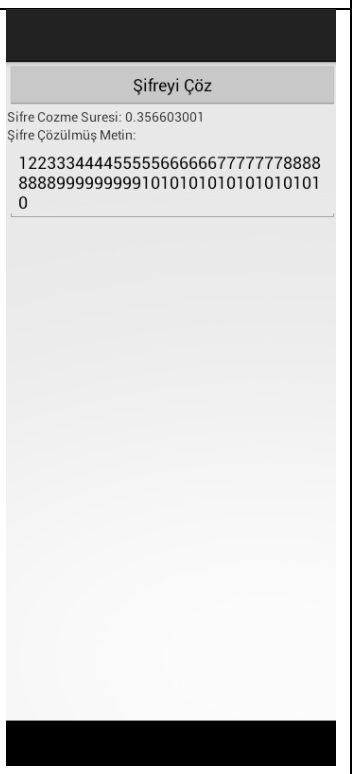
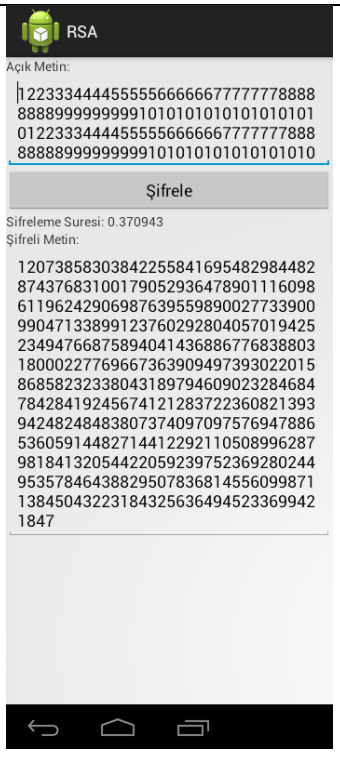
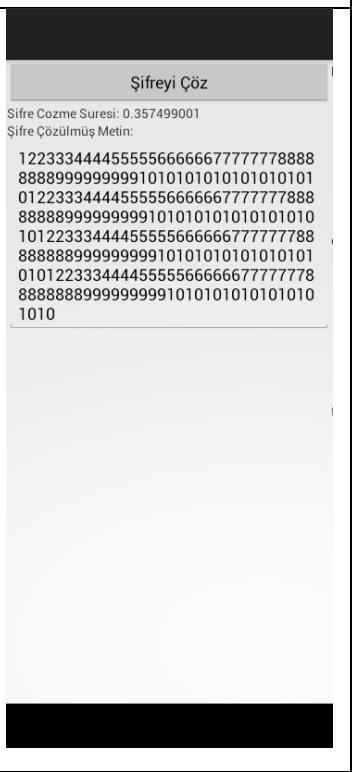
RSA algoritması için E ve D anahtarları Windows ortamında uygulama geliştirilerek üretilmiştir. İki farklı büyüklükte E anahtarı kullanılmıştır. E_1 420 basamaklı E_2 308 basamaklı olarak seçilmiş ve her iki anahtar için herbiri 420 basamaklı iki D sayısı hesaplanmıştır.

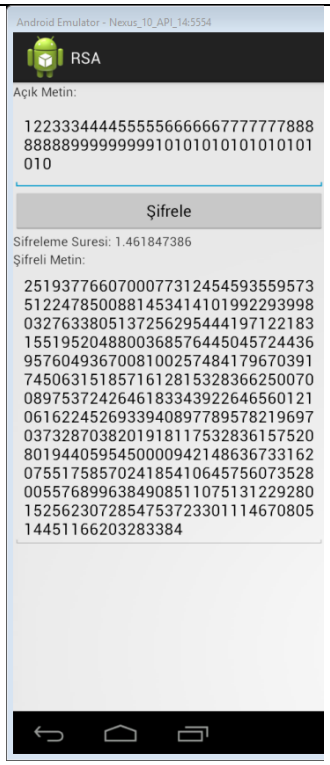
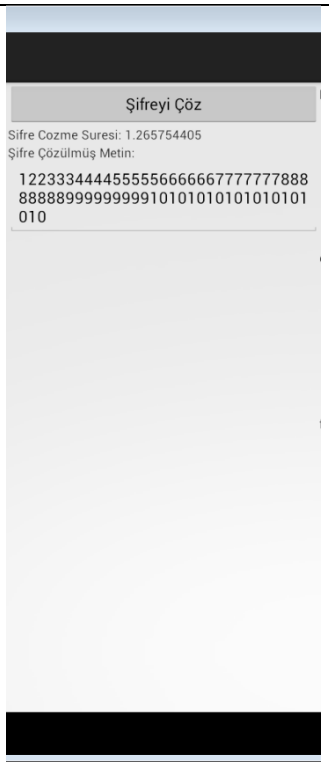
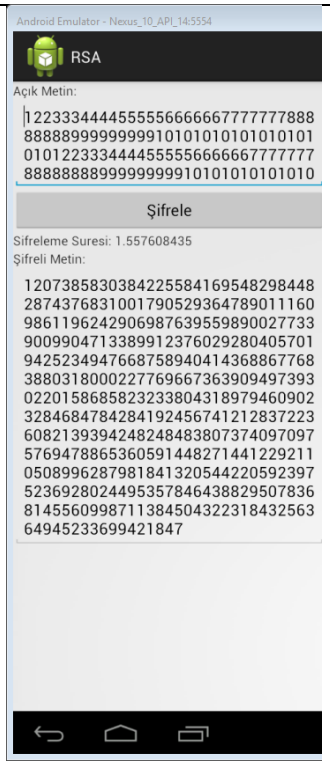
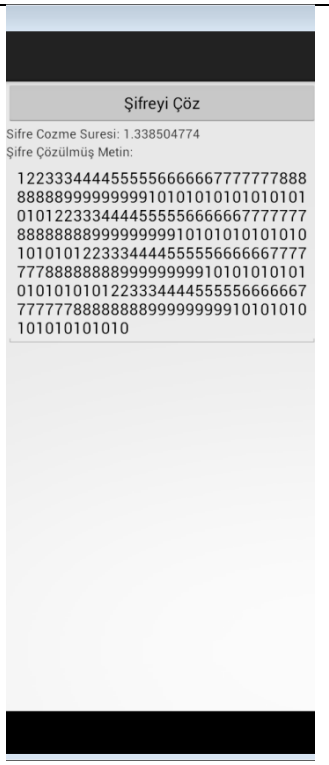
E_1=219100770047019029946923618920704654780753473413515819991871309638745318383257844367901619636661499361367622567440110817709893682197344237065412178825532003639041707530852179255612614538180946935055756586378210777259055692692918735485429836147390774001555113402470837863530244669842520322802040808293515399451846306437540155324649038786768125940836697831889235140434104142880088647385735930208366405965569285937616674153348639896427300375823168517

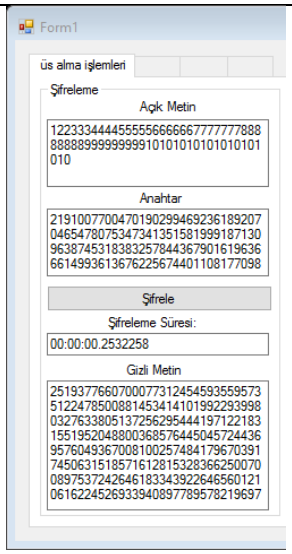
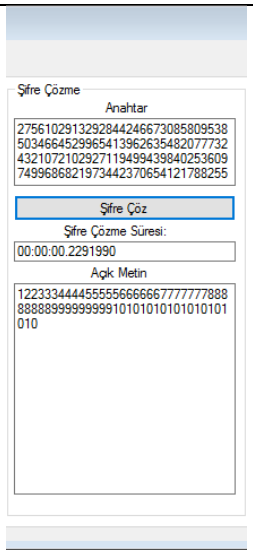
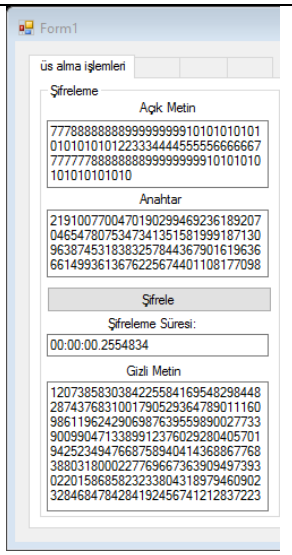
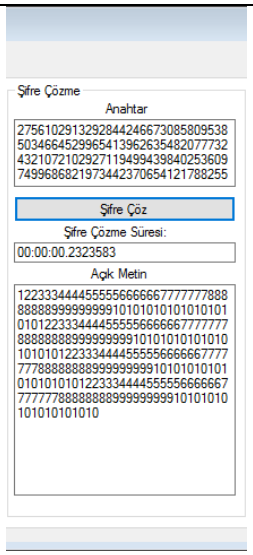
E_2=315708373089097488425021449668536410244502647288180957489215817834474129205029080507103654722281168713194040426421514457423857113014817847656441966584545024462891225816173193483793563318500081792590289497518616067319348379356331850008179259028949751861606

D_1=275610291329284424667308580953850346645299654139626354820777324321072102927119499439840253609749968

D_2=206482482124087453104124624891275575533123318626838700517237795580730787812058749176171053305919677893709948022295929390104800354482269174207994755508533397088920623999900066062268802345827968136886267519465886243413404622461586461980999632804471440168292933215929685080891895514393918731525078914675680151100713910241777283863021899292128291196252206821874403960889807145789250565190299813745951901757616181042652186335

		Şifreleme	Şifre Çözme
Motorola XOOM	65 Basamak - 213 Bit		
	260 Basamak - 861 Bit		

Emülator	65 Basamak - 213 Bit		
	260 Basamak - 861 Bit		

PC	65 Basamak - 213 Bit		
	260 Basamak - 861 Bit		

BIGINTEGER SINIFI

Biginteger sınıfı Microsoft Windows işletim sistemine .NET framework 4 ile dahil olmuş bir sınıftır. Çok büyük sayıları depolamaya ve onlarla işlem yapmaya yarar. Üst sınırı yoktur. Sayılar birer nesne gibi kabul edilir. Integer sayılar ile yapılabilen işlemler Biginteger sınıfı içinde özel metotlarla tanımlanmıştır. Ayrıca math sınıfındaki pow alma vb. metotlar da sınıfın içinde mevcuttur. Üst sınırının olmaması RSA algoritması için kullanılabilmesini kolaylaştırır. Ayrıca aynı sınıf java dilinde de mevcuttur. [5,6]

SONUÇLAR

	Platform	Açık Metin Uzunluğu	Şifreleme Süresi (sn)	Şifre Çözme Süresi (sn)
E1 =420 BASAMAK - 1395 BİT	Masa Üstü PC	260-BASAMAK 861-BİT	0,30	0,27
		65-BASAMAK 213-BİT	0,25	0,26
E2 =308 BASAMAK - 1023 BİT		260-BASAMAK 861-BİT	0,21	0,28
		65-BASAMAK 213-BİT	0,19	0,28
E1 =420 BASAMAK - 1395 BİT	Motorola Xoom	260-BASAMAK 861-BİT	0,37	0,35
		65-BASAMAK 213-BİT	0,35	0,35
E2 =308 BASAMAK - 1023 BİT		260-BASAMAK 861-BİT	0,28	0,35
		65-BASAMAK 213-BİT	0,21	0,35
E1 =420 BASAMAK - 1395 BİT	Emulator	260-BASAMAK 861-BİT	1,55	1,33
		65-BASAMAK 213-BİT	1,46	1,26
E2 =308 BASAMAK - 1023 BİT		260-BASAMAK 861-BİT	1,14	1,39
		65-BASAMAK 213-BİT	1,01	1,37

Elde edilen sonuçlara göre RSA algoritması mobil cihazlarda kabul edilebilir sürelerde şifreleme işlemlerini gerçekleştirebilmektedir. Günümüzde mobil cihazların donanımları kişisel bilgisayarların seviyesine geldiği düşünülecek olursa RSA algoritmasının sağladığı güvenlik uygulamalarda tercih edilebilir.

KAYNAKLAR

1. ÖZÇELİK M. A., KARABULUT M., SUBAŞI A., Bluetooth üzerinden güvenli veri iletimi. 2 ELECO '2012 Elektrik - Elektronik ve Bilgisayar Mühendisliği Sempozyumu, 29 Kasım - 01 Aralık 2012
2. ÇAKMAK A. ADALI E. , Mesajların Şifrelenmesinde Yeni Bir Yöntem ve Android Uygulaması. TÜRKİYE BİLİŞİM VAKFI BİLGİSAYAR BİLİMLERİ ve MÜHENDİSLİĞİ DERGİSİ ISSN 1305-899,1 Yıl 2013 Sayı 7
3. YERLİKAYA T., GENÇOĞLU H., EMİR M. K., ÇANKAYA M., BULUŞ E. RSA Şifreleme Algoritması Ve Aritmetik Modül Uygulaması. İstanbul Aydın Üniversitesi Dergisi Yıl 3 Sayı 9, Sayfa (95 - 104), 2011
4. UÇAN O. N., YERLİKAYA T., GENÇOĞLU H., GÜVENLİ HABERLEŞME TEKNİKLERİ. İstanbul Aydın Üniversitesi Dergisi Yıl 3 Sayı 12, Sayfa (69 - 82), 2011.
5. MSDN BigInteger Structure https://msdn.microsoft.com/tr-tr/library/system.numerics.biginteger(v=vs.110).aspx

6. Java™ Platform, Standard Edition 7, Class BigInteger
https://docs.oracle.com/javase/7/docs/api/java/math/BigInteger.html

7. University of Tennessee at Martin Primes Page
https://primes.utm.edu/lists/small/small3.html

http://dergipark.gov.tr/tujes
Trakya University Journal of Engineering Sciences, 18(1): 53-71, 2017
ISSN 2147–0308
Derleme Makale / Review Article

ÖZEL KİRALIK KONUT SEKTÖRÜ VE POLİTİKALARI: DÜNYADAN FARKLI YAKLAŞIM VE DÜZENLEME ÖRNEKLERİ

Aysu UĞURLAR[1*], Tanyel ÖZELÇİ ECERAL[2]

[1] *Yüzüncü Yıl Üniversitesi, Mimarlık ve Tasarım Fakültesi, Şehir ve Bölge Planlama Bölümü, Van*

[2] *Gazi Üniversitesi, Mimarlık Fakültesi, Şehir ve Bölge Planlama Bölümü, Ankara*

Özet: Kent ekonomisinin önemli bir bileşeni olan konut sektörü, düzenleme mekanizmalarının geliştirilmesini gerektirmektedir. Üretilen konut politikalarının en temel amacı, tüm hanehalklarının ister kiralık ister satılık olsun, ödeyebilecekleri "iyi ve yeterli bir konutu" elde edebilmeleridir. Bu bağlamda kiralık konut politikaları konut politikalarının daima önemli bir bileşeni olmaktadır. Gelişmiş Avrupa ülkelerinin kiralık konut sistemi içinde sosyal kiralık konut ve özel kiralık konut üretiminin bir arada yer aldığı görülmektedir. Buna karşın, Türkiye gibi gelişmekte olan pek çok ülkede kiralık konut sistemi sosyal kiralık konut sisteminden yoksun, serbest piyasa koşullarında, özel kiralık konut sistemi denilen, kendiliğinden oluşan bir arza dayanmaktadır. Bu makalede, farklı ülkelerin (gelişmiş) özel kiralık konut sistemlerini, özel kiralık konut arz ve talebini oluşturan temel aktörleri, özel kiralık konut sektörüne yönelik düzenlemeleri değerlendirilmektedir. Sonuç olarak, farklı gelişmiş ülke örneklerinin yaşadığı tecrübelerin Türkiye'de kendiliğinden oluşan özel kiralık konut arz ve talebine yönelik özel kiralık konut politikalarına ve düzenlemelerine nasıl yol gösterebileceği tartışılmaktadır.

Anahtar kelimeler: konut politikası; özel kiralık konut sektörü; özel kiralık konut düzenlemeleri

PRIVATE RENTED SECTOR AND POLICIES: DIFFERENT APPROACHES AND REGULATIONS FROM WORLD CASES

Abstract: Housing market is one of the most important components of urban economics. The main target of housing policies is to achieve "a good and sufficient house" for the every household, either as rental or as for sale. In this respect, rental housing policies have always been an important part of housing policies. In rental housing system of developed European countries, social and private rental housing production take place. However, severaldeveloping country rental housing policies, also in Turkey, lack social rental housing production and the system depends on a self organizing supply in free market conditions. In this article, private rental housing systems of various countries, the actors shaping the demand and supply of private rental housing market and relevant regulations are evaluated. As a conclusion, the experience of these developed countries are discussed for guiding policies and regulations in Turkey, where the market is mostly self organized.

Keywords: housing policy; private rented sector; private rented housing regulations

[*]Corresponding Author: Aysu UĞURLAR

Tel: +90 (432) 225 17 21, e-mail: augurlar@yyu.edu.tr

GİRİŞ

Konutun, toplumların sosyo-ekonomik yapısının önemli bir göstergesi olması konutu kent ekonomisinin en önemli bileşenlerinden biri durumuna getirmektedir. Konutun sosyal ve ekonomik boyutları, konut sektöründe düzenleme mekanizmalarının geliştirilmesini gerektirmektedir (Emür, 1999). Bu nedenle devletler her dönemde konut sorununa ilişkin politikalar üretmektedirler. Konut politikalarının en temel amacı tüm hanehalkları için iyi ve yeterli bir konutu (Oxley ve Smith, 1996) ödeyebilecekleri bedelden elde edebilmeleridir (Türel, 1997). Bu temel amacın yanı sıra yeni konut üretimi, mevcut stokun iyileştirilmesi, farklı konut kullanım biçimleri (kiracı, ev sahibi) içindeki grupların eşitliği, kar amacı gütmeyen konutların sağlanması ve mülk konutun cesaretlendirilmesi alt amaçları oluşturmaktadır (Oxley ve Smith, 1996). Kiralık konut politikaları konut politikalarının daima önemli bir bileşenidir. Gelişmiş Avrupa ülkelerinin kiralık konut sistemi içinde sosyal kiralık konut ve özel kiralık konut üretiminin bir arada yer aldığı görülmektedir.

Sosyal (kiralık) konut terimi, genellikle piyasa mekanizmalarının aksine, idari prosedürleri karşılayan konut arzının farklı türleri çerçevesinde kullanılmaktadır (Pittini ve Laino, 2011). King'e (2006) göre sosyal konut; kamu fonlarının aktif olarak kullanıldığı; fiyatların ya da kiraların belirlenmesinde kar motifinin baskın olmadığı; miktarının, kalitesinin ve sunum biçiminin belirlenmesinde siyasi karar mekanizmalarının önemli etkiye sahip olduğu konutlardır (Akalın, 2016).

1970lerin ortalarından 1990lara kadar özellikle Avrupa ülkelerinin birçoğunda sosyal kiralık konut üretiminde tarihi bir zirve yaşanmıştır. Ancak günümüzde konut stokunun büyük ve kalıcı bir parçası olarak daha az belirgin hale gelmiştir (Tutin, 2008). Bu durum temel olarak bazı nedenlere dayanmaktır; konut kıtlığı içinde olunmadığı inancı, inşaat sektörünün kapasitesinin gelişmesi ile hanehalklarının seçimlerinin artması, gelir artışı ve buna bağlı olarak minimum standartların üzerinde konut talebi, mülk konutu teşvik eden ya da etmek isteyen konut politikaları, arz yanlı sübvansiyonların etkinliğinin sorgulanması, monetarist bir yaklaşımla makro ekonomik politikalar lehine olduğu düşünülerek kamu harcamalarının kesilmesi, en fazla ihtiyacı olanlara yönelik "hedef" yardımlar için duyulan arzu ve 1980 ve 1990lardaki finansal serbestleşme ile daha yüksek tüketim ve mülk konutun artmasına fırsat tanınması ve küresel ekonomik krizlerdir (Oxley ve Smith, 1996; Tutin 2008). Avrupa Birliği konut politikası alanında doğrudan bir yetkinliğe sahip olmasa da konut sorunları, özellikle küresel finansal krizden bu yana giderek daha da önem kazanmaktadır. Son zamanlarda, konut ile ilgili hizmetlerin ekonomik ve finansal krizler tarafından olumsuz etkilenmesi, özellikle Avrupa ülkelerinde sosyal konut anlayışını ve kimin için kullanılacağını değiştirmektedir (Scanlon vd., 2015).

Gelişmiş ülkelerde sosyal kiralık konut düzenlemelerinin yanı sıra özel kiralık konut düzenlemelerinin özellikle İkinci Dünya Savaşı'ndan bu yana geliştiği görülmektedir. Özel kiralık konutun genel kabul görmüş tek bir tanımı olmamakla birlikte "özel" terimi özel mülkiyet ya da kar yönelimli olma eğilimini ve aynı zamanda sübvansiyon eksikliğini yansıtmaktadır (Whitehead vd., 2012). Haffner vd.'ne (2007) göre özel kiralık konut, piyasa tarafından tahsis edilen kiralık konut olarak tanımlanırken, sosyal konut genellikle piyasa değerinin altında kiralara sahip, idari (yönetsel) olarak tahsis edilen kiralık konut olarak tanımlanır. 1980lerden bu yana sosyal konutun özelleştirme ve serbestleşmesinin daha geniş ekonomik politikalar içinde giderek kabul görmesi, büyüklüğü ne olursa olsun iyi işleyen bir "özel kiralık konut sisteminin" önemini ön plana çıkarmıştır. 1980li yıllarla birlikte liberalleşme eğilimlerine bağlı olarak sosyal sektörün küçülmesi, özel kiralık konutun daha geniş bir hanehalkı aralığınca (gençler, mobil bireyler

vb.) tercih edilmesi, özel kiralık konutun önemini arttırmıştır. Ayrıca özel kiralık konut sektörünün sosyal konuttan daha esnek, diğer bir deyişle daha fazla erişim kolaylığı sağladığı, iyi kalite yönetimi ve bakımı konusunda kiracılara daha iyi hizmet veren bir sektör olduğu ve devlet desteğine gereksinimin azaltılmasının bir yolu olarak da etkili olduğu vurgulanmaktadır (Whitehead vd., 2012).

2008 ekonomik krizinin ardından Tablo 1.'de gelişmiş Avrupa ülkelerinde farklı konut kullanım biçimlerinin (sosyal kiralık konut, özel kiralık konut, mülk konut, diğer) oranları ve sosyal kiralık konut stokunun 10 yıllık süre içindeki değişimi görülmektedir. Buna göre nispeten refah düzeyi daha yüksek olan Avrupa ülkelerinin (Hollanda, Fransa) diğer konut kullanım biçimleri göz önüne alındığında sosyal konut oranının yüksek veya orta düzeyde olduğu görülmektedir. Daha düşük sosyal konut oranına sahip İspanya, İrlanda gibi ülkeler ve komünizmin çöküşünden sonra sosyal konutları(kamuya ait) özelleştirilen Macaristan, Çek Cumhuriyeti gibi ülkelerde ise mülk konut oranının daha yüksek olduğu görülmektedir. Almanya ise Kuzey Avrupa'daki refah devletlerinden biri olarak görülmekle birlikte sosyal konuta yaklaşımı komşularından farklı, "özel kiralık konut oranının yüksek olduğu" bu gruptaki bir istisnadır (Scanlon vd. 2015).

Tablo 1. Farklı Ülkelerin Konut Kullanım Biçimleri Dağılımı (%) ve Soysal Kiralık Konut Değişimi (%)

Sosyal Konut Oranına Göre Ülkelerin Sınıflandırılması	Ülke	Yıl	Sosyal Kiralık Konut			Özel Kiralık Konut Oranı (% toplam konut stoku içinde)	Mülk Konut Oranı (% toplam konut stoku içinde)	Diğer Oranı (% toplam konut stoku içinde)
			Konut sayısı(000)	Oran (%Toplam konut stoku içinde)	10 yıl içindeki Değişim (%)			
Yüksek	Hollanda	2010	2.300	32	-4	9	59	-
	İskoçya	2011	595	24	-6	12	64	-
	Avusturya	2012	880	24	+1	16	50	10
	Danimarka	2011	541	19	+1	17	49	18
	İsveç	2008	795	18*	-3	19	41	22 (kooperatif)
Orta	İngiltere	2011	4.045	18	-2	18	64	-
	Fransa	2011	4.472	16	-1	21	58	5
	İrlanda	2011	144	9	+1	19	70	3
	Çek Cumhuriyeti	2011	312	8	-9	10	65	18
Düşük	Almanya	2010	1054	5	3	49	46	-
	Macaristan	2011	117	3	-1	6	90	1
	İspanya	2011	307	2	+1	11	85	2

* Belediye şirketleri tarafından üretilen sosyal konutlar bu orana dahil edilmemiştir.

Kaynak: Scanlon, K., Fernández, A. M. , Whitehead, C. M. E. 2015. Social housing in Europe. European Policy Analysis (17). s.3.

Gelişmekte olan ülkelerde de mülk konutu özendiren politikalara karşın dar gelirli hanehalklarının konut seçimi oldukça kısıtlı bir ortamda gerçekleşmekte ve özellikle dar gelirli hanehalkları enformel düzenlemelere başvurmaktadır (Ballesteros, 2004). Gelişmiş ülkelerin aksine gelişmekte olan ülkelerde sosyal konut inşası sınırlı kalmıştır ve 1970lerden sonra bazılarında kira için inşa edilen konutlar hızla satılmıştır (UNCHS, 2003). Gelişmekte olan ülkelerde özel kiralık konut sektörü konut piyasasında önemli rol oynamaktadır. Ev sahiplerinin çeşitliliği ya da türleri, ev sahibi-kiracı arasındaki ilişki (düzenlemeler) ve mevzuat ülkeden ülkeye değişmektedir. Gelişmekte olan ülkelerde küçük ölçekli ev sahipleri belirgin iken kurumsal kiralama (sosyal kiralık konut vb.) yetersizdir (Wits University, 2009). Kiralık konuta yönelik finansmanın azalması ve finansal desteklerin olmaması nedeniyle gelişmekte olan ülkelerde özellikle küçük ölçekli ev sahipleri için finansman yaratma çabaları gösterilmektedir. Örneğin Nijerya'da kiralık konut stokunu ve üretimini desteklemek için küçük ölçekli üreticiye iki yıllık kira kadar finansal destek sağlanmaktadır (UNCHS, 1993).

Literatürde özel kiralık konutun işlevinin belirlenmesinde, düzenlemelerin rolüne ilişkin farklı yaklaşımlar bulunmaktadır. Piyasa merkezli ekonomistler, serbest konut piyasasını özel kiralık konutun yeniden canlandırılmasının tek aracı olarak görmektedir. Buna karşın yönetim odaklı (governance oriented) yaklaşıma sahip ekonomistler ise güçlü ve istikrarlı düzenlemeler aracılığı ile özel kiralık konut sektörünün daha iyi işleyeceğini ileri sürmektedirler. Güçlü ve istikrarlı düzenlemeler (kira artış kontrolü, kiracı ve ev sahiplerinin haklarının korunması, barınma güvencesi vb.) konut gereksinimlerini tam kapsamlı bir biçimde sağlamada daha etkin olabilecektir (Whitehead vd., 2012).

Genel olarak dünyada 1980 sonrası yaşanan değişimler hem gelişmiş hem de gelişmekte olan ülkelerin konut politikalarını etkilemiştir. 1980 ve 1990larda küresel olarak artan kentleşme eğilimi özellikle gelişmekte olan ülkelerde arsa sıkıntısı, arsa ve konut fiyatlarının artması ve enformel yerleşimlere toleransın azalması gibi etkenlere bağlı olarak kiralık konut talebini belirgin bir şekilde arttırmıştır (Peppecorn ve Taffin, 2013).

Küreselleşme sürecinde liberal politikaların baskın olduğu gelişmiş ülke politikalarını izleyen, Türkiye gibi gelişmekte olan ülkelerin mülk konutu özendiren politikalarının, barınma ya da konut sorununu çözmede yeterli olmadığı görülmüştür. Sosyal kiralık konut politikaları ve uygulamalarının da çok sınırlı olduğu ya da hiç olmadığı bu ülkelerde, hükümetlerin konut ile ilgili sorumlulukları pasif olmakta, barınma konusu ikincil kalmakta ve konut arzı daha çok serbest piyasa koşullarına göre gelişmektedir. Sosyal kiralık konut politika ve uygulamalarının olmadığı ya da yetersiz olduğu, dar gelir grubunun kiracı olmaktan başka seçeneği olmadığı gelişmekte olan ülkelerde kiralık konut arzı kendiliğinden gelişmektedir. Bu durum özel kiralık konut sektörünü ön plana çıkartmaktadır. Farklı ülkelerin (gelişmiş) özel kiralık konut sistemlerini, özel kiralık konut arz ve talebini oluşturan temel aktörleri, özel kiralık konut sektörüne yönelik düzenlemeleri aktarmayı amaçlayan bu çalışmanın literatüre beklenen en önemli katkısı serbest piyasa koşulları içinde kendiliğinden doğan kiralık konut arzına sahip Türkiye gibi gelişmekte olan ülkelerin özel kiralık konut politikalarına ve düzenlemelerine yol göstermesidir.

ÖZEL KİRALIK KONUT SEKTÖRÜNÜN ÖZELLİKLERİ

Ülkelere göre farklı tanımlamaları olmakla birlikte özel kiralık konut bazı ülkelerde mülkiyete ya da ev sahipliğinin türüne göre tanımlanabilmektedir. Bazılarında da kiracılığın türüne göre ve konutun kullanım türüne göre tanımlanabilmektedir (Scanlon, 2011) (Tablo 2).

Tablo 2. Farklı ülkelere göre özel kiralık konut sektörünün tanımlanması

ABD	Kar amaçlı ya da kar amacı gütmeyen kuruluşlar/konutu sübvanse edilen kiracılar
Avustralya	Kar amaçlı
Avusturya	Kar amaçlı: kişisel veya kurumsal mülkiyet
Almanya	Kamuya açık olmayan küçük özel şirketler, kar amacı gütmeyen konut kooperatifleri, kiliselerin sahip olduğu konut şirketler, ayrıca küçük amatör ev sahipleri, kar amacı gütmeyen kuruluşlar
Danimarka	Kar amaçlı tek mülkiyetli üç ya da daha fazla birimlerden oluşan bloklar
Hong Kong	Kar amaçlı
İngiltere	Yerel yönetimler ya da konut birliklerine ait olmayan tüm kiralık konutlar
Hollanda	Kuruluşlar, özel kişi ve aileler
İsviçre	Kar amaçlı ev sahipleri ve devlet tarafından düzenlemiş kurumsal yatırımcılar(emekli sandığı gibi)
Norveç	Belediyelerin sahip olmadığı ve kontrol etmediği konutlar
Fransa	Düzenlenmiş ve sübvanse edilmemiş kiracılık
İspanya	Belirli yasal koşulları karşılayan kiracılık
Finlandiya	İkamet amaçlı kiralık konutlar

Kaynak: Scanlon, K. Private Renting in Other Countries. 2011. Scanlon K. & Kochan B. (eds.), Towards a Sustainable Private Rented Sector: The Lessons from Other Countries, LSE London, s. 15.

Tablo 2'de görüldüğü gibi bazı ülkelerde sadece kar amaçlı ev sahiplerinin özel kiralık konut sektörü olduğu kabul edilirken, Almanya gibi bazı ülkelerde kiliseler, yardım kuruluşları gibi kar amacı gütmeyen kuruluşlar da özel kiralık konut sektörü içinde kabul edilmektedir. İsviçre'de özel kiralık konut sektörü, bireyler ya da ailelerden, sigorta şirketleri, emlakçılar gibi kurumsal organizasyonlardan, devlet tarafından düzenlenmiş kurumsal yatırımcılara (emekli sandığı) kadar uzanmaktadır. İsviçre'de çok geniş bir özel kiralık konut sektörü vardır. Gayrimenkul portföylerinin bir parçası olarak emeklilik fonları özel kiralık konut sektörü için büyük rol oynamaktadır. Özel kiralık apartmanlar, emeklilik fon yöneticileri için popüler bir varlıktır. Hong Kong'da ise öğrenci evi, mobilyalı kiralama, hosteller dahi özel kiralık konut olarak kabul edilmektedir (Whitehead vd., 2012).

Özel Kiralık Konut Sektörünün Büyüklüğü

1900lerin başından bu yana neredeyse tüm Avrupa ülkelerinde özel kiralama geniş düzenleyici müdahalelere konu olmuştur. 1970 ve 1980lerden bu yana özelleştirme ve serbestleşmenin daha geniş ekonomik politikalar içinde giderek kabul görmesi, büyüklüğü ne olursa olsun iyi işleyen bir özel kiralık konut piyasasının önemini ön plana çıkarmıştır (Whitehead vd., 2012).

Sosyal konut programlarının azalması ayrıca niceliksel olarak talebi karşılayamaması üzerine özel kiralık konut sektörünün yirmi yıl öncesi öngörülenden daha

fazla öne çıkacağı ve rol alacağı öngörülmektedir. Özel kiralık konut sektörü, bir geçiş olarak görülmekten öte, hanehalkları için mülk konut ya da sosyal kiralık konuttan daha arzu edilir görülmekte ve 20. yüzyıl boyunca bu sektörü reddeden ülkelerde hem sosyal kiralık konut hem de mülk konut için uzun dönemli bir alternatif olacağı öngörüsü artmaktadır (Scanlon ve Whitehead, 2004; Doling ve Ford, 2007).

Tablo 4'de 1980li yılların başından itibaren bazı ülkelerin, özel kiralık konut büyüklüğündeki (oran) değişim görülmektedir. Örneğin son yirmi yılda İngiltere'de sektörün büyüklüğü neredeyse iki katına çıkmıştır (Scanlon, 2011; Tang, 2013). Bununla birlikte Avusturya, Danimarka, Hollanda ve İspanya'da özel kiralık konut sektörü giderek küçülmektedir (Tablo 4). Scanlon'a (2011) göre bu durum sektörün bu farklı yönlerini ve her ülkenin belirli düzenleyici ve ekonomik durumlarını yansıtmaktadır.

Tablo 4. 1980'den bu yana özel kiralık konut sektörünün gelişimi (%)

Ülkeler	Özel Kiralık Konut Oranı (%)				1980'lerden 2000'lere değişim	2000 sonrası değişim
	1980'lerin başı	1990'lerin başı	2000'lerin başı	2000 sonrası		
ABD	33	35	32	32	Değişmedi	Değişmedi
Almanya	Yaklaşık 60	Yaklaşık 60	Yaklaşık 60	Yaklaşık 60	Değişmedi	Değişmedi
Avustralya	21	22	23	25	Yükseldi	Yükseldi
Avusturya	25	21	18	16	Düştü	Düştü
Danimarka	22	18	18	16	Düştü	Düştü
Fransa	25	21	21	21	Düştü	Yükseldi
Hollanda	19	13	13	10	Düştü	Düştü
Hong Kong	24	14	15	16	Düştü	Yükseldi
İngiltere	11	9	10	17	Yükseldi	Yükseldi
İrlanda	13	10	7	10	Düştü	Yükseldi
İspanya	19	15	11	7	Düştü	Düştü

Kaynak: Scanlon, K.. Private Renting in Other Countries. 2011, Scanlon K. & Kochan B. (eds.), Towards a Sustainable Private Rented Sector: The Lessons from Other Countries, LSE London, s.19

Özel Kiralık Konut Arz

Özel kiralık konutun tanımı ülkeden ülkeye değiştiği yukarıda ele alınmıştır. Bu çerçevede sektör içinde özel kiralık konut arzının aktörlerini; hane halkları, kurumlar, işverenler, kooperatifler ve kar amaçsız kuruluşlar, kiliseler ve kamu destekli kuruluşlar oluşturmaktadır. Ancak kar amaçsız kuruluşlar, kamu destekli kuruluşlar ve kiliselerin daha çok özel kurumların ev sahipliğini yaptığı ve sosyal kiralık konut niteliğinde olduğu da gözden kaçırılmamalıdır (Tablo 3).

Tablo 3. Arzın (ev sahiplerinin) türüne göre özel kiralık konut arzını sağlayan aktörler

Ülkeler	**Özel Kiralık Konut Arzını Sağlayan Aktörler (%)**		
	Hanehalkları (Birey ya da çift)	**Kurumsal**	**Diğer**
Fransa	95,1	3,3	1,6
İrlanda	Çoğunluk	Çok az	
Avustralya	Çoğunluk	Yok	Bazı İşverenler
Belçika	86,0	14,0	
İspanya	86,0	6,7	7,2 (Kamu destekli kuruluşlar)
Norveç	78,0	22,0	
ABD	78,0	13,0 (Şirketler- GYO)	9,0 (Kooperatif ve kar amaçsız kuruluşlar)
Almanya	61,0	17,0	10,0 (kooperatif, kilise vb.)
Hollanda	8,0	10,0	>50 (profesyonel ev sahipleri)
Avusturya	Çok az	Çoğunluk(Şirketleri belediye organları)	

Kaynak: Scanlon, K.. Private Renting in Other Countries. 2011, Scanlon K. & Kochan B. (eds.), Towards a Sustainable Private Rented Sector: The Lessons from Other Countries, LSE London, s.23.

İngiltere'de özel kiralık konut stokunun büyük bir kısmını bireysel ev sahipleri/mülk sahipleri oluşturmaya devam etmektedir. Son 20 yıldır kurumsal yatırımı artırmak için çalışılmışsa da özel kiralık konut sektöründe kurumsal yatırım çok başarılı olmamıştır. Hollanda ve Avusturya dışında hemen hemen tüm ülkelerde bireysel ev sahipleri baskındır. (Scanlon,2011). Kurumsal yatırımda bir model olan ABD'de de stokun çoğu hanehalklarına aittir. Kurumsal yatırımcılar (GYO ve diğer şirketler) bu büyük gayrimenkullerin %24'üne sahiptir. Avusturya'da bireysel mülkiyet altındaki tek üniteli birimler, özel kiralık konut stokunun küçük bir kısmını oluşturmaktadır. Bu nedenle birey ya da çift hanehalkı ev sahiplerinin payı düşüktür. Çoğunlukla şirketler çok katlı kiralık yapıların sahibi olma eğilimindedir (Scanlon,2011).

Özel Kiralık Konut Talebi

1980 sonrası liberalleşme eğilimlerine bağlı olarak sosyal (kiralık) konut sektörünün küçülmesi ile özel kiralık konut, konut piyasasında daha esnek erişimi (piyasa fiyatlarını ödeme gücü olmayanlar için uygun fiyatlı konut) sağlamaya yardımcı olma potansiyeline dönüşmektedir. Böylece özel kiralık konutun rolü, daha geniş bir hanehalkı aralığını içine alan farklı hanehalkı gruplarına doğru devam etmektedir. Özel kiralık konutun, daha genç bireyler ve daha mobil hanehalkları için daha uygun olduğu ve iyi işleyen bir iş gücü piyasasına da katkısı olduğu düşünülmektedir (Whitehead vd., 2012). Örneğin İngiltere'de özel kiralık konut sektöründe gençler, göçmenler ve hatta sosyal konutta oturmaya hak kazanmayan dar gelir gurubu hanehalkları yer almaktadır. İngiltere'de özel kiralık konut sektörü içinde yer alan hanehalklarının

yaklaşık %35'i konut kira yardımı (yerel konut kira yardımı) almaktadır. Bu aynı zamanda İngiltere'de özel kiralık konut sektörü içinde yer alan dar gelirli hanehalkının payının bir göstergesidir (Scanlon,2011).

Scanlon ve Whitehead (2004), bazı ülkelerin (toplam 17 ülke) konut kullanım biçimi ve ipotekli konut kredisi sistemini inceledikleri çalışmalarında genç ve orta yaşlı grupların ev sahipliğine geçişini incelemektedir. Çalışmada ortalama gelire sahip 25 yaş civarı çocuksuz iki yetişkin "genç", 45 yaş civarı orta yaşlı ve iki çocuklu yetişkinler ise "orta yaşlı" gruplar olarak ele alınmıştır. Çalışmaya göre genç grupların daha çok kiralık konut sektörü içinde yer aldığı, orta yaşlı grupların ise büyük çoğunluğunun mülk konut sektörü içinde yer aldığı görülmektedir. Bununla birlikte ülkelerin çoğunluğunda (İsveç, Hollanda, Çek Cumhuriyeti hariç), kiralık konut sektörü içinde yer alan genç grupların özel kiralık konut sektörü içinde yer alma oranının sosyal kiralık konuttan daha yüksek olduğu görülmüştür.

Özel kiralık konut sektörü içinde, gençlerin yanı sıra dar gelirli aileler, bekârlar, çocuksuz aileler ve göçmenlerin de olma olasılığı daha yüksektir. Özellikle İngiltere, Avustralya'da özel kiralık konut sektörü içinde göçmenlerin görülme olasılığı yüksektir. Hong Kong'da kamu kiralık konutlarına erişim konusunda güçlü kısıtlamaların olması dar gelirli göçmen ailelerin özel kiralık konuta yönlenmesinin gerektiği anlamına gelmektedir. Danimarka'da özel kiralık konut içindeki kiracıların 2000 yılı Danimarka ortalamasının % 30 altında bir gelire sahip olması özel kiralık konut sektörünün dar gelirli birey ya da hanehalklarını da barındırdığının göstergesidir. Belçika'da da, dar gelirli hanehalkları, bekârlar, birlikte yaşayan çiftler, işsizler özel kiralık konut sektörü içinde fazlasıyla görülmektedir (Scanlon, 2011). Ancak özel kiralık konut sektörünün en alt düzeyindeki bileşim ülkeden ülkeye değişmektedir. Örneğin Avustralya'da savunmasız ve daha yaşlı kiracılar özel kiralık konut sektörü içindeki en büyük sorun iken İngiltere'de bu gruplar ağırlıklı olarak sosyal konut sektörü içindedir (Scanlon, 2011). Kemp ve Keoghan'a (2001) göre kiracıların istekleri ve değişen talebi göz önüne alındığında, özel kiralık konut (sosyal kiralık konut yerine) daha iyi bir çevre ve konutta yaşamak için de tercih edilebilmektedir.

ÖZEL KİRALIK KONUT SEKTÖRÜNE YÖNELİK DÜZENLEMELER

Bir konut piyasasında kiralık konut sektörünün başarısı aynı zamanda mülk konut sektörünün de başarısına bağlıdır. Konut piyasasının bu iki önemli bileşeni birbirinden bağımsız düşünülmemelidir. Ekonomide mülkiyet hakkının serbest olması herkesin konut sahibi olacağı anlamına gelmemektedir. Bu sebeple kiralık konutların kiraya verildiği ve kiralandığı bir piyasa vardır. Ancak kiralık konut piyasasında konut miktarı yetersizse, konut arz edenler bu durumdan yararlanmak ve gelirlerini daha çok artırmak isteyeceklerdir. Böyle bir durum ekonomik ve sosyal bağlamda sorunların yaşanmasına neden olabilmektedir.

Literatürde özel kiralama genellikle istekli satıcının konutu sağladığı, istekli alıcının da konutu tüketmek için bir araya geldiği, düzenleme mekanizmaları ile tadil edilen bir piyasa sistemi olarak tanımlanır. Kiralar arz ve talep tarafından belirlenir ve kira seviyeleri, hem ev sahiplerinin hem de kiracıların kararlarını etkiler. Böylece talep tarafında tüketicilerin istekleri/tercihleri onların gelirlerine bağlıdır. Her hane halkı istedikleri konutun yaklaşık değeri, konumu ve diğer konut kullanım biçimlerinin göreli fiyatına göre bir karar verir. Arz tarafında ise diğer yatırımlarla karşılaştırıldığında göreli riskleri dikkate alarak geri dönüşüne dayalı olarak ev sahipleri özel kiralık konutu sağlamaya karar vermektedir. Eğer piyasa iyi çalışırsa, talep tarafı kiralardan memnun olacağından arz tarafı da bu sektörde kalmak için teşvik edilmiş olacaktır (Whitehead vd., 2012).

Konut yaşamın bir gereğidir ve özellikle düşük gelirliler olmak üzere hane halkları gelirlerini yüksek

oranda tüketme eğilimindedir. Eğer özel kiralık konut sektörü içindeki kiralar gelir çizgisinin dışına çıkarsa, bireylerin ya da hane halklarının ödeyebileceği yeterlilikte konut için, hükümete müdahale etmesi için baskı oluşacaktır. Aynı şekilde eğer aniden kira yükselirse de (örn. doğal afet, savaş vb.) müdahale için baskı oluşacaktır. Devlet müdahalesi birçok şekilde olabilir. Örneğin, piyasa-altı kiralarla sosyal konut, daha yoksul hane halklarına verilen gelir sübvansiyonları, vergi indirimleri vb.. Ancak tarihsel olarak düzenleme mekanizmaları, özellikle piyasadaki ve barınma koşullarındaki ani değişimlere ilk yanıt olarak ortaya çıkmıştır (Whitehead vd., 2012).

Literatürde özel kiralık konutun işlevinin belirlenmesinde düzenlemelerin rolü son derece tartışmaya açıktır. Bir diğer yandan özel kiralık konut sektörünün sürdürülebilmesi ve geliştirebilmesi için de hangi düzenlemelerin gerekli olduğunun anlaşılması açısından incelenmesi önemlidir ((Whitehead vd., 2012; Tang, 2013). Literatürde özellikle piyasa merkezli ekonomistler, "düzenlemelerin" hem ev sahipleri açısından hem de kiracılar açısından tamamen olumsuz olduğunu savunmaktadır (Gilbert, 2003,Whitehead ve ark., 2012). Ayrıca, konut sahibinin mülkiyet hakkına sınırlama getirdiği düşünülmektedir (Lipsey ve ark., 1984). Bu yaklaşım içindekiler özel kiralık konutun yeniden canlandırılmasının tek aracı olarak "serbestleşmeyi" görmektedir. Buna karşın yönetişim odaklı (governance oriented) yaklaşıma sahip olanlar ise güçlü ve istikrarlı düzenlemelerin sonucunda özel kiralık konut sektörünün daha iyi işleyeceğini ve böylece özel kiralık konut sektörünün, konut gereksinimlerini kapsamlı bir biçiminde sağlamada daha etkin olacağını ileri sürmektedirler (Whitehead vd., 2012). Böylece farklı düzenleme yaklaşımlarının arkasında yatan ilkeler incelenmekte ve düzenlemelerin gücü ve özellikleri tarif edilebilmektedir (Whitehead vd., 2012).

Kira düzenlemeleri genellikle iki ana unsurdan oluşmaktadır. Birincisi kira artış düzeyinin kontrolü; kiracıların ödeyebileceğinden fazla tutmamayı amaçlayarak kiraların artışını uygun fiyatta korumak ve ekonomik olarak tahliyeleri (evden çıkarılmaları) önlemeye çalışmaktır. İkincisi**,** barınma güvenliği; oturma süresi, belirli ve sınırlı nedenler dışında kiracıların ev sahiplerince çıkarılmasına getirilen sınırlılıklardır (Pomeroy ve Godbout, 2011).

Kira kontrolü

Kiralık konut talebi çok esnektir. Bunun birçok nedeni vardır. Bir bölgedeki kiralık konutun nispi fiyatı arttıkça aşağıdakilerden biri meydana gelecektir (Lipsey vd., 1984):

- Bireyler ya da hanehalklarının bazıları konutu kiralamaktansa satın almayı tercih edecektir.
- Bireyler ya da hanehalklarının bazıları kiralık konutun daha ekonomik ya da düşük olduğu yere taşınacaktır.
- Bireyler ya da hanehalklarının bazıları daha küçük ve ucuz konutları kiralayarak tükettikleri konut miktarından tasarruf edeceklerdir. Hatta bazıları, konutlarının bir ya da iki odasını başkalarına kiralayabilirler.
- Bireyler ya da hanehalklarının bazıları evlenebilecek, bazıları da evlenemeyecektir. Örneğin ailesinin yanından daha rahat ayrılarak bağımsız yaşamayı tercih eden genç erişkinler, ailelerinin yanlarından önceden olduğu gibi kolay gidemeyeceklerdir.

Yukarıdaki davranış biçimleri kiralık konutun yüksek talep esnekliğine katkıda bulunacaktır. Kiralardaki artış, talep edilen miktarı büyük ölçüde düşürecektir. Kira kontrolü ya da denetimi böyle bir artış olmasını önleyen, devletin aldığı yasal ve yargısal tedbirlerle kiraların belirli sınırlar içinde tutulması ya da dondurulmasıdır. Kira kontrolü yüksek enflasyonun yaşandığı ve buna bağlı olarak kiralık konut stok açığının yaşanması durumunda kiracı hanehalklarını korumayı amaçlayan kısa vadeli bir politikadır (Lipsey vd., 1984).

Kira kontrolleri "birinci kuşak kira kontrolleri", "ikinci kuşak kira kontrolleri" (Şahin, 2005) ve "üçüncü kuşak kira kontrolleri" olarak sınıflandırılmaktadır. Birinci kuşak kira kontrolleri yürürlükte olan kiraların piyasa seviyesinin altında dondurulmasıdır. İlk olarak 1900lerin başında Birinci Dünya Savaşı sırasında ve sonrasında savaşın olumsuz etkilerini hafifletebilmek amacıyla Avrupa'da uygulanmaya başlanmıştır (Keleş, 2010; O'Sullivan ve De Decker, 2007; Şimsek, 2010). 1970'lerde gerçekleşen "ikinci kuşak kira kontrolleri" ise 1973 petrol krizinden sonra pek çok Avrupa ülkesi ve ABD'de enflasyonu azaltmaya yönelik stratejilerin bir parçası olarak düzenlenmiştir ve kiralarda yıllık belirli bir miktar artışına izin verilmiştir (Lind, 2001; O'Sullivan ve De Decker,2007 Şimşek, 2010). Genel yaşam maliyeti ve konutun iyileştirilmesi gibi durumlar yıllık kira belirlenmesinde dikkate alınmıştır (O'Sullivan ve De Decker, 2007). Birinci kuşak kira kontrolleri, tahliyeleri yasaklama eğilimi içindeyken, ikinci kuşak kira kontrolleri belirli koşullar altında tahliyelere izin vermektedir (Gilbert, 2003). Birinciye göre daha esnek olduğu düşünülen ikinci kuşak kira kontrolleri yerini, enflasyonun düşmesi üzerine 1990ların başında üçüncü kuşak kira kontrolleri olarak bilinen, bireysel düzenlemelere bırakmıştır (O'Sullivan ve De Decker, 2007; Şimsek, 2010; Ellingsen ve England, 2003). Günümüzde güncel olan "üçüncü kuşak kira kontrolü" kiracının kiracılık hak ve statüsüne dayalı, kiracılık süresince geçerli (O'Sullivan ve De Decker, 2007) kiracı ve ev sahibi arasındaki bireysel sözleşmeye dayalıdır (Ellingsen ve England, 2003). Kısaca birinci kuşak kira kontrolleri kira düzeylerinin korunması olarak tanımlanabilirken, ikinci ve üçüncü kuşak kontroller kiraların artışları üzerindeki farklı türdeki kontrollerdir (Whitehead vd., 2012).

Barınma güvencesi

Kira düzenlemeleri barınma güvenliği ile yakından ilgilidir (Scanlon, 2011). Kira kontrolleri ilk kez uygulanmaya başladığı zaman, ev sahipleri bu uygulamanın hemen ardından oturan kiracıları tahliye ederek daha yüksek kiraları verecek ya da ödemeye hazır kişileri tercih etmiştir. Bu yüzden güvenlik maddeleri eklenmiş ve bazı zamanlar yeni nesiller bile, sözleşme koşullarını yerine getirdiği sürece mülk içinde kalma hakkını elde etmiştir. Barınma güvencesi (kiracılığın düzenlenmesi), ev sahibi-kiracı arasındaki bir dizi hükümlerden oluşan sözleşme (kontrat) ile kiracının ikamet süresince korumaya alınmasıdır. En önemlisi, "ekonomik tahliye" riskine karşı güvence sağlanmasıdır. Çünkü ev sahibi daha fazla ödemeye hazır birini bulduğunda kiracıyı konutundan çıkarmak isteyebilir. Tahliye süreçlerinin etkinliği genellikle konut politikalarından çok hukuk sistemine bağlıdır. Sözleşme sürecinin her aşamasında ev sahibi ve kiracı arasındaki göreli güç genel olarak yansıtılmaktadır (Whitehead vd., 2012).

Kira düzenlemeleri ile birlikte ele alındığında, kiralarla ilgili olarak barınma güvenliğinin geleceğine ilişkin belirsizlikler azalır. Bu, konutun boş kalması ve geri dönüşüm maliyetinin azaltılması olarak hem ev sahibi hem de kiracıya yardımcı olmaktadır. Ayrıca barınma güvenliğinin düzenlenmesi ile ev sahibinin konutunu satmak istemesi ya da başka birine transfer etmek istemesi gibi durumlara karşı bir açıklık (netlik) getirmektedir (Arnott 2003). Bu kapsamda barınma güvenliği "standart sözleşme süresi, bildirim süresi ve sözleşme feshi, erken feshetme hakları, kira sözleşmesinin mülkiyetin satışı üzerinde etkisi" gibi faktörlerden etkilenmektedir (Whitehead vd., 2012).

Kira sözleşmeleri belirli ya da belirsiz süreli olabilmektedir. Ancak daha çok belirli süreye dayalı kira sözleşmeleri yaygındır. Belirli süreli kira sözleşmelerinin minimum süresi, ülkeler hatta bazen farklı sözleşme türlerine bağlı olarak ülkelerin kendi içerisinde dahi farklılıklar gösterebilmektedir. Minimum ya da standart bir sözleşme süresi ev

sahibine bağlı olarak değişebilir. Sözleşme süresi dolduktan sonra devam ettirebilir ve biçimi değişebilir (Whitehead vd., 2012). Belirli süreye dayalı kira sözleşmelerinde barınma güvencesi, sözleşme koşullarına uyulduğu sürece sözleşme süresince yüksektir (Haffner vd., 2007).

Her iki türde sözleşme altında barınma güvencesi çeşitli faktörlere bağlıdır. Eğer ev sahibinin feshetme hakları iyi düzenlenmiş ise, uzun dönemli kira sözleşmeleri belirsiz sözleşmelerden daha yüksek güvenlik sağlayabilir. Ayrıca kiracı hakları açısından da sınırlılığı azaltmaktadır. Belirsiz sözleşmelerde, barınma güvencesi bildirim süresi ve ev sahibinin feshetme hakları ile belirlenir (Whitehead vd. , 2012; Tang, 2013). Düzenlemeler daha azdır ve kiracı daha güvensizdir. Bu bağlamda uzun bildirim süreleri ya da sözleşme sonuna kadar kısıtlı haklar ile barınma güvencesi yüksek olabilir. Bu tedbirler alınmazsa barınma güvencesi son derece düşüktür. Genellikle kiracı belirsiz sözleşmelerde ayrılma konusunda daha özgürdür, ev sahibi sözleşme koşullarına mutabık kalarak bildirim (ihbar) sürecine uymak zorundadır (Whitehead vd., 2012).

Barınma güvencesinin seviyesi ne olursa olsun, ev sahipleri eğer gerekiyorsa konutunu bir akrabanın/yakınının kullanımı için tahsis etmesi ve bazı büyük yenilemeler gibi belirli durumlarda sözleşme feshedilebilir. Ancak feshedebilmek için bildirim süreleri içinde ev sahibinin kiracıya durumu bildirmesi gerekmektedir ve hatta maddi tazminat ödemesi gerekebilir. Kira düzenlemelerinde olduğu gibi, kiracılığın düzenlenmesi sözleşmeler ve her iki tarafın da hakları açısından ülkeler arasında farklılıklar bulunduğu için ülkelerin karşılaştırılmasında barınma güvencesinin derecesini belirlemek kolay değildir (Whitehead vd., 2012).

Konut kalitesi düzenlemeleri

Konut kalitesinin yönetimine ilişkin düzenlemeler genellikle güvenlik ve yeterli bina ve standartların sağlanmasını hedeflemektedir. Bu standartlar, ekonomik büyüme ve genel yaşam standartlarında gelişmeler ile artış eğilimindedir. Kalite ile ilgili düzenlemeler belirli bir konut kullanım biçimi ile ilgili olmayıp tüm kullanım biçimlerini kapsar (Whitehead vd., 2012). Konut kalitesi ile ilgili düzenlemelerin yürürlüğe konmasının ana nedenlerinden biri de özel kiralık mülklerin minimum düzeyde güvenliğinin sağlanmasını garanti altına almaktır (Whitehead vd. , 2012; Tang, 2013). Gelişmiş ekonomilerin çoğunda, konut standartlarına ilişkin temel gerekli kriterler oluşturulmuştur (Whitehead vd., 2012).

Birçok ülke mevcut konut stokunun sürdürülebilmesi ve korunması için ev sahiplerini teşvik eden güçlü devlet girişimlerine ilişkin uzun bir tarihe sahiptir. Örneğin 2005 yılında Fransa'da ev sahiplerinin konutlarını yenilemeleri için, yenileme sübvansiyonları ve vergi indirimleri uygulanmaya başlanmıştır (Ball, 2011). Diğer bir deyişle hükümet sübvansiyonları ve vergi indirimleri (belirli standartları karşılamaya koşullu) kaliteyi yükseltmek için ev sahiplerine teşvikler sağlamakta, salt düzenleme aracılığıyla zorunlu hale getirilmemektedir (Whitehead vd., 2012).

Dünyada Özel kiralık Konut Sektörüne Yönelik Düzenlemeler

Özel kiralık konut düzenlemelerinin, özellikle İkinci Dünya Savaşı'ndan bu yana geliştiği görülmektedir. Günümüzde Avrupa'nın Danimarka, Hollanda gibi sosyal hakların güçlü olduğu ülkelerde özel ve sosyal kiralık konut sektörleri arasında kalite ve çekicilik en aza indirgenerek kiralar arasındaki fark minimize edilmeye çalışılmaktadır (Kemeny, 1995; 2006). Buna karşın güçlü neoliberal eğilimlerin hâkim olduğu İngiltere gibi ülkeler, kiralık konut piyasalarında ayrı düzenlemeleri benimsemiştir. Neoliberal eğilimli

ülkeler, daha az düzenlenmiş özel kiralık konut sektörü ve sıkı kontrollü sosyal kiralık konut sektörü ile karakterize edilir (Tang, 2013).

Özel kiralık konut sektörü içindeki farklı kira düzenlemelerine sahip ülkelerin düzenleme gücünü karşılaştıran Tablo 5 incelendiğinde, özel kiralık konutun düzenleyici çerçevesinin İngiltere, Finlandiya ve Norveç'te genellikle zayıf ve sınırlı olarak algılandığı görülmektedir. Almanya, Danimarka, Fransa, İspanya, İsveç ve İsviçre'de ise özel kiralık konut sektörüne yönelik düzenlemelerin önemli ve belirleyici bir etkiye sahip olduğu görülmektedir. En güçlü özel kiralık konut düzenlemelerine sahip ülke Hollanda'dır. Bu durum, ülkenin sosyal demokrat refah rejimine sahip olması ile yakından ilişkilidir (Tablo 5).

Tablo 5. 2000'li yıllarda düzenlemelerin düzeyine(gücüne) genel bir bakış

Ülkeler	Başlangıç (ilk) kirası	Kira artışları	Kiralama uzunluğu	Kira feshi	Mülkün satışı	Uygulamada karşılaşılan sorunlar	Düzenleyici çerçevenin genel algısı
Almanya	Orta	Orta	Yüksek	Orta	Orta	Orta	Önemli/belirleyici
Danimarka	Düşük	Orta	Yüksek	Orta	Yüksek	Orta	Önemli/belirleyici
Finlandiya	Düşük	Düşük	Yüksek	Düşük	Düşük	Orta	Sınırlı
Fransa	Düşük	Orta	Orta	Orta	Düşük	Yüksek	Önemli/belirleyici
Hollanda	Yüksek	Yüksek	Yüksek	Orta	Orta	Orta	Güçlü
İngiltere	Düşük	Düşük	Düşük	Orta	Orta	Orta	Sınırlı
İspanya	Düşük	Orta	Orta	Orta	Orta	Yüksek	Önemli/belirleyici
İsveç	Orta	Orta	Yüksek	Orta	Orta	Orta	Önemli/belirleyici
İsviçre	Düşük	Orta	Yüksek	Orta	Düşük	Düşük	Önemli/belirleyici
Norveç	Düşük	Orta	Orta	Düşük	Orta	Yüksek	Sınırlı

Kaynak: Whitehead vd. (2012, s.20) ve Tang (2013) 'den yararlanılarak oluşturulmuştur.

Kira düzenlemeleri ve kira başlangıç ayarlamaları açısından farklılıklara bakılacak olursa başlangıç kiraları ya da kira artışlarına dayalı olarak düzenlemeler iki biçimde olabilmektedir. Örneğin İsveç'te özel kiralık konut sektörünün başlangıç kiraları sosyal kiralık konut sektörünün kiralarına bağlı olarak düzenlenmektedir. Sosyal kiralık konut kiralarını dikkate alan bu yaklaşım ile kiralık konut piyasası dengelenmektedir. Bu yaklaşıma sahip ülkelerde (Hollanda vb.) güçlü ve belirleyici bir kira düzenleme çerçevesinin olduğu görülmektedir. Buna karşın daha zayıf kira düzenlemelerine yaklaşımına sahip ülkelerde (Finlandiya vb.) özel kiralık konut başlangıç kiraları düzenlemeye tabi değil ve serbestçe düzenlenmektedir (Ball, 2011).

Kira düzenlemelerinde kontrol mekanizmaları birçok şekillerde olabilir. İsveç'te kira artışları her yıl müzakere edilir ve özel kira artışları sosyal konut sektöründeki kira artışları ile bağlantılıdır. Almanya'da ve Norveç'te kiralar, belirli bir zaman noktasında yerel kira düzeylerini yansıtacak şekilde revize edilebilmektedir (Whitehead vd., 2012). Hollanda'da 1979 yılında yürürlüğe giren Konut Kiracılığı (Residential Tenancies) Yasası'na göre kiralar yılda bir kez artırılabilir ve bu artış devletin belirlediği orandan daha fazla olamaz. Bu yasa, öngördüğü kira kontrolüne ek olarak, konut kalitesine göre en yüksek kira değerinin belirlenmesi için "birim değer sistemi" (point value system) öngörmüştür. Ancak bu kurallar, kirası sadece belirli bir seviyeden düşük konutlar için

geçerlidir (Sarıoğlu, 2007). İsviçre'de eğer ev sahibinin maliyetleri artmaya başlarsa kira artışına izin verilmektedir. İspanya'da ise yıllık kira artışı genel yaşam indeksi maliyetine bağlı olarak artmaktadır (Whitehead vd., 2012).

Bazı ülkeler kira artışlarının düzenlenmesinde bu farklı biçimlerin bir kombinasyonunu kullanmaktadır (Whitehead vd., 2012). Örneğin Almanya'da başlangıç kiraları serbest olarak düzenlenebilmektedir ancak kiralar aynı bölgedeki kiralarla karşılaştırabilir düzeyde olmalıdır ve kira oranları söz konusu bölgedeki kiraların oranını %20'den fazla geçmemelidir, aksi takdirde bu bir suç teşkil etmektedir (Kemp ve Kofner, 2010, Whitehead vd., 2012). Kiracılık süresince kiralar yerel düzeyin altında ise sadece iki yılda bir, en fazla % 20 oranında arttırılabilir (Ball, 2011; Whitehead vd., 2012). İsveç'te ise kira sözleşmeleri serbestçe düzenlenir. Fakat Almanya'da olduğu gibi kiracıların sorgulama hakkı vardır (Tang, 2013).

Günümüzde Avrupa'da baskın olan kira düzenlemeleri üçüncü kuşak kira kontrollerinin versiyonları olsa da (O'Sullivan ve De Decker, 2007) farklılıklar olabilmektedir. Bununla birlikte kiralar genellikle artan maliyet (bakım ve işletme) ve enflasyonla yakından ilişkilidir. Finlandiya ve İrlanda'da kira artışları üzerinde resmi bir düzenleme yoktur. Buna karşın, belirleyici ve güçlü sistemlerde (Tablo 5) kira düzenlemeleri sıkıdır ve kiralık konut pazarı kısmen serbesttir. Örneğin, Danimarka ve Hollanda'da 1991 sonrası inşa edilen pahalı gayrimenkullerin piyasa kiralarını şarj etmelerine izin verilmiştir ve yüksek değerli gayrimenkullerin kira artışları ile ilgili kısıtlama yoktur (Tang, 2013).

Barınma güvencesi açısından ülkeler incelendiğinde, Avrupa ülkeleri arasında kiracılara verilen kiralama süresinin farklı olduğu görülmektedir. Örneğin Fransa ve Norveç'te üç yıl, İrlanda'da dört yıl, İspanya'da beş yıldır (Haffner vd., 2007; Tang, 2013). Almanya, Avusturya ve Hollanda'da başlangıçta (belirsiz bir tarihe varana kadar) uzun vadeli sözleşmeler ile çok sıkı güvenlik vardır. Almanya'da, Hollanda'da olduğu gibi kiracı hanehalkları ve yaşlılar özellikle güvence altındadır ve düzenlenmiş kiralar ile yönetilir (Scanlon, 2011). Danimarka, Finlandiya, İsveç ve İsviçre'de kira sözleşmeleri belirsizdir ya da herhangi bir süre ile sınırlandırılmamıştır, kiracının talebi üzerine tekrar yenilenir (Haffner vd., 2007; Tang, 2013). İngiltere ise "Garantili Kısa Dönemli Kiracılık" adı altında altı aylık bir güvence ile en kısa kiralama süresi sunan bir yapıdadır (Scanlon,2011; Tang, 2013). Güvenli dönemde, sözleşmede yan bir madde olmadığı sürece ne kiracı ne de ev sahibi bir bildirim verebilir. Belirli bir süre sona erdikten sonra özel bir neden olmaksızın, ev sahipleri iki ay önceden kiracı da bir ay önceden bildirimde bulunabilir (Tang, 2013). Avrupa ülkeleri dışında Amerika ve Avustralya'da da kira sözleşmeleri belirlidir ve ev sahibinin yenileme zorunluluğu yoktur (Scanlon,2011).

Ev sahiplerinin mülkiyet (sahiplik) kapasitesi ve kiracı tahliyesi açısından bir değerlendirme yapılacak olursa, İngiltere en kısa dönemli güvenli kiracılığa sahip olduğu için, özel ev sahipleri mülklerinin kullanımı üzerinde en güçlü kontrole sahiptir. Finlandiya, Almanya, İsveç ve İsviçre, Hollanda'da kiracılık süresi belirsizdir. Bu ülkelerde ev sahipleri hala, aile için kullanım gerekliliği, iyileştirme ya da yıkım gerekliliği ya da piyasada boş bulunduğu için satmak gibi belirli koşullar altında mülklerini yeniden elde etmek kapasitesine sahiptir. Çünkü serbest piyasada mülk satılacağı zaman, kiracıların İngiltere hariç, Avrupa'nın pek çoğunda mülkün satışını reddetme hakkı vardır (Ball, 2001; Tang 2013). Ayrıca Almanya, Hollanda ve Belçika'da kiralık bir birimin satılması yeni ev sahibini bağlar ve kiracıyı etkilemez (Scanlon, 2011). Danimarka'da ise ev sahipleri kiralık mülklerinin satışında en az güce sahiptir. Çünkü mülkiyetin kullanım biçimi genellikle sabittir. Ayrıca başlangıçta binalar "kalıcı olarak" kiralık konut biçiminde belirlenmiştir. Bu nedenle kiralık konutlar bireysel

birimler olarak, ev sahiplerince satılamaz. Sadece kiralık yapılarda altıdan fazla birim varsa kiracılara piyasa fiyatından satılabilir. Benzer biçimde, Amerika'da San Francisco dahil olmak üzere kiralık apartman (kondominyum) birimlerinin satışı kısıtlıdır. Bu sınırlamaların amacı erişilebilir kiralık birimlerin kaybını önlemektir. Belediyenin kira kontrol mevzuatı oturan kiracıların kiralarını düşük tutar ancak ev sahiplerinin karları ile sınırlıdır (Scanlon, 2011).

Avrupa'da pek çok ülkede özel ev sahipleri, kira ödenmemesi ya da sözleşme (kontrat) koşullarına uyulmaması durumunda tahliye gücüne sahiptir. Ancak genellikle tahliye işlemleri, karmaşık, maliyetli ve zaman alıcı bulunmaktadır. Örneğin İspanya'da ev sahipleri yasal sistem içinde çok az güvene sahiptir ve kiracının ödeme yapmadığı durumlarda tahliyesi ile ilgili maliyetler çok pahalıdır (Tang, 2013). Tang'e (2013) göre kiracı ve ev sahibi arasındaki çıkarları dengelemek için uzun dönemli bir kiracılık içinde kira artışları bir indekse bağlanabilir. Böylece ev sahipleri sürekli ve makul gelire sahip olurken, kiracılarda uygun fiyatlı ve daha uzun süreli bir barınma olanağına kavuşur. Çünkü, uzun dönemli ve ödemelerini tam zamanında yapan kiracı, kiralık konut sisteminde ev sahipleri için güvenli bir kazanım olarak görülmektedir (Whitehead vd., 2012).

Yukarıda Tablo 5. de görüldüğü gibi, genel olarak İngiltere'de düzenlemeler zayıftır ve özel ev sahiplerinden yanadır. Çünkü kira artışları ve üzerinde kısıtlama yoktur ve kiracılığı istedikleri zaman sonlandırabilen esnekliklere sahiptir. Buna karşın Hollanda'da düzenleme sistemleri güçlüdür ve özel kiracılardan yanadır. Çünkü kiralar piyasa kiralarının altında ve uzun dönemli barınma güvenliği vardır (Tang, 2013). Bu durumun, liberal ve sosyal refah devletlerinin konut ve kiralık konut politikalarına bakışının bir yansıması olduğu söylenebilir. Çok sıkı düzenlemelere sahip Hollanda'da özel kiralık konut sektörünün sınırlı bir büyümesi olduğu görülmektedir. Bu güçlü sosyal kiralık konut politikalarının yanı sıra son zamanlarda tüm dünyada olduğu gibi mülk konutu destekleyen politikalarla da ilgilidir.

Almanya ve İsviçre'de özel kiralık konut sektörü oranı yüksektir. Her iki ülkede de mülk konuta erişimin sınırlı olması özel kiralık konut talebini sürdürmede yardımcı olmuştur. Aynı zamanda özel kiralık konut sektörü içindeki yatırımı teşvik eden mali teşvikler (örneğin ev sahiplerine yönelik vergi indirimleri, yeni özel kiralık konut arzını desteklemek için inşaat firmalarına sübvansiyonlar, yenileme sübvansiyonları vb.) kurumsal ev sahiplerinin yanı sıra bireysel ev sahiplerinin özel kiralık konut arzının sürdürülebilmesini sağlamaktadır (Tang, 2013). Bu bağlamda Hollanda, Almanya ve İsviçre örnekleri göz önüne alındığında düzenleme sistemlerinin güçlü ya da zayıf olmasının sektörün büyüklüğü ile değil politikalarla ilgili olduğu söylenebilir. Hollanda Avrupa'da oldukça az rastlanan örnek bir ülke olarak ev sahipliği ve kiracılığı farklı politikalar ile desteklemektedir. Konut yardımı ve İkinci Dünya Savaşı'ndan beri devam eden kira denetimi uygulamaları kiracılığın desteklenmesinde önemli role sahiptir. Diğer taraftan, ev sahipleri için gelişmiş bir ipotekli kredi sistemi ve bu sistem içinde faiz giderlerinin tamamının gelir vergisinden düşülebilmesi gibi olanaklar mevcuttur (Sarıoğlu, 2007).

Diğer Düzenlemeler ve Sübvansiyonlar

Kira yardımları, özel kiralık konut sektöründe önemli sübvansiyonlardandır. Örneğin İngiltere formel bir kira düzenlemesine sahip olmasa da özel kiralık konut piyasasının en alt kesimi için dolaylı bir kira kontrolü vardır (Whitehead vd., 2012; Tang, 2013). Bu durum, düşük gelirli hane hanehalklarına uygun kira seviyelerinin sınırlı olmasından kaynaklanmaktadır (Whitehead vd., 2012). Bu kiracılar genellikle konut (kira) yardımından yararlanırlar. Hatta Wilcox and Perry'nin (2013) çalışmasına göre özellikle bu alt sektörün hakim olduğu alanlardaki ev sahipleri "Yerel

Konut Yardımlarını" düşük düzeyde yansıtacak şekilde kiralarını ayarlamaya gönüllüdürler (Tang, 2013).

İngiltere'nin yanı sıra hem özel hem de sosyal kiralık konuta yönelik kira yardımı Hollanda, Danimarka, Norveç, Finlandiya, Almanya ve İsveç'te de yer almaktadır (Whitehead vd., 2012). Pomeroy ve Godbout'a (2011) göre bu yöntemle, doğrudan sosyal konut ev sahipleri için sağlanan sübvansiyonların olduğu ülkelerdeki hakim rekabetin önlenmesi istenmektedir. Bu sübvansiyon sistemleri aynı zamanda kiralık konut arzını tevsik etmek içindir (Pomeroy ve Godbout, 2011).

İngiltere'de özel kiralık konut sektörü içindeki kiracıların %35'i yerel konut kira yardımlarıyla desteklenmektedir. Bu kira yardımları, yerel bölgedeki medyan kiralara ve konut büyüklüğüne (ülke çapında) dayalıdır. Ancak bu durum Londra'nın merkezi dâhil olmak üzere, yüksek fiyatlı alanların dışındaki fiyatları da artıracağı endişesini taşımaktadır. Hükümet, yerel konut kira yardımı ile doğrudan ev sahipleri için ödeme imkânı sunarak geçici olarak kiraları azaltma teşviki içindedir (Scanlon,2011). Hollanda'da 1990lar itibariyle, kullanıcıya özgü yardımlar hanehalkının gelirine, hanehalkı büyüklüğüne (bir kişilik-iki ve daha fazla kişilik ve 65 yaş ve üzeri-65 yaş altı) konutun kirasına bağlı olarak belirlenmektedir. Sadece en yüksek kira seviyesi (liberalisation limit) altındaki konutlar için kira yardımı yapılmaktadır. Ayrıca, geliri belirli bir seviyenin üzerinde olan hanehalkları da yardımdan yararlanamamaktadır (Sarıoğlu, 2007). Sınırlı sosyal kiralık konuta sahip olan İspanya'da ise kira yardımı sadece belirli bölgelerde özel kiralık konut için yapılmaktadır (Whitehead vd., 2012). Avrupa ülkelerinin dışında Kanada'da kiralar yıllık enflasyon indeksine bağlı olarak piyasa koşullarına göre artmaktadır. Kanada'da düşük gelirli hanehalkları ile ev sahipleri arasında bir sözleşmeye bağlı olarak, doğrudan ev sahiplerine verilmek üzere kira takviyesi yapılmaktadır. Hanehalkı, gelirinin % 30'unu kira olarak ödemektedir ve piyasa değeri arasındaki fark bunun üzerine eklenmektedir. Ayrıca yardım programı çerçevesinde kalitesiz konutu desteklemediği için konutların asgari yaşam standartları taşıması koşuluyla kiracılar seçtikleri bir konutta oturabilir. Ev sahibi ile bir sözleşme olmaksızın, bu kiracılara da gelirlerinin yüzde %30'u ile kira piyasa değeri arasındaki farkın %60-70'i kadar yardım ödenmektedir (Pomeroy ve Godbout, 2011). Kira yardımları uygun ya da erişilebilir fiyatlı kiralık konutlar açısından önemli bir avantajdır. Bu nedenle geniş bir mevcut kiralık konut stokuna sahip olan Amerika ve Kanada gibi ülkelerde etkilidir. Fakat Pomeroy ve Godbout'a (2011) göre bu ülkelerde kira yardımlarının belirli mülk özelliklerine bağlı olması ve konut harcamalarına ek bir gelir sağlaması nedeniyle daha düşük gelirli aileler için uygun ya da yeterli olmamaktadır.

Bazı ülkelerde sübvansiyonlu kredi veya vergi indirimleri mevcuttur. Örneğin Fransa'da "scellier" adlı bir vergi indirimi uygulamasıyla yeni kiralık konutun değerinin % 13-22'si arası bir gelir vergi indirimi sağlanmaktadır. Kira tavan fiyatlarınının değişimine (yükseltebilmek) en az dokuz yıl sonra izin verilmektedir. Danimarka'da özel kurumsal yatırım teşvikleri (emeklilik ve sigorta şirketleri) için tasarlanmış bir vergi vardır ve sadece bu düşük kiralara bağlı değildir. 2002'den bu yana, normal şirketlerin kazanç vergileri % 30 üzerinden değerlendirilirken, özel kiralık konut sektörüne yönelik yatırımların kazançları % 15 ile vergilendirilmektedir (Scanlon, 2011).

Vergi uygulamaları her ülkede değişebilmektedir. Ancak, Danimarka, İspanya, Hollanda, Almanya, ABD, Avustralya diğer gelirlere karşı kiralama kayıplarına karşı kiralama zararlarını önlemek için ev sahiplerine bir dizi vergi teşviki sunmaktadır (Scanlon, 2011) (Tablo 6). Benzer uygulama Yeni Zellanda'da söz konusudur (Pomeroy ve Godbout, 2011). Kiralık gayrimenkul gelir vergisi de yaygın olarak değişmektedir. Bazı ülkelerde uzun vadeli yatırımı teşvik etmek için ya da düzenlenmek için sermaye gelir

vergisi oranı düşmektedir (Scanlon, 2011). İngiltere'de böyle bir uygulama yoktur. Pomeroy ve Godbout'a (2011) göre gelir vergisi indirimi kurumsal yatırımcılara göre küçük yatırımcılar üzerinde daha önemli bir etkiye sahip olma eğilimindedir. Bunlardan başka Avusturya ve Almanya'da da özel bireysel ev sahipleri on yıl sonra vergisiz kiralık konut mülkü satabilirler (Scanlon, 2011).

Tablo 6. Kira gelirlerinin, gelir vergisi uygulamaları

Ülkeler	Kira Gelirlerinde Düşük Vergi	Morgıç Faiz İndirimi	Maliyetin Vergiden Düşürülmesi	Amortisman Payı	Kiralama kayıpları diğer gelirlere karşı
İngiltere	Yok	Var	Var	Yok	Yok
Avusturya	Yok	Var	Var	Düşük gelire yönelik kiralık birimler için	Yok
Danimarka	Sadece kurumsal yatırımlara	Var	Var	Yok	Var
Hollanda	Yok	Var	Var	Var	Var
Almanya	Yok	Var	Var	Var	Var
İspanya	Var	Var	Var	Yok	Var
Avustralya	Yok	Var	Var	Sadece yeni yapılarda	Var
ABD	Yok	Var	Var	Var	Var(sınırlı)

Kaynak: Scanlon, K.. Private Renting in Other Countries. 2011, Scanlon K. & Kochan B. (eds.), Towards a Sustainable Private Rented Sector: The Lessons from Other Countries, LSE London, s.26.

Özel kiralık konut sektörünün desteklenmesinde, Almanya, İngiltere, Avusturya, Hollanda, İspanya, Kanada, ABD'de de olduğu gibi piyasanın altında faiz oranları (Pomeroy ve Godbout, 2011; Scanlon, 2011) Almanya, Hollanda, Kanada'da olduğu gibi bağışlanabilir vergiler ve hibeler de etkilidir (Pomeroy ve Godbout, 2011).

Bunların dışında bazı ülkelerde, gayrimenkul yatırımlarını teşvik etmek için özel vergi tasarruflu araçlar geliştirilmiştir. Bunlar ABD'de GYO olarak bilinen gayrimenkul yatırım ortaklıklardır. Benzer biçimde İngiltere'de 2007 yılından bu yana özel kiralık konut sektörü içinde kurumsal yatırımı teşvik etmek için izin verilmiştir. 2011 yılında İngiliz Gayrimenkul Federasyonu yirmi üç GYO listelemiş ve bunların sadece bir tanesi konut yatırımıdır. ABD'de de GYO fonlarının yaklaşık % 15'i konut emlak yatırımıdır. ABD ve İngiltere'nin yanı sıra Finlandiya ve İspanya'da da GYO tipi araçları sağlamak için yeni mevzuat geçmiştir (Scanlon, 2011).

Bakım ve yönetim açısından, pek çok ülkede özel kiralık konutun bakımından başlıca ev sahibi sorumludur. İngiltere'deki özel kiralık konut sektörü içindeki ev sahiplerinin çoğu mülklerinin bakımlarını bir emlakçı vb. bir kuruluşa yaptırmaktadır. Özelleşmiş bakım firmaları vardır ve bazı kiracılık girişimleri kendi bakımlarını karşılayacak personele sahiptir (ABD'de yaygındır, İngiltere'de sosyal konutta yaygındır). Bakımın kalitesi profesyonel yönetim kuruluşlarının kullanılmasına bağlı değildir. Örneğin Almanya'da hem özel hem de profesyonel ev sahipleri konut stokunu iyi durumda tutarken, küçük özel ev

sahiplerinin de en iyisini yapmaya çalıştığı kabul edilir. Avusturya'da ise özel kiralık konut sektörü belediye organları tarafından kontrol edilir ve enerji tasarrufu iyileştirmeleri için yüksek sübvansiyonlar alır. Bunlardan başka yasal olarak özel kiralık konut ev sahiplerinin bakım ve onarım masraflarını karşılamak için brüt kira yüzdesinin bir kısmını ayırması gerekmektedir.

SONUÇ

Liberal politikaların hakim olduğu küreselleşme sürecinden tüm dünya etkilenmektedir. 1980 sonrası yaşanan değişimler tüm dünya ülkelerinin konut ve kiralık konut politikalarını da etkilemiştir. Buna bağlı olarak günümüzde kamu giderek konut sektöründen çekilmekte ve gelire yönelik kira konut yardımları ile devlet müdahalesini azaltan (sosyal kamu konutlarının özelleştirilmesi, yetkilerin desantralize edilmesi) piyasaya daha fazla güvenen politikalar izlenmektedir.

Farklı ülkelerin (gelişmiş) özel kiralık konut sistemlerini, özel kiralık konut arz ve talebini oluşturan temel aktörleri, özel kiralık konut sektörüne yönelik düzenlemelerini aktaran bu çalışma ile İngiltere gibi liberal refah devletlerinde özel kiralık konut sektörüne yönelik düzenlemelerin, zayıf ve ev sahiplerinden yana kiracıların düşük barınma güvencesine sahip olduğu görülürken, özel kiralık konut üretiminin sınırlı olduğu Hollanda gibi sosyal refah devletlerinde özel kiralık konut sektörüne yönelik düzenlemelerin güçlü ve özel kiralık konut sektörü içindeki kiracılardan yana özellikle kira yardımları ile yüksek barınma güvencesine sahip olduğu görülmektedir. Ayrıca Almanya, İsviçre gibi gelişmiş ülkelerde de özel kiralık konut sektörü içinde ev sahiplerine yönelik vergi indirimleri, yeni özel kiralık konut arzını desteklemek için inşaat firmalarına sübvansiyonlar, yenileme sübvansiyonları vb. sübvansiyonlarla özel kiralık konut arzının sürdürülebilmesinin sağlandığı görülmektedir. Özetle farklı ülkelerdeki özel kiralık konut düzenleme sistemlerinin güçlü ya da zayıf olmasının özel kiralık konut sektörünün büyüklüğü ile ilgili olmadığı konut politikaları ve yaklaşımları ile ilgili olduğu görülmektedir.

Bir konut piyasası kiralık konut piyasası ile bütündür. Gelişmiş ülkelerin kiralık konut sistemlerinde sosyal ve özel kiralık konutun bir arada yer aldığı görülmektedir. Buna karşın Türkiye gibi gelişmekte olan ülkelerin pek çoğunda sosyal kiralık konut deneyimlerinin başarısız olduğu ya da sosyal kiralık konutun hiç yer almadığı ve kiralık konut arzının serbest piyasa koşullarında kendiliğinden geliştiği görülmektedir. Gelişmiş ülkelerde giderek sosyal konut programlarının azalması buna bağlı olarak niceliksel olarak talebi karşılayamaması, hanehalklarının küçülmesi, daha genç bireyler ve daha mobil hanehalkları için daha uygun olması; gelişmekte olan ülkelerde ise düşük gelir grubu hanehalklarının barınabilmesini sağlayan tek seçenek olması, günümüzde hem gelişmiş hem de gelişmekte olan ülkelerde özel kiralık konut sektörünü öngörülenden daha fazla öne çıkarmaktadır. Bu özellikleri ile özel kiralık konut sektörünün hanehalkları için mülk ya da sosyal kiralık konuta yönelik güçlü bir alternatif olacağı görüşü artmaktadır. Serbest piyasa koşulları içinde kendiliğinden doğan kiralık konut arzına sahip, sosyal ve özel kiralık konut sistemlerinin bir arada olmadığı doğrudan özel kiralık konut sektörünün yer aldığı ya da öne çıktığı Türkiye vb. ülkelerde fırsat eşitliğinin sağlanabilmesi için güçlü özel kiralık konut sistemlerine sahip gelişmiş ülkelerin deneyimlerinden yararlanılabilmesi bu ülkelerdeki kiralık konut sisteminin işleyişi, sürdürülebilirliği ve toplumun tüm katmanlarına erişebilirliğini güçlendirmesi açısından önemlidir. Bu nedenle Türkiye gibi gelişmekte olan ülkelerde etkin ve güçlü özel kiralık konut politikaları ve düzenlemelerinin ortaya konulabilmesi iyi ve gelişmiş bir konut sisteminin gerekliliğidir.

Teşekkür

Bu makale "Türkiye'de Kiralık Konut: Ankara Örneğinde Talep ve Kullanım özellikleri Ankara'da Kiralık Konut Talebi: Kiracı Hane halklarının özellikleri" başlıklı ve 2011FB-DO31 Kodlu Yüzüncü Yıl Üniversitesi Doktora Tezi Bilimsel Araştırma Projesinden yararlanılarak gerçekleştirilmiştir.

KAYNAKLAR

1. AKALIN, M. Sosyal Konutların Türkiye'nin Konut Politikaları İçerisindeki Yeri ve TOKİ'nin Sosyal Konut Uygulamaları. *Fırat Üniversitesi Sosyal Bilimler Dergisi*, 26(1):107-123, 2016.
2. ARNOTT, R. Tenancy Rent Control, *Swedish Economic Policy Review*, 10: 89-121, 2003.
3. BALL, M. European Housing Review, London: RIC, 45-60, 2011.
4. BALLESTEROS, M.M. Rental Housing for Urban Low-Income Households in the Philippines, *Philippine Institute for Development Studies*, 47(1): 1-20, 2004.
5. DOLING, J. & Ford, J., A Union of Home Owners, *European Journal of Housing Policy*, 7 (2): 113-127, 2007.
6. ELLİNGSEN, T., ENGLUND, P. Rent regulation: An introduction. *Swedish Economic Policy Review*, 10(1): 3-10, 2003.
7. EMÜR, A. Urban Rental Housing and Tenant Households In Turkey: Towards Viable Alternative Policies For The Rental Sector. Yayınlanmamış Yüksek Lisans Tezi. City and Regional Planning, Middle East Techinal University, 1999.
8. GILBERT, A. Rental housing: An Essential Option For The Urban Poor In Developing Countries, UNHABITAT, 83-85, 2003.
9. HAFFNER,M., ELSINGA, M., HOEKSTRA, J. Balanca Between Landlord and Tenant? A Comparison of The Rent Regulation In The Private Rental Sector In Five Countries. *ENHR International Conference on vSustainabile Urban Area*, Rotterdam, 2007.
10. KELEŞ, R. Kentleşme Politikası, 10. Baskı, İmge Kitabevi, Ankara, 120, 2010.
11. KEMENY, J. Corporatism and Housing Regimes. *Housing, Theory and Society.* 23(1): 1-18, 2006.
12. KEMENY, J. From Public Housing to The Social Market : Rental Policy Strategies in Comparative Perspective, London : Routledge, 194, 1995.
13. KEMP, P.A, KEOGHAN, M. Movement Into And Out of The Private Rental Sector In England. *Housing Studies.* 16(1**)**: 21-37(2001).
14. KEMP, P.A. and KOFNER, S. Contrasting varieties Of Private Renting: England and Germany, *International Journal of Housing Policy*. 10(4): 379-398, 2010.
15. LİND, H. Rent Regulation: A Conceptual and Comparative Analysis. *European Journal of Housing Policy.* 1/1: 41-57, 2001.
16. LIPSEY, R., STEINER, P., PURVIS, D., COURANT, P. İktisat 1, Bilim ve Teknik Yayınevi, Ankara, 150-170, 1984.
17. O'SULLİVAN, E., DE DECKER, P. Regulating the Private Rental Housing Market in Europe. *European Journal of Homelessness.* 1: 95-116, 2007.
18. OXLEY,M., SMITH, J. Housing Policy and Rented Housing Europe, E and FN Spon, London, 3-4;17-18;25, 1996.
19. PEPPERCORN, I.G., TAFFIN, C. Rental Housing Lessons from International Experience and Policies for Emerging Markets, The World Bank Washington DC, 71;98;103;127, 2013.
20. PITTINI, A., LAINO, E. Housing Europe Review 2012 : The Nuts and Bolts of European Social Housing Systems, CECODHAS Housing Europe Observatory, Brussels, 22-30, 2011.
21. POMEROY, S., GODBOUT, M. Development of the Rental Housing Market in Latin America and the Caribbean, Inter American Development Bank, No. IDB-DP-173 , 1-2, 2011.
22. SARIOĞLU, G. P. Hollanda'da Konut Politikaları ve İpotekli Kredi Sistemi, *METU JFA.* 27(2): 1-16, 2007.
23. SCANLON, K. Private Renting in Other Countries. LSE London, 15-44, 2011. [Editorler: SCANLON K., KOCHAN B. Towards a Sustainable Private Rented Sector: The Lessons from Other Countries].
24. SCANLON, K., WHITEHEAD, C. M. E.International Trends in Housing Tenure and Mortgage Finance, Council of Mortgage Lenders, London, 17, 2004.
25. SCANLON, K., FERNÁNDEZ, A. M. , WHITEHEAD, C. M. E. Social housing in Europe. *European Policy Analysis.* 17: 1-12, 2015.
26. ŞAHİN,Y. Kira Denetim Politikası Üzerine Bir Değerlendirme. *Ankara Üniversitesi SBF Dergisi*. 60(4): 213-247, 2005.
27. ŞİMŞEK, S.,Taşınmaz Kiralamaları ve Sınırlamaları. *İstanbul Barosu Dergisi*, 84(5): 2855-2898, 2010.
28. TANG, C.P.Y. Could regulation benefit the English private rented sector? Experience from Europe, Preliminary Draft, *WS*-22: Private Rented Markets, *ENHR 2013 Conference*, 2013.
29. TUTİN, C.Social Housing and Private Markets: From Public Economics to Local Housing Markets. LSE London,47-61, 2008. [Scanlon, K., Whitehead C .M.E..Social Housing In Europe II: A Review of Policies and Outcomes].
30. TÜREL, A., Türkiye'de Devletin Konut Sektörünü Destekleme Mekanizmaları, *Planlama 97/1.* 43-48, 1997.
31. UNCHS.Rental Housing: An Essential Option for The Urban Poor in Developing Countrie, Nairobi: UNCHS, 173,2003.
32. UNHCS.National Trends in Housing-Production Practices., Nairobi:UNHCS, 4, 1993.
33. WHITEHEAD, C.M.E., MARKKANEN, S., MONK, S., SCANLON, K, TANG, C.P.Y. The Private Rented

Sector in the New Century – A Comparative Approach, Denmark, Cambridge Centre for Housing and Planning Research and LSE London, 17-40, 2012.

34. Wits University. Section 1 International Review, Project Develeop A Rental Housing Policy an Rental Subsidy Program Report, South Africa, 4-32, 2009.

http://dergipark.gov.tr/tujes
Trakya University Journal of Engineering Sciences, 18(1): 73-83, 2017
ISSN 2147–0308
Derleme Makale / Review Article

A REVIEW ON NANOEMULSIONS: PREPARATION METHODS AND STABILITY

Kadir ÇINAR

Department of Food Engineering, Trakya University, Edirne, Turkey

Abstract: There is a growing interest for using of nano/sub-micron particles in the technology of pharmaceutical, cosmetic and also food. Especially, this interest has been increasing parallel with better emulsification techniques and stabilization mechanisms. There are two main groups of nanoemulsion preparation methods, namely high-energy and low-energy spontaneous emulsification methods. Preparation processes and components used are significant parameters that affect stability from few hours to years. Problems such as creaming, coalescence sedimentation and flocculation are not concern for nanoemulsions due to their small droplet size. However, the main destabilization mechanism is Ostwald ripening for them. In this paper, a comprehensive review is presented to give basic ideas about nanoemulsions, their preparation methods, and stability aspects.

Keywords: Nanoemulsion; preparation methods; stability; Ostwald ripening

NANOEMÜLSİYONLAR ÜZERİNE BİR DERLEME: HAZIRLAMA METOTLARI VE STABİLİTELERİ

Özet: İlaç, kozmetik ve gıda teknolojilerinde nano partiküllerin kullanılmasına yönelik gittikçe artan bir ilgi mevcuttur. Bilhassa, bu ilgi emülsifikasyon tekniklerinin ve stabilizasyon mekanizmalarının iyileşmesine paralel şekilde artmaktadır. Nanoemülsiyonların hazırlanmasına yönelik yüksek enerjili ve düşük enerjili-spontane olmak üzere farklı tipte metotlar vardır. Hazırlık süreçleri ve kullanılan bileşenler, stabilitenin birkaç saatten yıllara kadar sürmesini etkileyen önemli parametrelerdir. Nanoemülsiyonlar küçük parçacık boyutuna sahip olduklarından kremleşme, koalesans, sedimantasyon ve flokülasyon gibi problemlere maruz kalmazlar. Fakat Ostwald olgunlaşması nanoemülsiyonların destabilizasyonuna neden olan temel mekanizmadır. Bu derleme çalışmada, nanoemülsiyonlar hakkında temel bilgiler verilmiş ve nanoemülsiyonların hazırlama metotları ve stabilite durumları literatür incelenerek kapsamlı bir biçimde sunulmuştur.

Anahtar Kelimeler: Nanoemülsiyon; hazırlama metodları; stabilite; Ostwald olgunlaşması

*Corresponding Author: Kadir ÇINAR

e-mail: kadircinar@trakya.edu.tr

INTRODUCTION

Emulsions which have droplet sizes between 5-200 nm are named as nanoemulsions, ultrafine emulsions, submicron emulsions, translucent emulsions and miniemulsions (Solans et al., 2005; Caldero et al., 2011). Nanoemulsions are developed systems for the delivery of biologically active agents for controlled release and drug delivery. They are promising systems for the fields of cosmetics, diagnostics, drug therapy and biotechnology (Sukanya et al., 2013). Moreover, they possess great potential as a novel delivery system in food industry for fatty acids, polyphenols, natural colors, and flavors especially for producing functional foods (Silva et al., 2012). Lipophilic active compounds have poor water solubility and thus introducing them into food and beverages is a big challenge for food industry. Using nanoemulsions as a carrier system solve the solubility problem and also increase bioavailability of lipophilic active compounds such as vitamins and carotenoids (Chu et al., 2007; Sagis, 2015).

Emulsions, also called as macroemulsions, are generally described as two immiscible phases dispersed within another (Becher, 2001). There are two main differences between conventional emulsions and nanoemulsions which results from size and shape of the particles in the continuous phase. Firstly, particle sizes in nanoemulsions (5-200 nm) are very smaller than conventional emulsions (0.1-100 μm). Secondly, in emulsions there are roughly spherical droplets of one phase dispersed into another. However, nanoemulsions consist of various structures such as droplet like swollen micelles and bicontinuous structures (Fernandez et al., 2004; Deverajan & Ravichandran, 2011).

Table 1: Properties of emulsions (Fernandez et al., 2004; Zhang, 2011; Thakur et al., 2013).

Emulsion	Droplet Size	Thermodynamic Stability	Appearance
Macroemulsion	0.1-100 μm	Unstable	Turbid
Microemulsion	5-100 nm	Stable	Transparent
Nanoemulsion	5-200 nm	Unstable	Transparent

Both microemulsions and nanoemulsions are transparent or translucent systems. Although they have almost similar average droplet size as shown in Table 1, they are different due to their preparation methods. Both of them require energy input for preparation in such a way that mechanical shear is used for nanoemulsions and spontaneous emulsification methods are used for microemulsions. As compared with nanoemulsions (5-10 %, w/w), formation of microemulsions (>20 %, w/w) need high surfactant concentration (Tadros et al., 2004; Setya et al., 2014). However, differently from microemulsions, which are thermodynamically stable, nanoemulsions have only kinetic stability (Korelova & Yurtov, 2012). For this principal difference between them, nanoemulsions may separate into the constituent phases since they are not in equilibrium. In addition to these, comparing with microemulsions, nanoemulsions draw interest for utilizing in, pharmaceutical, cosmetic, chemical and food industry because moderate surfactant concentrations are sufficient to form them (Mei et al., 2011). Moreover, there are significant differences between their preparation methods, since nanoemulsions need a large input of energy.

METHODS OF PREPARATION

Nanoemulsions can be prepared by using high and low energy methods. In high energy methods, mechanical devices deliver required large disruptive forces. On the other hand, in low energy methods, there is no need for an external force. Production of nanoemulsions is achieved by using the intrinsic physiological properties of the system. In this nanoemulsion preparation method, stored energy of the system is utilized by alteration of parameters such as temperature, composition of the system (Setya et al., 2014). At the initial studies of nanoemulsions, the high energy methods were only choice for researches and thus high-energy stirring and ultrasonic emulsification were the most widely used methods (Korelova & Yurtov, 2012). Nowadays, low-energy methods have drawn considerable attention since they are 'soft', non-destructive and cause no damage to encapsulated molecules (Anton et al., 2008).

High-Energy Emulsification Methods

Nanoemulsions are non-equilibrium systems which cannot be formed spontaneously. For this reason, mechanical or chemical energy input is necessary to form them. Nanoemulsions are generally prepared by using high energy methods in which mechanical energy input is applied by high pressure homogenizers, high-shear stirring, and ultrasound generators (Sole et al., 2012). These mechanical devices provide strong forces that disrupt oil and water phases to form nanoemulsions. In high energy methods, input energy density is about 10^8-10^{10} W kg^{-1} (Gupta et al., 2016). Required energy is supplied in a shortest time to the system in order to obtain homogeneous small sized particles. High-pressure homogenizers are capable of doing this and therefore they are the most widely used devices for preparing nanoemulsions (Solans et al, 2005). Moreover, producing emulsions using ultrasound is a cost-effective process which needs less surfactant use (Kaltsa et al., 2013). Therefore, considering conventional mechanical processes more homogeneous batches are achieved (Tadros et al., 2004).

High Pressure Homogenization

It is the most popular method used for the production of nanoemulsions. This method benefits from the high-pressure homogenizer or the piston homogenizer (Figure 1) to manufacture nanoemulsions that particle sizes are up to 1 nm. During the method, the macroemulsion is forced to pass through in a small orifice at an operating pressure between 500 to 5000 psi (Chime et al., 2014). Extremely small droplet sized nanoemulsions are achieved because during the process several forces like hydraulic shear, intense turbulence and cavitation act together.

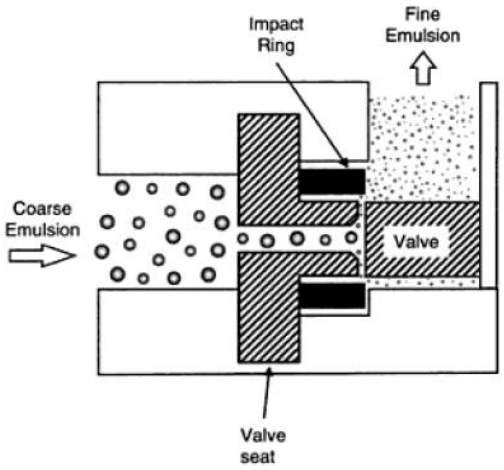


Figure 1. Schematic representation of high pressure valve homogenizer (McClements, 2005.)

This process can be repeated until the final product reaches the desired droplet size and polydispersity index (PDI). The uniformity of droplet size in nanoemulsions is specified by PDI (Jaiswal et al., 2015). Higher PDI means lower uniformity of droplet size in nanoemulsions. Monodisperse samples have PDI lower than 0.08, PDI between 0.08 and 0.3 states a narrow size distribution, whereas PDI greater than 0.3 indicates broad size distribution (Zhang, 2011). However, obtaining of small droplets that are in

submicron levels requires large amount of energy (Lovelyn & Attama, 2010). This amount of energy and increasing temperatures during high pressure homogenization process might cause deterioration of the components (Setya et al., 2014). Thermolabile compounds such as proteins, enzymes and nucleic acids may be damaged (Floury et al., 2000; Chime et al., 2014)

High-Shear Stirring

In this method, high-energy mixers and rotor-stator systems are used for the preparation of nanoemulsions. Droplet sizes of the internal phase can be significantly decreased by increasing the mixing intensity of these devices. However, obtaining emulsions with the average droplet size less than 200-300 nm is rather difficult (Korelova & Yurtov, 2012).

Ultrasonic Emulsification

There are two mechanisms which take part in ultrasonic emulsification. Firstly, acoustic field creates interfacial waves that makes oil phase to disperse in the continuous phase as droplets. Secondly, ultrasound provokes acoustic cavitation which provides formation and collapse of microbubbles respectively due to pressure fluctuations of a single sound wave. In this way, enormous levels of highly localized turbulence is generated and this causes micro implosions which disrupt large droplets into sub-micron size (Zhang, 2011).

In this method, premixed macroemulsion is agitated by vibrating solid surface at 29 kHz or larger frequencies. High-power ultrasonic devices such as focusing horns and pointed tips cause extreme shear and cavitation that result in breaking up of droplets. It has been observed that in most of the ultrasonic systems emitted sound field is inhomogeneous. For this reason, in order to have all droplets to experience highest shear rate, recirculation of the emulsion through the region of high power must be provided. Moreover, by doing this type of recirculation many times it is possible to obtain emulsions with uniform droplet size at dilute concentrations (Mason et al., 2006). Emulsifier type, the amount emulsifier, and viscosity of phases are the most critical parameters that affect homogenization efficiency (Maa & Tsu, 1999; Leong et al., 2009). Thus, optimization of these parameters is necessary to prepare nanoemulsions having fine droplets. However, there are some concerns about sonication methods due to fact that they have possibility to induce protein denaturation, polysaccharide depolymerization and lipid oxidation (Jafari et al., 2006; McClements & Rao, 2011).

Microfluidization

It is most widely employed in the pharmaceutical industry in order to acquire fine emulsions. In this method, a device called microfluidizer is used which provides high pressures (Figure 2). During the process, high pressure forces the macroemulsion to go through to the interaction chamber and thus nanoemulsions with submicron ranged particles can be produced. Uniform nanoemulsion production can be achieved by repeating the process many times and varying the operating pressure in order to get desired particle size (Chime et al., 2014; Jaiswal et al., 2015).

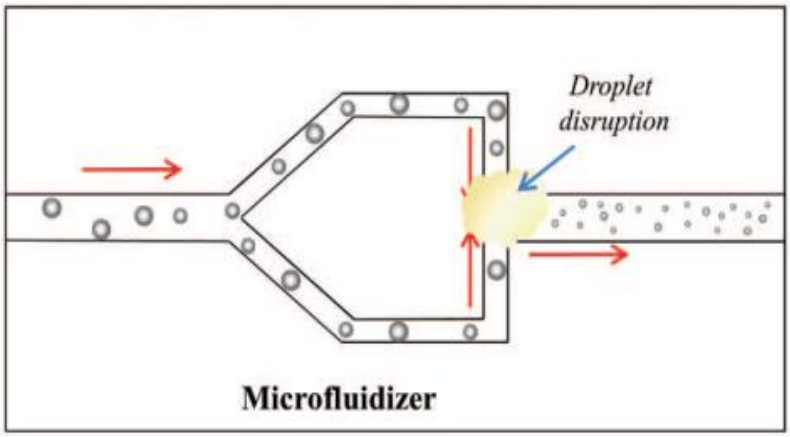


Figure 2. Schematic representation of microfluidizer (McClements & Rao, 2011).

There is a collision between crude emulsion jets from two opposite channels in the nozzle of microfludizer which is also called as the interaction chamber. The mobility of crude emulsion is provided by a pneumatically powered pump that has capability of compressing air up to pressures between 150 to 650 MPa. This high pressure forces the crude emulsion stream to go through microchannels and after the collison of two opposite channels enormous level of shearing force is obtained. Therefore, by the help of this force fine emulsions are produced (Gupta et al., 2010).

Low-Energy Emulsification Methods

Nanomulsification can also be achieved with low-energy methods which provides small size and more uniform droplets (Solans et al., 2005; Sole et al., 2012). These methods such as phase inversion temperature and phase inversion component provide smaller and more uniform droplets by using physicochemical properties of the system (Caldero et al., 2011). Although low energy procedures are generally more effective to produce small droplet sizes than high energy procedures, there are some limitations for them about the using of some types of oils and emulsifiers like proteins and polysaccharides. In order to overcome this problem high level of synthetic surfactant concentrations are used to produce nanoemulsions in low energy techniques but this narrows down their application area, especially for many food process (McClements & Rao, 2011).

Spontaneous Nanoemulsification

It benefits from the chemical energy releasement based upon dilution process with the continuous phase which occurs usually at constant temperature without any phase transitions in the system during the emulsification process (Solans & Sole, 2012). This method can produce nanoemulsions at room temperatures and no special devices are required. It basically subjected to interfacial tension, viscosity of interfacial and bulk, phase transition region, surfactant structure, and surfactant concentration (Setya et al., 2014). In the pharmaceutical industry, systems prepared by using this method are usually called as self-emulsifying drug-delivery systems (SEDDS) or self-nano-emulsifying drug-delivery systems (SNEDDS). When an oil phase with a water soluble substance is mixed with water, oil droplets spontaneously forms. The mechanism depends on the movement of water dispersible substance from the oil phase to the water phase, indicated as red arrows in Figure 3. This leads to interfacial turbulence and thus formation of spontaneous oil droplets (McClements & Rao, 2011).

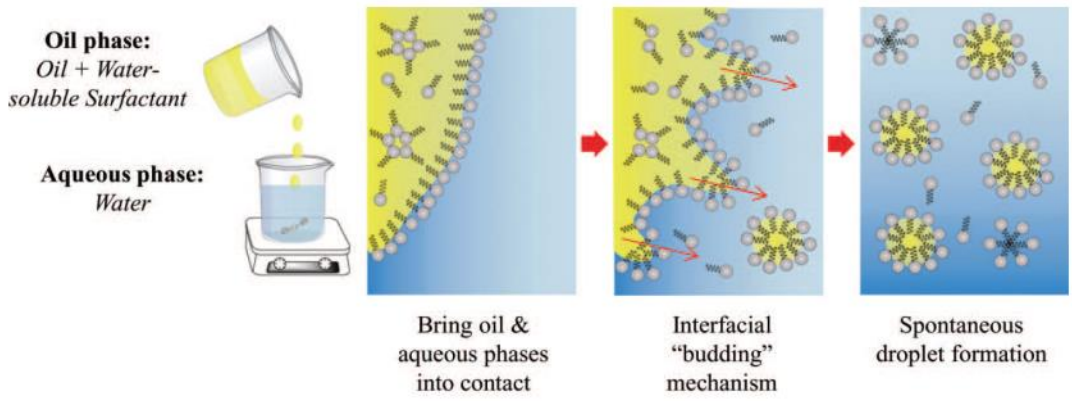


Figure 3. Schematic representation for spontaneous emulsification (McClements & Rao, 2011).

Phase Inversion Methods

These methods utilize the chemical energy that is released because of the phase transitions during emulsification process (Anandharamakrishnan, 2014). Required amount of phase transitions are achieved by changing the composition at constant temperature or by changing the temperature at constant composition (Thakur et al., 2013).

Phase Inversion Temperature (PIT)

In this method, temperature is changed at constant composition. Non-ionic surfactants which have temperature dependent solubility like polyethoxylated surfactants play important role. Emulsification is achieved by modifying affinities of surfactants for water and oil as a function of temperature (Lovelyn & Attama, 2010; Chime et al., 2014). During heating of polyethoxylated surfactants they become lipophilic due to dehydration of polyoxyethylene groups. Therefore, this circumstance establishes the principle of producing nanaoemulsions by PIT method. In order to prepare nanoemulsions by using PIT method, it is necessary to bring sample temperature to its PIT level or hydrophile–lipophile balance (HLB) level (Anandharamakrishnan, 2014). In the PIT method, the droplet sizes and the interfacial tensions reach their minimum value. This method promotes emulsification by benefiting from the extremely low interfacial tensions at the HLB temperature. Nevertheless, it has been observed that although emulsification is spontaneous at the HLB temperature, coalescence rate is greatly fast and emulsions are highly unstable (Ee et al., 2008). It has been reported that stable and fine emulsion droplets can be produced by rapid cooling of the emulsion near the temperature of PIT (Tadros et al., 2004; Rajalakshmi et al., 2011).

Phase Inversion Composition (PIC)

In this method, composition is changed at constant temperature. Nanoemulsions are obtained by consistently adding water or oil to the mixture of oil-surfactant or water-surfactant. The PIC method is more suitable for a large scale production than the PIT method since adding one component to an emulsion is easier than to generate abrupt change in temperature (Solans & Sole, 2012). By adding water to the system, volume of water increases and this result to reach a transition composition. In other words, the level of hydration of the the polyoxyethylene chains of the surfactant increases and thus spontaneous curvature of the surfactant goes to a change from negative to zero. As in the HLB temperature, in the transition composition a balance is obtained for the surfactant hydrophilic–lipophilic properties. When this transition composition is exceeded, small sized metastable oil in water droplet are composed due to the separation of the structures that have zero curvature (Anandharamakrishnan, 2014).

STABILITY OF NANOEMULSIONS

Emulsion stability is dependent on role of surfactants, its composition and the droplet size distribution. Surfactants have important role in nanoemulsion preparation methods by lowering the interfacial tension between two phases in order to obtain small sized droplets (Tadros et al., 2004). Emulsifier type influences the nanoemulsion stability against heating, cooling, pH, ionic strength and long-term storage (McClements & Rao, 2011). Surfactants promotes stability in different ways such as ionic surfactants provide electrical charge whereas non-ionic surfactants create a steric barrier with bulky molecular groups (Silva et al., 2012). In addition, effect of gravity on larger particles are much more than small ones (Fernandez et al., 2004).

Nanoemulsions possess great stability against coalescence, flocculation, sedimentation or creaming due to their characteristic particle size (Solans et al., 2005). Owing to the fact that nanoemulsions are subjected to Brownian motion rather than gravitational forces because of their very small droplet size, creaming or coalescence do not generally pose problem (Klang et al., 2012). Also, smaller droplet size provides less adhesion and higher stability against flocculation accompanied by steric stabilization which is a natural prevention for nanoemulsions (Anton et al, 2008; Delmas et al., 2011). On the other hand, Ostwald ripening is the main destabilization mechanism for them due to their nature of droplet sizes. Therefore, Ostwald ripening causes great limitation for their utilization for developing applications (Gutierrez et al., 2008).

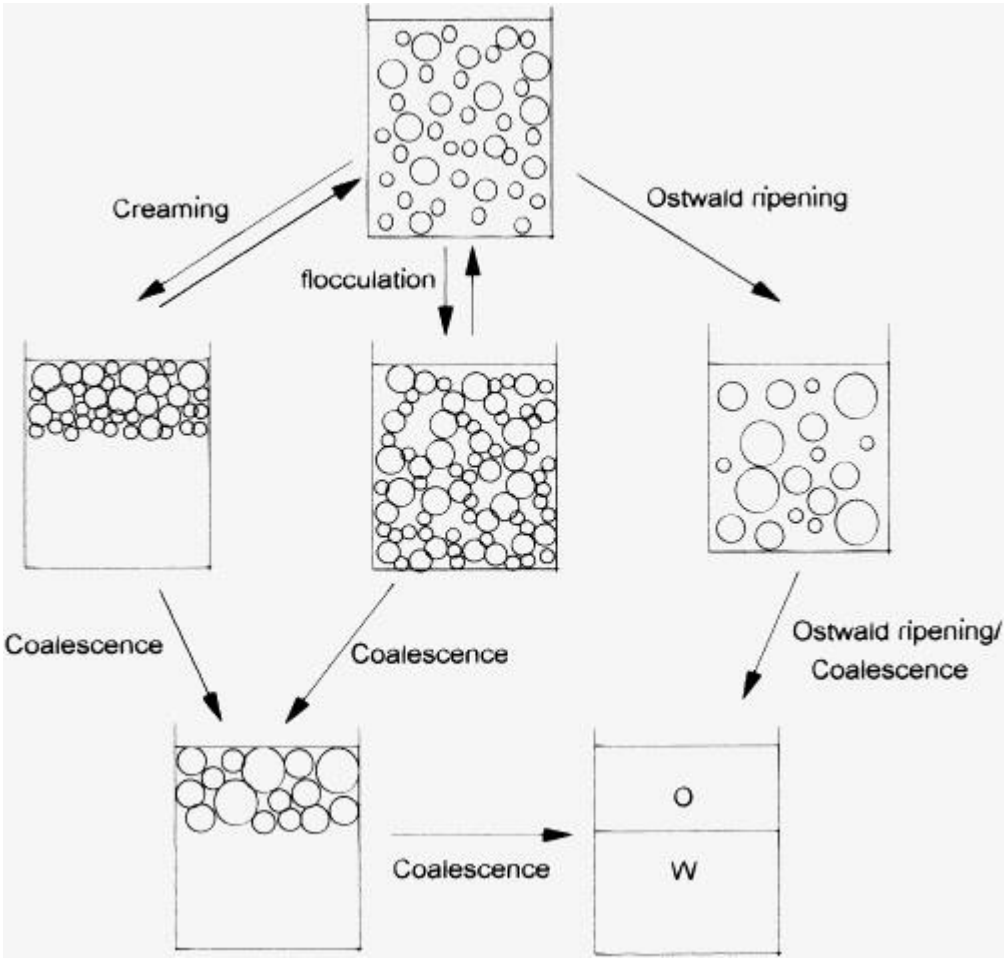


Figure 4: Physicochemical mechanisms cause instability (Taylor, 1998).

Ostwald ripening results from polydispersity of emulsions and the solubility difference between small and large droplets (Rajalakshmi et al., 2011). It is actually a mass transfer phenomenon which takes place between the droplets through the bulk phase (Figure 4). Due to the differences between droplet radiuses, chemical potential differences of the materials occurs inside of the droplets. The free energy in the emulsion begin to reduce and this give rise to decrease of the interfacial area. Thus, smaller sized droplets start to combine with bigger ones (Delmas et al., 2011). The reason for this is migration of the dispersed phase through bulk from small ones to bigger ones, because small droplets have higher solubility in the bulk than bigger droplets. Therefore, Ostwald ripening starts and accelerates during the process (Solans et al., 2005; McClements & Rao, 2011).

The Ostwald ripening rate for nanoemulsions can be decreased by some methods. For example, using a compound less soluble in the dispersion medium as the internal phase can be effective. It has been shown that the stability of the emulsions against the Ostwald ripening significantly increases with decreasing the hydrocarbon solubility in water as dispersion medium (Setya et al., 2014). Moreover, adding less polar lipid like long chain triglycerides can also reduce Ostwald ripening rate. Addition of this compound causes insolubility in water and therefore provides a kinetic barrier for Ostwald ripening (Wooster et al., 2008). Molecular weight of oil phase is another important factor since diffusion coefficient is correlated with the molecular weight. Therefore, the rate of Ostwald ripening can be diminished by using high molecular weighted oils (Zhang, 2011).

Some Studies on the Stability of Nanoemulsions

Ee et al. (2008) studied the formation and stability of nanoemulsions by using PIT emulsification method. According to their results, heating and cooling methods and the final temperature obtained after phase inversion have great influence on the size distributions. They found out that at the optimum storage temperature (20°C below PIT) which was dependent on surfactant concentration, nanoemulsions were most stable and most smallest-sized (25 nm to 54 nm) with low polydispersity indices (~0.2). The droplet sizes of nanoemulsions grow faster at room temperatures due to the Ostwald ripening. However, nanoemulsions stored at optimum temperatures retained their smallest droplet sizes, lowest polydispersity indices and superior stability. For this reason, they concluded that destabilizing effect of Ostwald ripening may be retarded by keeping nanoemulsions at the optimum storage temperatures.

A study about the influence of different kinds of inorganic salts on the PIT, electrophoteric properties and long term stability of nanoemulsions was conducted by Mei et al. (2011). They found that salts caused to growth of the emulsion droplets with time due to decreasing level of zeta potential and the PIT. The reason of that was explained by the countering and the salting-out effect of the inorganic salts. On the other hand, nanoemulsions containing emulsifiers with high PITs, could be formed more easily by adding salting-out salts in water which provides to obtain an optimum temperature by decreaing the PIT of the systems. They indicated that Ostwald ripening was responsible for the instability of nanoemulsions.

In another study, Yang et al. (2009) investigated stability of isopropyl mysristate (IPM) in water nonoemulsions (stabilized by PEG-60 hydrogenated caster oil varied ethanol concentration) which was prepared by PIC method at room temperature. Ostwald ripening was the main instability mechanism in their work. They assessed long term stability and found that flocculation may not occur due to the higher negative zeta potential of nanoemulsion. Addition of ethanol to the stock nanoemulsions (0.007 wt% IPM, 0.3 wt% ethanol, 0.007 wt% surfactant and water at 23°C) showed increasing rate of Ostwald ripening which was

explained by the increasing solubility of isoproplymysristate in the system. Moreover, increasing ethanol concentration in the continuous phase caused much larger droplet sizes for nanoemulsions. For this reason, they indicated that the difference between densities of continuous phases might be the main factor for controlling droplet sizes in nanoemulsions.

Delmas et al. (2011) applied ultrasonication method in order to obtain nanoemulsions which have very small sized droplets and high stability. They determined that the characteristic decay time for the mean droplet sizes had direct relationship with frequency of bubble collapse and thus sonication power. They showed also that Ostwald ripening was still the main destabilization mechanism but coalescence could be readily hindered because of the very small size of droplets.

CONCLUSION

This paper provides general information about nanoemulsions and presents the current studies about nanoemulsion stability. All of the studies point out that main destabilization mechanism for nanoemulsion stability is Ostwald ripening. Although small droplet sizes provide natural defense system in nanoemulsions for flocculation, Ostwald ripening occurs whatever the preparation method is. However, this does not change the truth of long-term stability of nanoemulsions if they are stored at proper conditions. There is increasing use of nanoemulsions in many practical applications primarily in pharmacy as a drug delivery system since they are capable of solubilized non polar active compounds. However, a deeper understanding is necessary in order to develop nanoemulsions in food processing applications. Having elucidative mechanisms that rule the preparation and stability of food nanoemulsions can be beneficial for better formulation and application for nanoemulsions to use in food industry. In the light of these information, further work is needed to be done about nanoemulsion formulations and their stability.

REFERENCES

1. Anandharamakrishnan, C., Techniques for Nanoencapsulation of Food Ingredients, *Springer*, 2014.
2. Anton, N., Benoit, J.P., and Saulnier, P., Design and production of nanoparticles formulated from nano-emulsion templates-A review, *Journal of Controlled Release*, 128, 185-199, 2008.
3. Becher, P., Emulsions: Theory and Practice, Oxford University Press, New York, 2001.
4. Caldero, G., Maria, J.G.C. and Solans, C., Formation of polymeric nano-emulsions by a low-energy method and their use for nanoparticle preparation, *Journal of Colloid and Interface Science*, 353, 406–411, 2011.
5. Chime, S.A., Kenechukwu, F.C., and Attama, A.A., Nanoemulsions-Advances in Formulation, Characterization and Applications in Drug Delivery, Ali DS, *Application of Nanotechnology in Drug Delivery, Crotia: InTech*, 77-111, 2014.
6. Chu, B.S., Ichikawa, S., Kanafusa, S., and Nakajima, M., Preparation of protein-stabilized β-carotene nanodispersions by emulsification–evaporation method, *Journal of the American Oil Chemists' Society*, 84(11), 1053-1062, 2007.
7. Delmas, T., Piraux, H., Couffin, A.C., Texier, I., Vinet, F., Poulin, P., Cate, M.E. and Bibette J., How To Prepare and Stabilize Very Small Nanoemulsions, *Langmuir*, 27(5), 1683–1692, 2010.
8. Devarajan, V. and Ravichandran, V., Nanoemulsions: As Modified Drug Delivery Tool, *Devarajan V / Pharmacie Globale (IJCP)*, 4 (1), 2011.
9. Ee, L.S., Duan, X., Liew, J. and Nyugen, Q.D., Droplet size and stability of nano-emulsions produced by the temperature phase inversion method, *Chemical Engineering Journal*, 140, 626–631, 2008.
10. Fernandez, P., Andre, V., Rieger, J. and Kühnle A., Nano-emulsion formation by emulsion phase inversion, *Colloids and Surfaces A: Physicochem. Eng. Aspects*, 251, 53–58, 2004.
11. Floury, J., Desrumaux, A., and Lardieres, J., Effect of high-pressure homogenization on droplet size distributions and rheological properties of model oil-in-water emulsions, *Innovative Food Science & Emerging Technologies*, 1(2), 127-134, 2000.

12. Gupta, P.K., Pandit, J.K., Kumar, A., Swaroop, P., and Gupta, S., Pharmaceutical Nanotechnology Novel Nanoemulsion–High Energy Emulsification Preparation, Evaluation and Application, *The Pharma Research*, 3, 117-138, 2010.

13. Gutierrez, J.M., Gonzalez, C., Maestro, A., Sole, I., Pey, C.M. and Nolla J., Nano-emulsions: New applications and optimization of their preparation, *Current Opinion in Colloid & Interface Science*, 13, 245–251, 2008.

14. Jafari, S.M., He, Y.H., and Bhandari, B., Nano-emulsion production by sonication and microfluidization: A comparison, *International Journal of Food Properties*, 9, 475–485, 2006.

15. Jaiswal, M., Dudhe, R., and Sharma, P.K., Nanoemulsion: an advanced mode of drug delivery system, *3 Biotech*, 5, 123–127, 2015.

16. Kaltsa, O., Michon, C., Yanniotis, S., and Mandala, I., Ultrasonic energy input influence on the production of sub-micron o/w emulsions containing whey protein and common stabilizers, *Ultrasonics sonochemistry*, 20(3), 881-891, 2013.

17. Klang, V., Matsko, N., Valenta, C. & Hofer F., Electron microscopy of nanoemulsions: An essential tool for characterisation and stability assessment, *Micron*, 43, 85–103, 2012.

18. Koroleva, M.Y., and Yurtov, E.V., Nanoemulsions: the properties, methods of preparation and promising applications, *Russian Chemical Reviews*, 81(1), 21-43, 2012.

19. Leong, T.S.H., Wooster, T.J., Kentish, S.E., and Ashokkumar, M., Minimising oil droplet size using ultrasonic emulsification, *Ultrasonics Sono-chemistry*, 16(6), 721-727, 2009.

20. Lovelyn, C., and Attama, A.A., Current State of Nanoemulsions in Drug Delivery, *Journal of Biomaterials and Nanobiotechnology*, 2, 626-639, 2011.

21. Maa, Y.F., and Hsu, C.C., Performance of sonication and microfluidization for liquid-liquid emulsification, *Pharmaceutical Development and Technology*, 4(2), 233–240, 1999.

22. Mason, T.G., Wilking, J.N., Meleson, K., Chang, C.B., and Graves, S.M., Nanoemulsions: formation, structure, and physical properties, *Journal of Physics: Condensed Matter*, 18, 635-666, 2006.

23. McClements, D.J., Food Emulsions, principles, practice, and techniques, CRC Press, Boca Raton, FL, 2005.

24. McClements, D.J., and Rao, J., Food-Grade Nanoemulsions: Formulation, Fabrication, Properties, Performance, Biological Fate, and Potential Toxicity, *Critical Reviews in Food Science and Nutrition*, 51, 285–330, 2011.

25. Mei, Z., Xu J., and Sun, D., O/W nano-emulsions with tunable PIT induced by inorganic salts, *Colloids and Surfaces A: Physicochem. Eng. Aspects*, 375, 102–108, 2011.

26. Rajalakshmi, R., Mahesh, K., and Kumar, C.K.A., A Critical Review on Nano Emulsions, *International Journal of Innovative Drug Discovery*, 1, 1-8, 2011.

27. Sagis, L.M. (Ed.), Microencapsulation and microspheres for food applications, Academic Press, 2015.

28. Setya, S., Talegaonkar, S., and Razdan, B.K., Nanoemulsions: Formulation Methods and Stability Aspects, *World Journal of Pharmacy and Pharmaceutical Sciences*, 3, 2214-2228, 2014.

29. Sole, I., Solans, C., Maestro, A., Gonzalez, C. and Gutierrez J.M., Study of nano-emulsion formation by dilution of microemulsions, *Journal of Colloid and Interface Science*, 376, 133–139, 2012.

30. Solans, C., Izquerdo, P., Nolla, J., Azemar, N. and Garcia-Celma, M.J., Nano-emulsions, *Current Opinion in Colloid & Interface Science*, 10, 102-110, 2005.

31. Solans, C., and Sole, I., Nano-emulsions: Formation by low-energy methods, *Current Opinion in Colloid & Interface Science*, 17, 246–254, 2012.

32. Silva, H. D., Cerqueira, M. Â., & Vicente, A.A., Nanoemulsions for food applications: development and characterization, *Food and Bioprocess Technology*, 5(3), 854-867, 2012.

33. Sukanya, G., Mantry, S., and Anjum, S., Review on Nanoemulsions, *International Journal of Innovative Pharmaceutical Sciences and Research*, 1(2), 192-205, 2013.

34. Tadros, T., Izquierdo, P., Esquena, J. and Solans, C., Formation and stability of nano-emulsions, *Advances in Colloid and Interface Science*, 108, 303–318, 2004.

35. Taylor, P., Ostwald ripening in emulsions, *Advances in colloid and interface science*, *75*(2), 107-16, 1998.

36. Thakur, N., Walia, M.K., and Kumar, S.L.H., Nanoemulsion in Enhancement of Bioavailability of Poorly Soluble Drugs: A Review, *Pharmacophore*, 4(1), 15-25, 2013.

37. Yang, H.J., Cho, W.G. and Park, S.N., Stability of oil-in-water nano-emulsions prepared using the phase inversion composition method, *Journal of Industrial and Engineering Chemistry*, 15, 331–335, 2009.

38. Wooster, T.J., Golding, M. and Sanguansari, P., Impact of oil type on nanoemulsion formation and Ostwald ripening stability, *Langmuir*, 24 (22):12758-12765, 2008.

39. Zhang, J., Novel Emulsion-Based Delivery Systems, Faculty of The Graduate School of the University of Minnesota, Master Thesis, 2011.

dergipark.gov.tr/tujes
Trakya University Journal of Engineering Sciences, 18(1): 85-94, 2017
ISSN 2147–0308
Derleme Makale / Review Article

KRİPTOLOJİDE KULLANILAN ASAL SAYI TEST ALGORİTMALARI

Tarık YERLİKAYA[1], Onur KARA[1*]

[1] *Trakya Üniversitesi, Bilgisayar Mühendisliği Bölümü, 22000 Edirne.*

Özet: Günümüzde şifreleme çok önemli hale gelmiştir. Asimetrik şifreleme yönteminin kırılması zordur. Bu yüzden önemli verileri şifrelerken tercih edilir. Asimetrik şifrelemenin temeli asal sayılara dayanmaktadır. Asal sayıların gizeminin hala çözülememesi bu alana olan ilgiyi arttırmaktadır. Şifrelemenin güçlü olması için yeteri kadar büyüklükte asal sayı bulabilmek önemlidir. Küçük sayıların asal olup olmadığı kısa sürede anlaşabiliyorken büyük sayıların asal olup olmadığını anlamak çok uzun sürmektedir. Bunun içinde asallık testlerine başvurulmaktadır. Asallık testleri sayesinde çok büyük sayıların asal olup olmadığı anlaşılabilmektedir.

Anahtar Kelimeler: Kriptoloji; Asal sayı; Asallık testi

Abstract: Cryptography has gained much more importance today. Asymmetric cryptography as a method is more favored as it is more difficult to break. Asymmetric cryptography is based on prime numbers. The mystery of the prime numbers keeps drawing attention on the subject. In order to make a strong encrypting it is important to find prime numbers that are big enough for encrypting. While it is quite easy to determine whether a small number is prime, it takes a long time to determine whether a large number is prime. For this reason, primality tests are utilized as they help us determine whether a very big number is prime.

Keywords: Cryptology; Prime numbers; Primality test

GİRİŞ

Teknolojinin gelişmesiyle birlikte bilgisayar ve internet hayatımızda büyük yer sahibi olmuştur. Buna paralel olarak internet üzerinden yapılan işlem sayısı da artmıştır. Kullanıcılar ticari işlerini, devlet işlerini, özel işlerini ve benzeri önemli işlevlerini sorunsuz yapabilmesi için güvenliğe dikkat etmesi gerekmektedir.(Yerlikaya, Gençoğlu, Emir, Çankaya, Buluş)

Güvenliği sağlamanın yolu da şifreleme ve kimlik denetiminden geçmektedir. Şifreleme işlemi Simetrik ve Asimetrik şifreleme olmak üzere 2'ye ayrılır. Asimetrik şifrelemenin temelini asal sayılar oluşturur. Kriptografik uygulamalarda "anahtar" olarak kullanılmak üzere çok büyük / çok uzun asal sayılara ihtiyaç duyulmaktadır. (Karaarslan, 2001)

Her dönemde bilim insanlarını teorik açıdan cezbeden asal sayılar, günümüzde elektronik güvenlik protokolleri ve açık anahtar şifreleme gibi kritik uygulamaların merkezinde yer almaktadır. Bu nedenle hem teorik hem uygulama açısından asal sayılar üzerinde yoğun olarak çalışılmaktadır. Asallık tanımından yola çıkarsak, bir n tamsayısının asal olması için 2 ile n arasında hiç bir böleni olmaması gerekir. Bu işlemi ufak sayılar için yapmak mümkün olsa da sayıların büyüklüğü arttıkça bunun hesaplanması mümkün olmamaktadır. Büyük sayıların asal olup olmadıklarını anlamak için daha gelişmiş asallık testleri gerekmektedir.(Granville, 1992)

Uzun yıllardan beri asal sayılar konusunda birçok çalışma yapılmıştır. Bu çalışmalar içerisinde en

önemli olanlar, asallık testleridir. Bir sayının asal olup olmadığını incelemek için kullanılan bu testlerin en eskileri "elek" olarak bilinmektedir. Sonraki buluşlar, matematiksel yöntemlerden yararlanarak oluşturulan çeşitli testlerdir. Böylece çok büyük sayıların asallık kontrolleri kolaylıkla yapılabilmektedir.(Yıltaş, 2003)

MATERYAL VE METOD

Bu çalışmada bir sayının asal olup olmadığının nasıl anlaşılacağı anlatılmıştır. Asal sayı test algoritmalarından Miller&Rabin, Slovay&Strassen ve Fermat testleri karşılaştırılmıştır.

Asal Sayılar

Birden büyük, sadece kendisine ve bire bölünen tam sayılara asal sayı denir. Asal olmayan sayılara ise bileşik sayı denir.(Can, 2002) Örneğin 48259 sayısı asaldır. Çünkü 1 ve 48259'dan başka pozitif böleni yoktur. Ama 111 sayısı 3 ve 37 bölünebildiğinden asal değildir. 1 den büyük her pozitif tam sayının en az iki tane pozitif böleni vardır. Bunlar 1 ve sayının kendisidir. 1 sayısı ise ne asal ne de bileşik sayıdır.

Asal sayılar ve özellikleri detaylı olarak ilk kez antik Yunanlı matematikçiler tarafından incelemiştir. M.Ö. 500-300 yılları arasında Pythagoras okulunun matematikçileri tarafından asal sayıların temelleri keşfedilmiştir(O'Connor ve Robertson, 2001). Euclid, asal sayılar hakkında birçok önemli sonucu ve aritmetiğin temel teoremini ispatlamıştır. M.Ö. 200 yılında Eratosthenes, asal sayıları hesaplayan "Sieve of Eratosthenes" algoritmasını geliştirdi. Fermat, 17'inci yüzyılda yeni bir teorem buldu. Fermat'ın teoremine göre herhangi bir n sayısının asal olması için obeb(a,n)=1 eşitliğini sağlayan her a sayısı ile $a^{(n-1)} = 1 \pmod n$ eşitliğini sağlaması gerekmektedir. Bu teoremin temelleri 2000 yıl önce geliştirilmiş eski bir Çin hipotezine dayanmaktadır.

Bu hipoteze göre n'nin asal olması için n'nin 2^n - 2'yi bölmesi gerekmektedir. Mersenne, asal olan n değerleri için 2^n-1'in de asal olduğunu iddia etti. Bu eşitliği sağlayan sayılara Mersenne Sayıları denmektedir. Her ne kadar bu formül bütün asal n değerleri için geçerli olmasa da bu formül bilinen en büyük asalların bulunmasını sağlamaktadır. Daha sonraki yıllarda Euler, Fermat'ın teoremini geliştirerek $n \geq 1$ için [1,n] aralığında n'e göreceli asal sayıların adedini veren Euler phi (totient) fonksiyonu Q(n)'i oluşturdu(Menezes ve Oorschot , 1997).

Legendre ve Gauss, büyük n değerleri için n'e yakın asalların yoğunluğunun 1/log n olduğu sonucunu 1798 yılında buldular. Bu sonuç Asal Sayı Teoremi olarak bilinmektedir. Bu teorem 1896 yılında Hadamard ve Valle Poussin tarafından ispatlanmıştır.

Asal sayılar konusunda çözüm bekleyen birçok problem bulunmaktadır. Bunlardan bazıları Riemann hipotezi, Goldbach Sanıtı, Mersenne Asalları, Carmichael Sayıları ve İkiz Asal sayılardır. Mersenne Asalları ve Carmichael Sayıları hakkında bilgiler aşağıda anlatılmıştır. Bu tür problemler çözülürken Sayılar Kuramında ve matematik başta olmak üzere birçok bilim dalında da ilerlemelere yol açıldığı unutulmamalıdır.

Asal sayılar ile ilgili bazı bilgiler şöyledir:

- 0 ve 1 asal sayı olarak kabul edilmez.
- 0 ve 1 dışındaki herhangi bir sayı, ya bileşik sayıdır ya da asal sayıdır.
- En küçük asal sayı olan 2, tek çift asal sayıdır.
- 5'ten büyük hiç bir asal sayı 5 ile bitmez.
- En büyük asal sayı, Mersenne Asalları Büyük İnternet Araştırması (GIMPS) projesindeki gönüllüler ile Dr. Curtis Cooper yaklaşık bir ay süren çalışmalar sonucunda bulundu. 22.338.618 basamaklı bilinen en büyük asal sayı $\mathbf{2^{74,207,281} - 1}$ dir.

Tablo 1. En büyük 10 asal sayı listesi

Sıra	Sayı	Basamak sayısı	Yıl
1	$2^{74,207,281} - 1$	22.338.618	2016
2	$2^{57.885.161} - 1$	17.425.170	2013
3	$2^{43.112.609} - 1$	12.978.189	2008
4	$2^{42.643.801} - 1$	12.837.064	2009
5	$2^{37.156.667} - 1$	11.185.272	2008
6	$2^{32.582.657} - 1$	9.808.358	2006
7	$2^{30.402.457} - 1$	9.152.052	2005
8	$2^{25.964.951} - 1$	7.816.230	2005
9	$2^{24.036.583}$ -1	7.235.733	2004
10	$2^{20.996.011} - 1$	6.320.430	2003

Mersenne Asalları

Asal bir *n* için 2^n - 1 biçiminde yazılan sayılara Mersenne sayıları denir.

n = 2 için $M_2 = 22-1 = 3$

n = 3 için $M_3 = 23-1 = 7$

n = 5 için $M_5 = 25-1 = 31$

n = 7 için $M_7 = 27-1 = 127$

Bu sayıların her biri asal sayıdır. Ama bundan sonraki ilk asal sayısı olan 11 için M_{11}'in Mersenne sayısı olup olmadığını inceleyelim.

n = 11 için $M_{11} = 211-1 = 2047$

2047 = 23 x 89 olduğunda M_{11} sayısı asal değildir.

Tüm asal n sayıları için M_n'nin asal olmadığı görülmektedir. Burada akla gelen soru hangi *n* asalları için M_n sayısının asal olduğudur. Bu sorunun cevabı hala bulunamamıştır. Bu yüzden Mersenne asalların sonsuz sayıda olup olmadığı bilinmemektedir. Şu ana kadar bulunan en büyük asal sayı $2^{74,207,281}$ - 1 bir Mersenne asal sayısıdır. Internet üzerinde en büyük Mersenne sayısını bulmaya yönelik çalışmalar yürütülmektedir.

Carmichael Sayıları

Fermat teoremine göre: n'nin asal sayı olması için ve her a tabanı için a^n-a'yı bölmesi gerekmektedir fakat bu bölme işlemini sağlayan asal olmayan sayılar da vardır. Bu sayılara Carmichael sayıları denir. "$x^{(n-1)}$ = 1 mod n" eşitliğini sağlayan bileşik x sayıları olarak da ifade edilir. Bu sayıların kriterlerini 1899 yılında Korselt şu şekilde belirlemiştir:

1. n, kare bağımsız olmalıdır.
2. n'yi bölen p asal değerleri için (n-1) de (p-1) değerlerine bölünmelidir.

İlk olarak 1910 yılında R. D. Carmichael bu kriterlere uyan sayıların bir kısmını bulmuş. Bundan sonrada bu sayılara Carmichael sayıları denmiştir.

Bu sayılardan bazıları aşağıda verilmiştir.

561, 1105, 1729, 2465, 2821, 6601, 8911, 10585, 15841, 29341, . . .

Bu sayılar oldukça ender olmasına karşılık sonsuz sayıda olup olmadığı bilinmemektedir. Bu soruna karşılık 1992 yılında Alford, Granville ve Pomerance, x sayısına kadar $x^{2/7}$ den daha fazla Carmichael sayısı olduğunu ispatlamıştır.

Asal Sayı Teoremi

2300 yıl önce Euclid, asal sayıların sonsuz sayıda olduğunu kanıtladı. Bundan sonra ise herhangi bir sayıya kadar kaç tane asal sayı olduğunu hesaplama ihtiyacı duyuldu. Asal Sayı Teoremi de bu sorunu hesaplamak ile ilgilidir. Asal Sayı Teoremi 1791 yılında Gauss tarafından varsayım olarak ortaya atıldı. Bu teoreme eşit başka bir ifade 1798 yılında Legendre tarafından yayınlandı. Asal Sayı Teoremini kanıtlamak için ilk gerçek adım 1850 yılında Chebyshev tarafından atıldı. Asal Sayı Teoremi 1896 yılında, Charles de la Vallee Poussin ve Jacques Hadamard tarafından aynı anda ve birbirlerinden bağımsız olarak kanıtlandı. Bu teorem

rasgele bir x sayısının asal olması olasılığının yaklaşık olarak 1/ loge x olduğunu belirtir.

π(x) = x'e eşit ya da x'ten küçük asalların sayısı verir. Örneğin 25'den küçük asal sayılar = 2, 3, 5, 7, 11, 13, 17, 19, 23 Bu durumda; π(3) = 2, π(10) = 4, π(25) = 9

Tablo 2 x = [10, 10^{10}] için π(x) değerlerini göstermektedir (Caldwell, 2002)

Tablo 2. x = 10^{10}'ye kadar olan π(x) değerleri

X	**π (*x*)**
10	4
100	25
1,000	168
10,000	1,229
100,000	9,592
1,000,000	78,498
10,000,000	664,579
100,000,000	5,761,455
1,000,000,000	50,847,534
10,000,000,000	455,052,511

x'i geçmeyen asalların sayısı π (x), x / ln x 'e asimptotiktir.

$$\lim_{x\to\infty} \frac{\pi(x)\ln x}{x} \to 1 \qquad \text{(Formül 1)}$$

" a(x), b(x) 'e asimptotik" ile belirtilen bu ifadede x sonsuza yaklaşırken a(x) / b(x) oranının 1'e yaklaştığı görülmektedir.

Tablo 3'te 10^{10}'a kadar olan bazı sayılar için elde edilen değerler yer almaktadır (The University of Sheffield, 1999).

x bir asal sayı ise bir sonraki asal sayıya olan ortalama uzaklık yaklaşık olarak ln *x* 'tir. Asal sayı teoremi, asal sayıların dağılımı hakkında kısıtlı da olsa bir fikir vermektedir.

Tablo 3. Asal sayı teoremi ile ilgili 10^{10}'a kadar olan bazı sayılar için elde edilen değerler

x	**π(*x*)**	***x*/ln(*x*)**	**π(*x*)ln(*x*)/*x***
10	4	4.3	0.921034
10^2	25	21.7	1.15129
10^3	*168*	*144.8*	*1.1605*
10^4	1229	1085.7	1.13195
10^5	9592	8685.9	1.10432
10^5	78498	72382.4	1.08449
10^7	664579	620421	1.07117
10^8	5761455	5428681	1.0613
10^9	50847534	48254942	1.05373
10^{10}	455052511	434294482	1.0478

Asal Sayı Test Algoritmaları

Eski zamanlardan beri bir sayının asal olup olmadığını bulmaya yönelik birçok çalışma olmuştur. Günümüzde Asal sayıların şifrelemede önemli bir yeri olduğundan asallık testleri daha da önem kazanmıştır.

M.Ö. 240 yıllarında Erastotenes asallık testi için ilk yöntem olan Erastotenes Kalburu önermiştir. Erastotenes Kalburu'na göre: Eğer sayının kareköküne kadar olan bütün asal sayılar denenmiş ve bir çarpan bulunmamışsa, sayının kendisinden ve 1'den başka çarpanı yok demektir; dolayısıyla bu bir asal sayıdır. Buradaki sorun büyük sayıların çarpanlara ayırmadaki zorluğudur. 17. Yüzyılda Fermat'ın geliştirdiği Fermat teoremi ile çarpanlara ayırma işleminde büyük bir yol sağlanmıştır.

Fermat Teoremine göre: her a tamsayısı için p , (a^p-a)'yı böler. Bu teorem, asallık testleri ile ilgilenen kişilerin referans noktası olmuştur. O zamandan sonra asallık testi ile ilgili birçok algoritma

geliştirmiştir. Onlardan bazıları 1976 yılında Miller daha sonrada Rabin Genişletilmiş Riemann hipotezine dayanan olasılık algoritmaları geliştirdiler. 1983'te Adleman, Pomeiance ve Rumely algoritmaları geliştirildi. 1986'da Coldwaser ve Kilian eliptik eğrilerine dayanan bir algoritma ürettiler. Son olarak 2002 yılında Manindra Agrawal, Nitin Saxena ve Neeraj Kayal tarafından AKS Asallık testi geliştirilmiştir.

Asal sayı testlerini gerçekleştirirken temelde dikkat edilmesi gerekenler aşağıda belirtilmiştir.

1. Çift sayıları test etmeye gerek yoktur.
2. Asallığı test edilen sayıların; 3, 5, 7, 11 … gibi küçük asal sayılara bölünüp bölünmediğine bakarak birçok sayı elenebilir. Örneğin 23 sayısına kadar olan asal sayılar alınırsa, asal sayı olmayanların en azından 2/3'ü ayıklanabilir ve 3 kat daha hızlı sonuca gidilebilir (Segre, 2000).

Erastotenes Kalburu

Asallık testlerinin en basit metodu olan Erastotenes Kalburu M.Ö. 300'de Eratosthenes tarafından geliştirildi. Eratosthenes Kalburu sürekli bileşik sayıları eleyerek ilerler ve en sonunda kalan sayılar asal sayı olur. Bu yöntem $O(n\sqrt{n})$ zaman karmaşıklığına sahiptir. Verilen bir sayıya kadar olan bütün asal sayıları kesin olarak bulur. Fakat sayılar büyüdükçe asal sayıları bulmak için harcanan zaman çok fazla artar.

Eratosthenes Kalburu işleyişi:

1. Bir sayı belirlenir ve 2 den başlayarak bu sayıya kadar olan tüm sayılar yazılır.
2. Asal sayılar adında bir liste tutulur ve bu listeye ilk asal sayı olan 2 eklenir.
3. Yazılmış olan sayılar içinden 2 ve 2'nin tüm katları silinir.
4. Silme işleminden sonra kalan ilk tek sayı asaldır. Bu sayı Asal sayılar listesine eklenir.
5. Bu tek sayı ve tüm katları yazılmış olan sayılardan silinir.
6. Yazılmış olan sayılarda herhangi bir sayı kalmayıncaya kadar 4. ve 5. adımlar tekrarlanır.

Asal sayı test algoritmaları sayının asal olduğunu kanıtlayan(Bu durumda kanıtlanmış asal) ya da büyük olasılıkla asal denir. Sayı muhtemel asal çıkıyorsa bu tür testlere olasılıklı asallık testleri; eğer matematiksel olarak ispatlıyorsa buna da Gerçek asallık testleri denir.(Yerlikaya, 2006)

a. Kesin *(Deterministic)* Asallık Testleri

Bu tür asallık testleriyle ile bir sayının asal olup olmadığını kesin olarak belirlemek mümkündür. Bu tür yöntemler genellikle çarpanlara ayırmaya dayanmaktadır.

Kesin Asallık Testleri büyük sayıları test ederken çok fazla zamana ihtiyaç duyduğundan kullanışlı değildir. Aynı zamanda bu yöntemler çok karışıktır, uygulamada bir hata yapma olasılığı, olası asallık testinde hata yapma olasılığından daha fazladır (Silverman, 1997).

En çok kullanılan yöntemlerin bazıları: Cyclotomic Ring Testi, Lucas-Lehmer Testi ve AKS Testidir.

b. Olası Asallık Testleri

Olası Asallık Testlerini(OAT) geçen sayının yüksek olasılıkla asal olduğunu ispatlanır. OAT'de asal sayı üretmek için öncelikle *n* bitlik bir rastsal sayı üretilir. Daha sonra asallık deneyine tabi tutulur. Testi geçen asal sayılır seçilir ve istenilen yerde kullanılır. OAT'de hata payını en aza düşürmek için geçilmesi gereken test sayısı arttırılabilir. Bu sayede çok küçük bir hata payı ile sayının asal olup olmadığı anlaşılır. 2^{-100} den daha düşük bir hata payı ile bir sayının asal olduğu belirlenebilir (RSA, 1998). Bu deneyler, Kesin Asallık Testlerinden hızlı olduğu için daha çok tercih edilir.

En çok kullanılan OAT'nin bazıları şunlardır :

1. Fermat Testi

2. Lehmann Testi
3. Solovay Strassen Testi
4. Miller&Rabin Testi

Tanık (witness) Kavramı

Bir sayının asal olmadığını yani bileşik sayı olduğunu anlamak için çarpanlarına ayırmaya çalışılır. Fakat çarpanların yoğunluğu genelde çok az olduğundan bu yöntem etkili değildir. Bunun yerine OAT kullanılarak daha etkin bir çalışma yapılabilir. OAT, tanık kavramına dayanmaktadır ve tanıklık fonksiyonları olarak da adlandırılırlar. Tanık, n sayısının bileşikliğini göstermek için kullanılan 1 ile n arasında bulunan herhangi bir sayıdır. Tanıklık fonksiyonlarına göre, tanık sayıların yoğunluğu (d değeri) değişmektedir ve bu değerler Tablo 4'da gösterilmiştir. Daha büyük d değerleri, itimat eşiğine daha hızlı yaklaşma demektir (Segre, 2000).

Tablo 4. Tanıklık Fonksiyonlarında yoğunluk (d) değerleri

Tanıklık Fonksiyonları (Olası Asallık Testleri)	**Tanık Sayıların Yoğunluğu (d değeri)**
Lehmann	0,5
Miller&Rabin	0,75
Solovay – Strassen	0,5

OAT'ye sokulan bir sayının i iterasyon sonunda asal ilan edilmesine rağmen bileşik olma olasılığı vardır. Tanık sayıların yoğunluğu d olarak kabul edilirse, bir sayının bileşik olma olasılığı Formül 2 ile hesaplanmaktadır. Bir sayının asal olma olasılığı ise Formül 3 ile hesaplanmaktadır.

$$P(\text{bileşik sayı}) = (1-d)^i \quad \text{(Formül 2)}$$

$$P(\text{asal sayı}) = 1 - P(\text{bileşik sayı}) = 1 - (1-d)^i \quad \text{(Formül 3)}$$

Miller&Rabin testinde yoğunluk daha fazla olduğu için daha az adımda seçilen eşiğe ulaşılabilir. Lehmann yönteminin bir rastsal sayı için uygulanması sonucunda 1 veya -1 çıkarsa sayı testi geçmektedir. Yine de o sayının bileşik olma olasılığı 0,5 den daha az olmakla beraber hala mümkündür. OAT sonucunda hata payının daha da düşmesi için iterasyon değeri arttırılabilir. Aslında bu oranlar oldukça abartılıdır. Çoğu rastsal sayı için, rastsal seçilen bir a değerinin tanık olma olasılığı %99,99 'dur (Schneier, 1996).

Yalancı-tanıklık (non-witness) Kavramı

Bir bileşik n sayısı için, W(n) kümesi n'in asal olmadığını kanıtlayabilecek sayılardan yani tanık sayılardan oluşsun. Tümleyen küme L(n), $L(n) = Z_n - W(n)$ elemanlarından oluşacaktır ve bu kümenin elemanları yalancı-tanık olarak adlandırılır. Eğer testlerde parametre olarak yalancı-tanıklar kullanılırsa yanlış sonuçlara ulaşılması mümkündür. Çünkü testler bileşik sayının asal olduğunu bildireceklerdir. Bu tür yanlışlıklarla karşılaşmamak için bu tür testleri (yeteri kadar büyük bir t sayısı için) t kere tekrarlamamız hata olasılığını daha da düşürecektir (Menezes ve Oorschot, 1997). Miller&Rabin testi için yalancı-tanıkların sayısının çok az olduğu Higgins'ın yaptığı araştırmalarda ortaya çıkmıştır (Higgins, 2000).

Fermat Testi

Pierre de Fermat'ın teoremine göre herhangi bir n sayısının asal olması için [1, n-1] aralığından alınan bir a sayısı ile $a^{(n-1)} = 1 \pmod n$ eşitliği sağlaması gerekmektedir. Bu test, olası asallık testlerinin temelini oluşturmaktadır (Menezes ve Oorschot, 1997). 256 bit rasgele bir sayının bu testi geçip asal olmama olasılığı 10^{22}'de 1'dir (Rivest, 1990).

Örneğin: a=2 ve n=3 için $2^{3-1} = 1 \pmod 3$ $2^2 = 1 \pmod 3$ $4 = 1 \pmod 3$ görüldüğü gibi n=3 sayısının asal olduğunu hesapladık.

Fermat testi, Carmichael sayılarını tespit etmekte başarısız kalmaktadır. Diğer OAT, Fermat'ın teoremini temel olarak alsalar da aynı zamanda diğer birçok durumu da kontrol ettiklerinden daha gerçeğe

yakın sonuçlar döndürmektedirler. Fermat Teoreminin karşıtı doğru değildir. Yani $n \neq a$ ve $a^{n-1} \equiv 1 \pmod n$ olması *n* nin asal olmasını gerektirmez.

Lehmann Testi

n sayısının asal sayı olup olmadığını test etmek için rastgele olarak seçilen a sayılarıyla, b değeri Formül 4 ile hesaplanır (Segre, 2000). Eğer bütün b değerleri 1 veya –1 ise, fakat yalnız 1 veya yalnız -1 değilse n asal olarak kabul edilebilir (Menezes ve Oorschot, 1997).

$$b = a^{((n-1)/2)} \pmod n \qquad \text{(Formül 4)}$$

Legendre'nin geliştirdiği n/a Legendre sembolü bu foknsiyonun temellerini oluşturur. Legendre Sembolü'nün aldığı değerler ve açıklamaları Tablo 5'de belirtilmiştir (Menezes ve Oorschot, 1997).

Tablo 5. Legendre Sembolü Değerleri ve Açıklamaları

$\frac{a}{n}$	+1	eğer a, mod n'ye göre "quadratic residue" ise
	-1	eğer a, mod n'ye göre "non-quadratic residue" ise
	0	Eğer a, n'i bölerse

Euler'in teoremine göre, obeb(a,n) =1 ve n bir asal sayıysa Formül 5'deki eşitlik sağlanmaktadır. Bu teorem verilen n sayısının asal olup olmadığını test etmek için kullanılabilir. Sonuç olarak a tabanına göre Euler sözde asalı Formül 7'de olduğu gibi de ifade edilebilir. Yeteri kadar a sayısı denediği zaman n'in asal olup olmadığı anlaşılabilmektedir.

$$\left(\frac{a}{n}\right) = a^{(n-1)/2} \pmod n \qquad \text{(Formül 5)}$$

$$a^{(n-1)/2} = \left(\frac{a}{n}\right) \pmod n \qquad \text{(Formül 6)}$$

$$b = a^{((n-1)/2)} \pmod n \qquad \text{(Formül 7)}$$

Pretty Good Privacy (PGP) ilk başlarda $a^{(n-1)}$ değerini sadece bir a değeri için hesaplıyordu. Buradan çıkan sonuç 1 ise n'in asal olduğunu varsayıyorlardı. Ama bazı sayıların bu formülü sağladığı halde asal olmadığı görülmüştür. Carmichael Sayıları olarak bilinen bu sayılar bütün a değerleri için $a^{(n-1)} = 1 \mod n$ eşitliğini sağlamaktadır. Aynı sorun $a^{(n-1)/2} = 1 \mod n$ formülündeki a sayısı içinde geçerli olabilir. Eğer t adet rastsal seçilmiş a sayısı kullanıldıysa ve n asal değilse b değerinin 1 veya –1 den farklı sayı gelme olasılığı en azından $2^{(-t)}$ olmaktadır. t sayısını olabildiğince büyük alınırsa bu olasılık azaltılabilir. Böylece testin daha kesin sonuçlar vermesini sağlanabilir.

Slovay & Strassen Testi

Açık-Anahtar Kriptografisinde kullanılmış ilk testtir. Slovay-Strassen Algoritmasında n sayısının asal olup olmadığını bulmak için Jacobi Semboli kullanılmaktadır. Jacobi Sembolü n asal ise Legendre Sembolüne eşit olmaktadır. Algoritmanın aşamaları aşağıdaki gibidir(Schneier, 1996):

1. n 'den ufak rastsal bir sayı olan a seçilir
2. Eğer gcd (a,n) ≠ 1 ise o zaman n testi geçemez ve asal olmadığı anlaşılır.
3. $j = a^{(n-1)/2} \mod n$ hesaplanır.
4. Jacobi sembolü olan J (a, n) hesaplanır.
5. Eğer j ≠ J (a, n) ise n testi geçemez ve kesin olarak asal değildir.
6. Eğer j = J (a, n) ise n'nin asal olmama olasılığı %50'den fazla olamaz.

Slovay & Strassen Testi yerine kendisinden daha hızlı ve en az onun kadar doğru olan Miller-Rabin'in kullanılması önerilmektedir (Menezes ve Oorschot, 1997).

Miller&Rabin Testi

Miller-Rabin Testi (M&R Testi) güçlü asallık testi olarak bilinir. M&R Testinde, n sayısının asal olup olmadığını test etmek için ilk önce Formül 8'i sağlayan s ve r değerleri hesaplanır (Menezes ve Oorschot, 1997).

$n - 1 = 2^s r$ (Formül 8)

[1, n-1] aralığından taban olarak kullanılacak bir a değeri seçilir. Formül 9 veya Formül 10'daki eşitlik sağlanıyorsa n sayısının a tabanına göre güçlü asal olduğu kabul edilir (Menezes ve Oorschot, 1997).

$a^r = 1 \pmod n$ (Formül 9)

$a^{2^j r} = 1 \pmod n \ (0 \leq j \leq s-1)$ (Formül 10)

n sayısının asallığını test ederken; n aday asal sayısı 2'den büyük ve tek herhangi bir tamsayı, a taban değeri ise 2 … n-1 dizisinden seçilmiş rastsal bir sayı olsun. C(n,a) bileşik "boolean" fonksiyonunun özellikleri aşağıda belirtilmiştir (SCM, 2000):

• Eğer n asal ise, C(n,a) fonksiyonu sonucu "2 … n-1" aralığındaki her a için yanlış (false) olmalıdır.

• Eğer n bileşik ise C(n,a) fonksiyonu sonucu "2 … p-1" aralığındaki a'ların en fazla ¼ 'ü için yanlış olmalıdır. Eğer taban a için test başarısız olursa; n, a tabanına güçlü sözde asal olarak tanımlanır.

Bu test, diğer rastsal tabanlar için tekrarlanabilir. Bu test ile n sayısının kesin olarak asal olup olmadığı ispatlanabilir. Bunu yapmak için n sayısının asallık testini 1/4 n +1 adet taban için uygulamak gerekmektedir. Ancak büyük sayılar için bu çok zaman alacağından sadece belirli bir kısmında uygulanmaktadır. Bu yüzdende n sayısının asal olup olmadığı olası olarak belirlenmektedir. Asal olma olasılığını azaltmak için çok fazla tabanla bu işlem yapılmalıdır. Asal olma olasılığını hesaplamada t adet taban için testi geçen sayının maksimum $(¼)^t$ asal olacağı anlaşılır. Mesela test 30 kez tekrarlandığında, testi geçen sayının asal olmama olasılığı en fazla $8{,}3 \times 10^{-25}$ olacaktır. Bu da: 0,000000000000000000000000083 olmaktadır (SCM, 2000). Daha gerçekçi hesaplamalar da yapılmıştır. x bit asal adaylarında (x>100), bir tabanla uygulanan bir testin hatalı sonuç döndürme olasılığı k katsayısı için $(\frac{1}{4x})\ (2^{k/2})^{1/2}$ 'den daha düşük olmaktadır. 256 bitlik bir n sayısı için, 6 test sonucunda hatalı cevap alma olasılığı 2^{-51}'den daha düşük olmaktadır(Schneier, 1996).

M&R Testinde, bileşik sayıların asal sanılma olasılığı daha azalmaktadır. a sayılarının en az 1/3 'ünün tanık olması garantidir (Schneier, 1996). Bu test için yalancı-tanıkların çok az olduğu Higgins'ın yaptığı araştırmada ortaya çıkmıştır (Higgins, 2000). Bununla birlikte, testi geçen bileşik sayıların varlığı da bilinmektedir. Alford, Granville ve Pomerance tarafından bu bileşik sayıların varlığı kanıtlanmıştır. Bleichenbacher, 100'den küçük ve eşit tabanlar kullanıldığında M&R testini geçen 55 basamaklı bir bileşik sayı bulmuştur. M&R testinin 2, 3, 5, 7, 11, 13 ve 23 tabanlarına göre uygulandığında 10^{16}' dan küçük sayılar için doğru bir asallık testi olduğu kanıtlanmıştır. Çeşitli tabanlar için kullanılabilecek aralıklar Jaeschke tarafından belirlenmiştir (Maurer, 1994).

M&R Testinin Uygulaması

n rastsal sayısının M&R asallık testi için ilk önce n-1'in ikiye bölünme sayısı olan s değeri ile Formül 10'daki eşitliği sağlayan r değeri hesaplanır. Geriye kalan aşamaların adım adım uygulanması aşağıda verilmiştir (Schneier, 1996):

1. n den küçük olacak bir rastsal a sayısı bulunur.
2. j = 0 olarak ayarlanıp $z = a^r \bmod n$ hesaplanır.
3. Eğer (z = 1) veya (z = n – 1) ise n asallık testini geçer ve asal olabilir.
4. Eğer (j > 0) ve (z = 1) ise n asal değildir.

5. j = j + 1 olarak ayarlanır. Eğer (j < s) ve (z ≠ n-1) ise ($z = z^2 \bmod n$) olarak ayarlanır ve 4. Adıma geri dönülür. Eğer (z = n – 1) ise n asallık testini geçer ve asal olabilir.
6. Eğer (j = s) ve (z ≠ n - 1) ise o zaman n sayısı asal değildir.

M&R Testinde Asal Taban Almanın Avantajları

M&R Testi güçlü asallık testi olarak bilinir. Böyle olmasına rağmen bu testi yanıltan sayılar vardır. M&R Testini yanıltan sayılara güçlü yalancı tanık denir. Bazı bileşik sayılar, çok az sayıda güçlü yalancı tanığa sahiptir. Mesela bileşik 105 (3 x 5 x 7) sayısının yalancı tanıkları 1 ve 104'tür. Buradan varılan genelleme şudur: Bir n sayısı 2 veya daha fazla ilk tek asal sayının çarpımından oluşuyorsa bu sayının yalancı tanıkları sadece 1 ve n-1 olmaktadır. Güçlü yalancı tanıklar yüzünden M&R testinde yanlış sonuçlara varılmaması için taban olarak ilk asalların (2, 3, 5, 7 gibi) alınması önerilmektedir. Birçok bileşik sayı için güçlü yalancı tanıkların adedi, $Q(n)$[36] fonksiyonu için maksimum Q(n) / 4 olmaktadır (Menezes ve Oorschot, 1997).

Frobenius Testi

Frobenius Sözde Asalı, Sonlu Alan kuramına dayanmaktadır. Ayrıca bu kurama dayanan Frobenius testinin diğer testlerin genelleştirilmesi ve güçlendirilmesi ile oluşturulduğu belirtilmektedir (Grantham, 1998).

Frobenius testi ile bir bileşik sayıyı asal olarak belirleme hata oranının 1/7710 olduğu ölçülmüştür. Frobenius testinin M&R testinden üç kat daha yavaş çalıştığı ama 3 round'lu M&R testinin hata oranının en fazla $(1/4)^3=1/64$ olduğu belirtilmiştir. Bu da Frobenius testinin aynı zaman aralığında M&R testinden daha az hata oranı ile çalıştığını göstermektedir (Grantham, 1998).

Pratikte Asal Sayı Üretme Esasları

Asal sayı üretmek için aşağıda belirtilen aşamalar adım adım uygulanmalıdır:

1. n-bit rastsal sayı p üretilir.
2. İlk bit ve son bit'ler 1 olacak şekilde ayarlanır (Son bit'in 1 olması o sayının tek olmasını sağlamakta, ilk bit'in 1 olması da asal sayının istenilen (required) uzunlukta olduğunu belirlemektedir).
3. p'nin ufak asal sayılara (3,5,7,11 …) bölünmediği kontrol edilmelidir. Birçok uygulamada 256'dan küçük bütün asallarla kontrol ederken, en etkin olanı 2000'den küçük asallara bölünmediğini kontrol etmektir.
4. Miller&Rabin testi bir rastsal a değeri için uygulanır. Eğer p bu testi geçerse başka rastsal a değerleri için bu test tekrarlanabilir. Ufak a değerleri seçilmelidir ki hesaplamalar daha hızlı olsun. Testte kullanılacak a değerlerinin sayısı 5 (Seth, 1999) veya 10 (Segre, 2000) olarak seçilebilir. Eğer p değeri bu testlerden birisini geçemezse asal bir sayı değildir ve başka bir p değeri yaratılıp aynı işlemlerden geçirilmesi gerekecektir [11,17].
5. Miller&Rabin testini geçen sayılar, Lucas veya Frobenius testine sokularak daha güvenilir sonuçlar elde edilebilir (Silverman, 1997).

Her seferde rastsal p değeri oluşturmak yerine, ilk seferden sonra başlangıç rastsal sayısını arttırarak asal bir sayı bulana kadar da işleme devam edilebilir [11,17].

Asallık testinin yeterince kuvvetli olması için, testte sayının basamak adedi kadar taban (a değeri) alınması tavsiye edilmektedir (Pinch, 1994). Dikkat etmemiz gereken temel kriter, hata oranının 2^{-100} 'den daha büyük olmaması gerektiğidir (Silverman, 1997). Digital Signature Standard (DSS)'de; üretilen sayıların asallığını test ederken, Miller&Rabin algoritmasının en az 50 kez kullanılmasıyla kabul

edilecek bir hata olasılığına, yani 2^{-100} 'e ulaşılabileceği belirtilmektedir (Burrows, 1994).

SONUÇ VE ÖNERİLER

Kesin veya Olası Asallık testleri uygulanmadan önce bu sayıların Ufak Asallara Bölme testinden geçirilmesi testlerden daha kısa sürede sonuç almamıza olanak sağlamaktadır. Tek sayıların 3, 5 ve 7 ile bölüp bölünmediğinin testinin bu sayıların %54'ünü, 100'den küçük asallara bölmenin %76'sını, 256'dan küçük sayılara bölmenin ise %80'ini elediği tespit edilmiştir.

Lehmann testi, Slovay&Strassen'in bir varyasyonudur. Bu yüden Lehmann dışındaki diğer üç temel testi karşılaştırdığımızda Miller&Rabin testinin daha iyi olduğu ortaya çıkmaktadır. Bunun nedenleri ise Fermat testi, Carmichael sayılarını bulmakta zayıf kalmaktadır. Solovay&Strassen testi, çalışma zamanı olarak daha uzun sürmekte ve Jacobi sembol hesaplamaları yüzünden uygulanması daha zordur. Slovay&Strassen testi $(1/2)^t$ hata payıyla çalışırken Miller&Rabin testi $(1/4)^t$ hata payıyla daha gerçeğe yakın sonuçlar sunmaktadır.

Miller&Rabin testi en kötü şartlarda bile en fazla diğerleri kadar çalışmaktadır. Miller&Rabin ile birlikte Lucas veya Frobenius testlerinin birlikte kullanılması önerilmektedir. Bu sayede hata payı çok aza indirilmiş olacaktır.

KAYNAKLAR

1. BURROWS, J.H., Digital Signature Standard (DSS), *Federal Information Processing Standards Publication*, 1994.
2. CALDWELL, Chris K., The University of Tennesse at Martin, *Practical Applications of Prime Numbers*, 2002.
3. CAN, Ö., Asal Sayı Örüntüleri Ve Goldbach Sanısı Üzerine Bir Çalışma, 2002
4. GRANTHAM, J., A Probable Prime Test with High Confidence, *Journal of Number Theory*, 72, 1998.
5. GRANVILLE A., Primality Testing & Carmichael Numbers, Notices Amer. Math. Soc. 39, 696-700,1992.
6. HIGGINS, B.C., The Rabin-Miller Probabilistic Primality Test, Some Results on the Number of Non-Witnesses to Compositeness, 2000.
7. KARAARSLAN, E., Büyük Ölçekli Rastsal ve Asal Sayı Üretimi, 2001.
8. MAURER, U.M., Fast Generation of Prime Numbers& Secure Public-Key Cryptographic Parameters, *Journal of Cryptography*, 1994.
9. MENEZES, A. and OORSCHOT, P., Handbook of Applied Cryptography, CRC Press, 1997
10. O'CONNOR, J.J. and ROBERTSON, E.F., Prime Numbers, 2001.
11. PINCH, R.G.E., Some Primality Testing Algortihms, Proc 4th Rhine workshop on Computer Algebra, Karlsruhe, 1994.
12. RIVEST, R., Finding Four Million Large Random Primes, Advances in Cryptology, CRYPTO'90, LNCS 537, 625-626, 1990.
13. RSA, RSA FAQ v4, Frequently Asked Questions About Today's Cryptography – What's Primality Testing?, 1998.
14. SCHNEIER B., Applied Cryptography (Second Edition), John Wiley & Sons Inc, 1996.
15. SCM, Theory of the Miller&Rabin Test, Scheme Library, 2000.
16. SEGRE, A., Computer and Network Security, Iowa Üniversitesi "Data Security" Ders Notları, 2000.
17. SETH, A., The Data Encryption Page Newsletter , 1, 1–2, 1999.
18. SILVERMAN, R.D., Fast Generation of Random, Strong RSA Primes, RSA Laboratories' Crypto Bytes Magazine, 1997.
19. The University of Sheffield, Department of Pure Mathematics, 1999.
20. YERLIKAYA, T., Yeni Şifreleme Algoritmalarının Analizi, 2006.
21. YERLIKAYA, T., GENÇOĞLU, H., EMIR, M.K., ÇANKAYA, M., BULUŞ, E., Rsa Şifreleme Algoritması Ve Aritmetik Modül Uygulaması.
22. YILTAŞ, D., Kriptolojide Kullanılan Asal Sayı Test Algoritmalarının Performans Açısından Karşılaştırılması, 2003.