Mesajların Şifrelenmesinde Yeni Bir Yöntem ve Android Uygulaması

(A New Approach for Encryption and Application for Android)

Arzu Çakmak
İTÜ Bilgisayar ve Bilişim Fakültesi
cakmakar@itu.edu.tr

Eşref ADALI
İTÜ Bilgisayar ve Bilişim Fakültesi
adali@itu.edu.tr

Özetçe

Gelişen teknoloji, artan bilgi birikimi ve trafiği ile bilgilerin güvenliğini sağlamak kaçınılmaz bir gereksinim haline gelmiştir. Akıllı telefonların varlığı ile tüm bilgilerimiz ve iletişimimiz artık telefonlar üzerinden yapılmaktadır. Bu anlamda bilişim etiği önemli bir kavram olarak karşımıza çıkmaktadır. Bilişim etiği açısından da önemli olan mahremiyet açısından, bilgilerin başkaları tarafından görülmesi istenilmemektedir.

Bu amaç doğrultusunda çok karmaşık olmaması koşulu ile bir şifreleme yöntemi günümüzde yaygın olarak kullanılan Android işletim sistem üzerinde geliştirilmiştir.

Geliştirilen şifreleme yöntemi, şifrelemek ve şifrelenmiş metni çözmek için matris yapısında bir maske kullanmaktadır. Tüm şifreleme işlemleri gerçekleştirildikten sonra, elde edilen matrislerdeki karakterlerin ASCII kod karşılıkları alınarak bitmap resim formatına çevrilmektedir. Alıcı mesajı aldığında, anlamsız bir resim görmektedir.

Şifreleme yönteminin, kullanım amacı açısından basit olması istenmiştir. Yapılan çalışmanın amacı, cep telefonu ile gönderilen mesajların şifrelenerek gönderilmesini sağlamaktır.

Geliştirilen şifreleme yöntemi, temel olarak bir simetrik ve doğrusal olmayan şifreleme yöntemidir.

Anahtar Sözcükler *:* Şifreleme, Android

Abstract

Day by day; the technology, information and information tranmission are getting bigger. And also, smart phones are so popular. People use these smart phones to communicate. Under these conditions, privacy is the natural right. So, the cryptography is a necessary in these days for information security.

In this work a new cryptographic algorithm is developed as easy as possible. The algorithm is carried out by developing as Android Application. The developed algorithm uses a matrix in order to encrypt a message by rotating the key matrix .

After performing all cryptographic operations, the resulting matrixes' characters are converted into ASCII code. Than, it creates a bit map image to send it to the receiver. Then the receiver transfer the image to the converter in order to retrieve the plain text from the encrypted image. The converter decrypts the image with the key supplied by the user.

The developed encryption algorithm is base on symmetric and non linear algorithm.

Key words: *Encryption, Android*

1. Giriş

Kişiler veya kurumlar arası haberleşmede gizli kalması gereken bilgiler olabilmektedir. Özellikle askeri alanda çok eski çağlardan beri iletişimde gizlilik önemli bir konu olmuştur. İletinin gizli tutulması konusunda günün sağladığı teknik imkânlara göre gizliliği sağlayacak yöntemler araştırılmış ve kullanılmıştır.

Eski Mısır'da, Mısır hiyeroglif yazı ile metinlerin şifrelendiği; ulağın kafasını tıraş edip, kafasına iletinin yazıldığı ve saçları uzadıktan sonra karşı tarafa gönderildiği bilinen en eski yöntemlerdir. Daha sonraları Sezar şifresinin ve bir harfe karşılık şekil ya da bir sayının karşı düşüren yöntemlerin kullanıldığı bilinmektedir. Bu yöntemlerin ortak özelliği, bir harfe karşılık düşürülen harf veya

karakterin aynı olmasıdır; bir başka deyişle doğrusal olmalarıdır.

Bir harfe karşılık her seferinde farklı bir harfi karşılık düşürmeyi amaçlayan en gelişmiş mekanik şifreleyici Enigma'dır. Bilgisayar teknolojisinin gelişmesiyle daha gelişmiş şifreleme yöntemleri üretilmiştir. Bunlar arasında DES, 3-li DES, AES ve RSA sayılabilir.

2. Yakın Çalışmalar

Bu çalışmada geliştirilen ve tanıtılan şifreleme yöntemi, matris yapısındadır. Çalışmamızı çok yakın bir şifreleme yöntemi bulunmamakla beraber, kaynaklarda görülen en yakın şifreleme yöntemleri Polybius [1] ve Tabula Recta [2] şifreleme yöntemleridir. Bu iki yöntemde, düz metin matris içine şifreleme yöntemine uygun olarak yerleştirilmektedir.

3. Önerilen Şifreleme Yöntemi

Bu makalede tanıtlan şifreleme yönteminde, ham metnin harfleri bir matris içine yerleştirilmektedir. Harflerin matrise yerleştirilmesi sırasında kalbur ya da maske adını verdiğimiz, çapraz bulmacaya benzer bir araç kullanılmaktadır. Kalburun bazı yerleri delik bazı yerleri kapalıdır. Metin matrise yerleştirilirken kalburun delik olan kısımlarına yazılır. Kalbur ekseni etrafına dört kez döndürülerek tüm metin matris alanına yazılır. Matris içinde boş kalan alanlara, daha sonra rastgele harfler yazılır. Şifrelenecek metin bir matrise sığmadığında, ikinci bir matris oluşturulur.

Kalbur üzerindeki deliklerin oluşturulması çalışmamızın ana konusudur. Bu deliklerin birbiri ile çakışmadan ve karmaşık yapıda nasıl hazırlandığı aşağıda ayrıntılı biçimde anlatılmıştır.

Çalışma kapsamında kullanılmış olan bazı tanımlar şunlardır:

Eşlenik: Matristeki bir deliğin (gözün) 90 derece döndürüldüğünde yeni konumudur.

Sayfa Numarası: Birden çok matris oluşturulduğunda, her bir matrisin sıra numarasıdır.

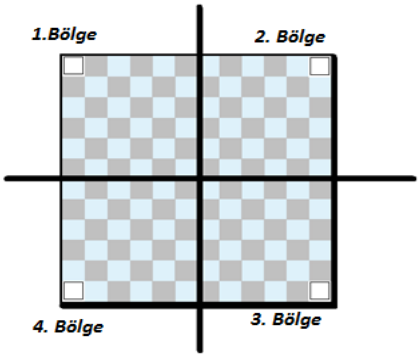
Şifreleme Yönteminin Adımları:

1. Matris boyutu istenildiği gibi seçilebilir. Örnek olması açısından 12x12 lik bir matris seçilmiştir. Söz konusu matris üzerinde belli gözler delinecek belli gözler kapalı tutulacaktır. Delinecek gözlerin rastgele olması, ancak, kalbur dört kez 90 derece döndürüldüğünde deliklerin üst üste gelmemesi gerekmektedir. Bu kuralları sağlamak üzere deliklerin nasıl belirleneceği aşağıda adım adım anlatılmıştır:
2. Şifrelenecek ham metnin harfleri; sadece delik gözlere gelecek şekilde yerleştirilmeye başlanır. Ardından matris 90 derece saat yönünde döndürülür ve delik olan alanlara ham metnin harfler yerleştirilmeye devam edilir. Bu işlem dört kez yinelenir.
3. Deliklerin sayısı ham metnin tüm harflerini sığdırmak için yetmez ise, yeni bir matris oluşturulur.

Ham metnin bu şekilde matrise yerleştirilmesinin ardından, bazı alanların boş kalacağı açıktır. Boş alanlara, rastgele harfler yerleştirilmektedir. Delik sayısının, metindeki harf sayısından fazla olduğu durumda, deliklere rastgele harfler yazılır. Parola içinde anlamlı harflerin bitiş yeri iletildiği için, anlamsız harfler kolaylıkla asıl metinden ayrılırlar.

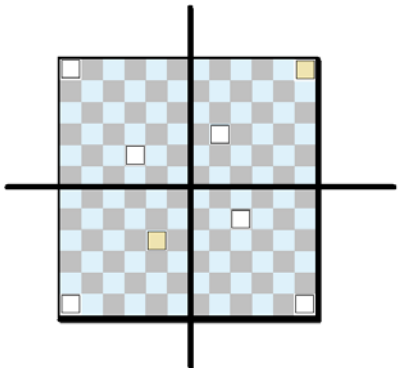
Kalbur üzerinde bulunan deliklerin, kalburun dört dönüşünde üst üste gelmemeleri koşulu, metnin harflerinin birbirini ezmemesini sağlamaktadır. Yani bir deliğin eşleniği ile çakışmaması için eşlenik gözlerden sadece bir tanesinin seçilmesi sağlanmaktadır. Bu yapıyı sağlamak üzere bir yöntem geliştirilmiştir. İlk olarak matris eşit boyutta dört bölgeye ayrılır. Örneğin 12x12 lik matris, 4 tane 6x6 matrise bölünür ve her biri saat dönüş yönünde numaralanır. Yöntemin nasıl çalıştığı aşağıda anlatılmıştır.

- I. Bölgede rastgele bir delik seçilir. Seçilen bu deliğin eşlenikleri II., III.ve IV. bölgede belirlenir. Durum Şekil-1 ve Şekil-2'de gösterilmiştir. Ortaya çıkan bu dört delikten biri rastgele seçilir ve eşlenikleri elenir. Şekil üzerinde açıklarsak; ilk delik I. Bölgede (1,1) gözü olarak seçilmiştir. Bu durumda (1,12), (12,12) ve (12,1) eşlenik delikler olacaktır. Şekil-2'de bu dört delikten biri (1,12) rastgele seçilmiştir. Seçilen delik, Şekil-2'de farklı tonda gösterilmiştir.



Şekil-1: Geliştirilen şifreleme algoritmasında ilk anahtar seçimi

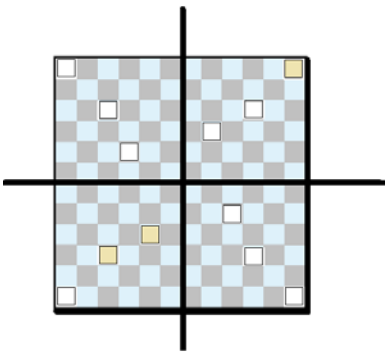
- İkinci adımda, I. Bölgede rastgele yeni bir delik seçilir (5,4). Bu delik için de eşlenik delikler belirlenir (4,7), (8,8), (8,5). Ortaya çıkan dört yeni delikten biri (8,5) rastgele olarak seçilir, diğerleri elenir. Durum Şekil-2'de gösterilmiştir.



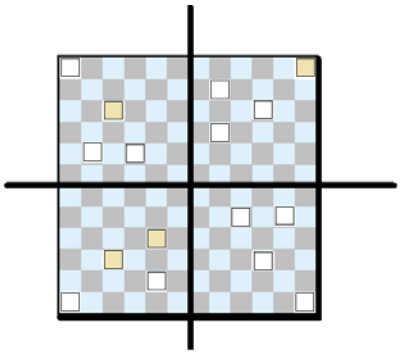
Şekil-2: Geliştirilen şifreleme algoritmasında ikinci anahtar seçimi

Birinci bölgeden seçilecek delik sayısı, kullanıcının isteğine bağlı olarak 18'e kadar çıkarılabilir. Delik sayısının artması, şifreleme algoritmamızın karmaşıklığını azaltmaktadır.

Her eklenecek delik için yukarıda anlatılan adımlar tekrarlanır. 3. ve 4. Delikler için örnekler Şekil-3 ve Şekil-4'te gösterilmiştir.



Şekil-3: Geliştirilen şifreleme algoritmasında üçüncü anahtar seçimi



Şekil-4: Geliştirilen şifreleme algoritmasında dördüncü anahtar seçimi

Yukarıda anlatılan biçimde, kalburdaki deliklerin kurallara uygun ve rastgele belirlenmesini sağlamak üzere bir algoritma geliştirilmiş ve bu algoritmaya uygun olarak çalışan bir program hazırlanmıştır.

Şifreleme yöntemimizin karmaşıklığı orta değerde tutmak adına I. Bölgede 18 rastgele delik seçilmiştir. Bu 18 deliğin diğer üç bölgede eşlenikleri belirlendiği ve bunlar içinden sadece bir tanesi seçildiğinde, 12x12 matris içine 72 karakter sığdırılabilmektedir.

Kalburu matris üzerinde dört kez döndürerek oluşan deliklere ham metnin harflerini teker teker yazarak metin şifrelenmiş olmaktadır. Daha önce belirtildiği gibi, matriste boş kalan alanlara rastgele harfler yazılmaktadır.

Şu ana kadar yapılan şifreleme yöntemi doğrusaldır. Şifrelemenin doğrusallığını bozmak için şöyle bir yöntem uygulanmıştır: Matrisin her kutusu, satır ve sütun numarası olarak düşünülmektedir. Satır ve

sütun numarası dörder bit halinde Şekil-5'teki gibi tutulmaktadır. Matrise yerleştirilen her harfin ASCII karşılığı bu konum değeri ile YADA'lanmaktadır (XOR işlemi). Böylece aynı harfe karşılık farklı harfler üretilmektedir. Bu işlem sadece şifrelenecek metnin harflerine uygulanmaktadır.

0001 0001	0001 0010	0001 0011
0001 0001	0001 0010	0001 0011
0010 0001	0010 0010	0010 0011

Şekil-5: Matris kutucuklarının konum değerleri

YADA'lama işleminden sonra elde edilen ve her bir gözünde 8 bitlik veri bulunan matris yapı daha sonra *bitmap* haline çevrilmektedir. Böylece alıcıya *bitmap* kalıbında bir resim gönderilmektedir.

Verici ve alıcı şifrelenmiş mesajlaşmaya başlamadan önce matris yapısı konusunda anlaşmış olacaklardır. Dolayısıyla geliştirilen şifreleme yöntemi, simetrik ve doğrusal olmayan bir şifreleme yöntemidir.

Üretilen anahtarın, doğal olarak bir başka kanal üzerinden alıcıya gönderilmesi gerekmektedir. Anahtar şu şekilde gönderilecektir:

Örneğin, delik konumları (1,2), (3,4), (4,5), (9,8), (1,1), (2,1)... şeklinde işaretlenecektir. Bu durumda (11,2) olarak gönderilmek istenen delik (1,1) olarak algılanacaktır. Bu şekilde yanlışları engellemek için anahtar gözlerin tek basamaklı ve onaltılık sayı düzeninde numaralandırılmıştır. Örnek anahtarın yeni biçimi;

12344598B2C... şeklindedir.

Alıcı taraf önce resim halinde gelen veriden karakterleri üretir ve bunları matrisin içine yerleştirir. Ardından, matris içinde bulunan her veriyi konum bilgisi ile YADA'lar; daha sonra matris kalburunu dört kez döndürüp asıl metni ortaya çıkarır.

Geliştirilen bu şifreleme yöntemi için ilk adım olarak bir metin düzenleyici gerekmektedir. Bunun için *"android virtual machine"* ile bir metin düzenleyici geliştirilmiştir [9]. Girilen metin "Encyript" düğmesi ile şifrelenmekte ve bir *bitmap* resme çevrilerek alıcıya telefon üzerindeki W*hatsApp* ya da *mms* kullanılarak gönderilmektedir [10].

4. Şifreleme Yönteminin Analizi

Anahtarın çözülme olasılığı şifreleme yönteminin gücünü göstermektedir.

Toplamda 12x12 matrisinde 4'e böldüğümüzde bir alanda 36 kutucuk bulunmaktadır.

Bu 36 kutucuktan n tanesi seçilecektir.

P=$\binom{36}{n}$ farklı kutu seçilme

olasılığı mevcuttur.

Seçilen bu **P** farklı kutu içinden de her biri için anahtarımızı seçebileceğimiz 4 farklı matris bölmesi olduğunda olasılık her bir kutu için 4 farklı olasılık mevcuttur.

Seçilen P farklı kombinasyon ile seçilen n adet anahtar içinde, genel matristeki yer seçimi için;

4^n farklı anahtar kombinasyonu mevcuttur.

Bu demektir ki ;
Anahtar sayısı : **A**
Seçilecek kutucuk sayısı: **n**
Belirli seçilen bir n değeri için;

$A = 4^n P$ yazılabilir

Tüm üretilebilecek anahtar sayısı, [11]

$$\mathbf{A} = \sum_{n=0}^{36} \binom{36}{n} * 4^n$$

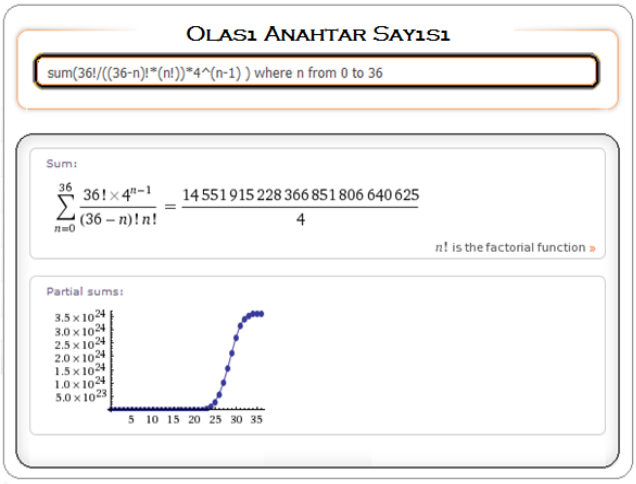
n=1 → 36*4 = 144
n=2 → 630*16=10080
n=3 → 7140*64=456960
n=4 → 58905*256=15079680
n=5 → 376992*1024=386039808.....
....

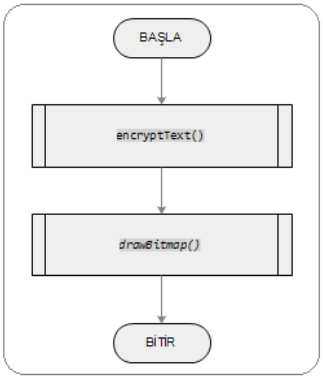
n=12→

$$\sum_{n=0}^{36} \frac{36! \times 4^{n-1}}{(36-n)!\,n!} = \frac{14\,551\,915\,228\,366\,851\,806\,640\,625}{4}$$

Hesaplama WorlframAlpha hesaplama motoru ile yapılmıştır.

Tablo 1: Şifre yöntemindeki anahtar sayısı

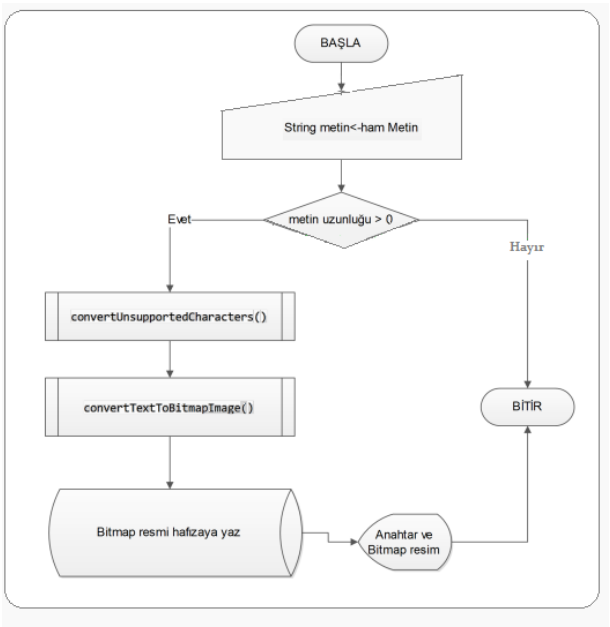




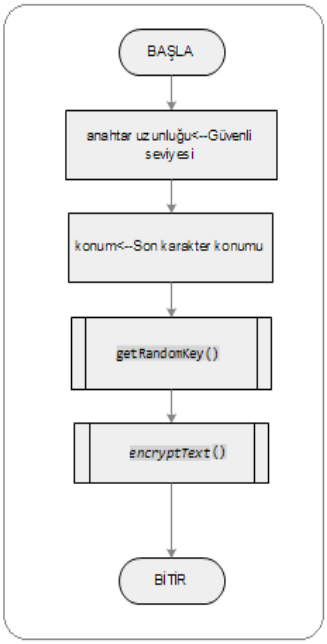
Şekil-7: Şifreleme Modellemesinde "convertTextToBitmapImage()" Akış Diyagramı

5. Gerçekleştirme ve Sınama

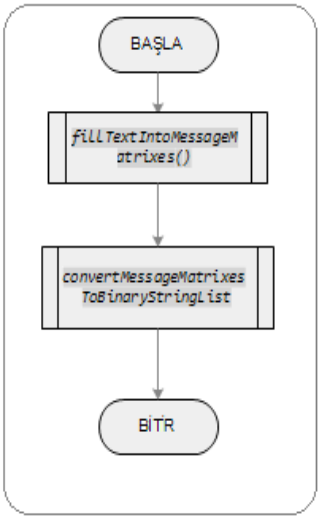
Şifreleme ve şifre çözme, alt yöntemlerine akış diyagramları ile Şekil-6,7,8,9,10,11,12,13 ve 14'te gösterilmiştir.



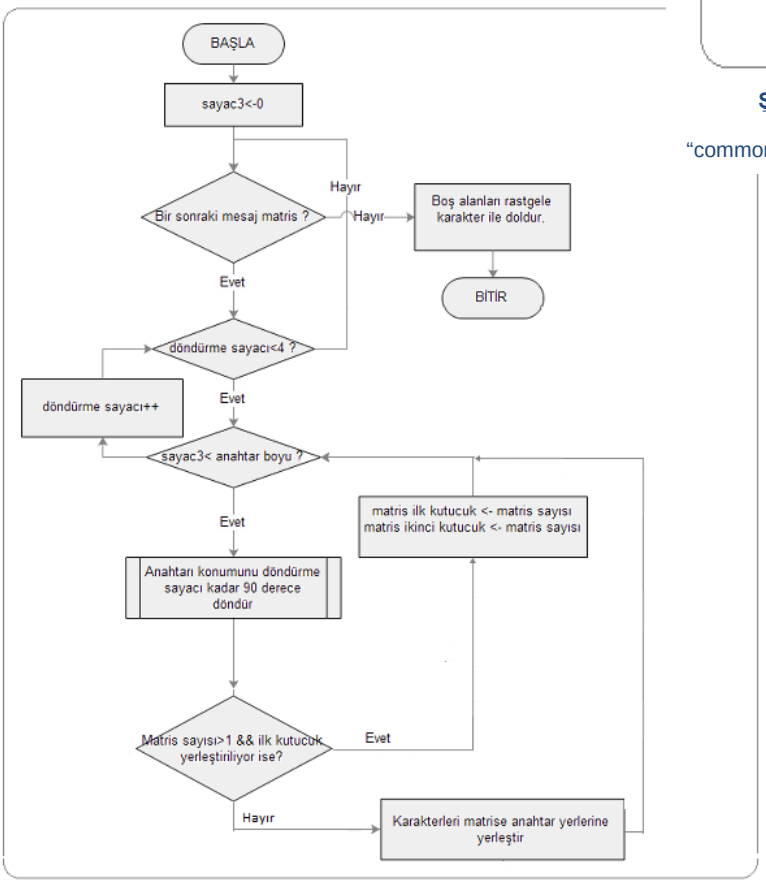
Şekil-6: Şifreleme Modellemesi Akış Diyagramı



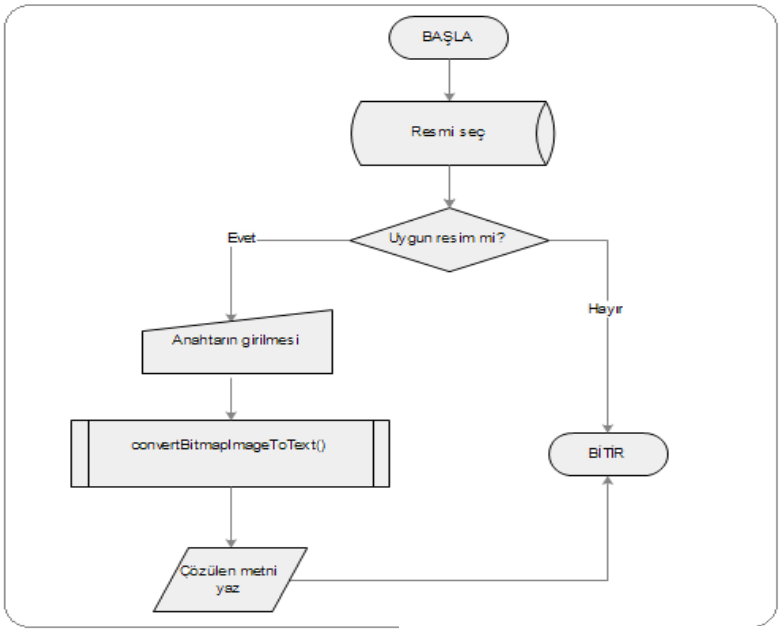
Şekil-8: Şifreleme Modellemesinde"encryptText()" Akış Diyagramı



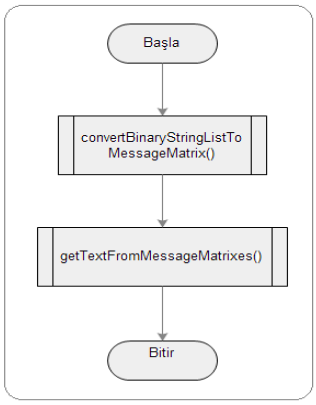
Şekil-9: Şifreleme Modellemesinde "commonController.encryptText()"



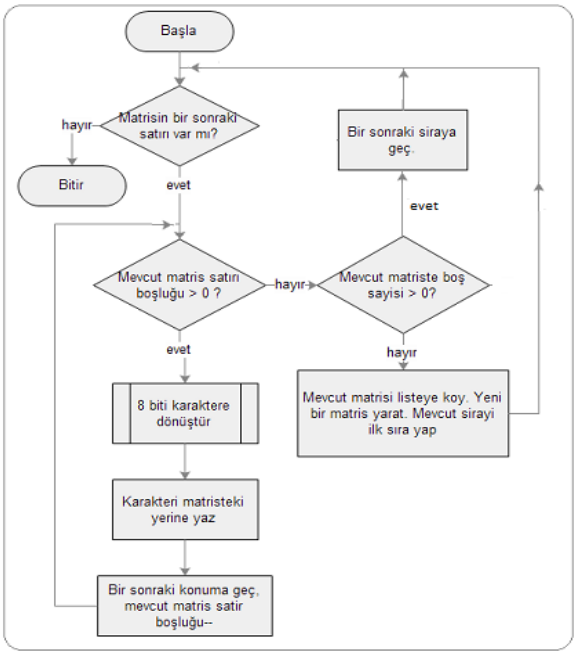
Şekil-10: Şifreleme Modellemesinde "fillTextIntoMessageMatrixes" Akış Diyagramı



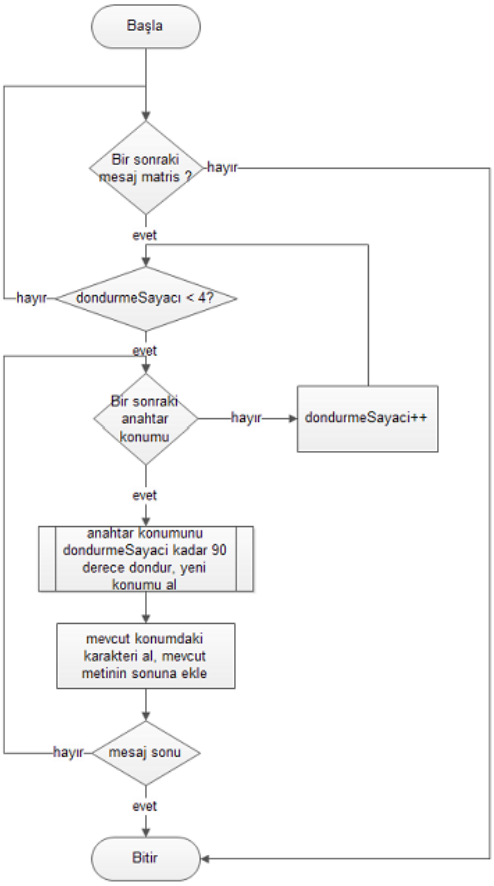
Şekil-11: Şifre Çözümü Akış Diyagramı



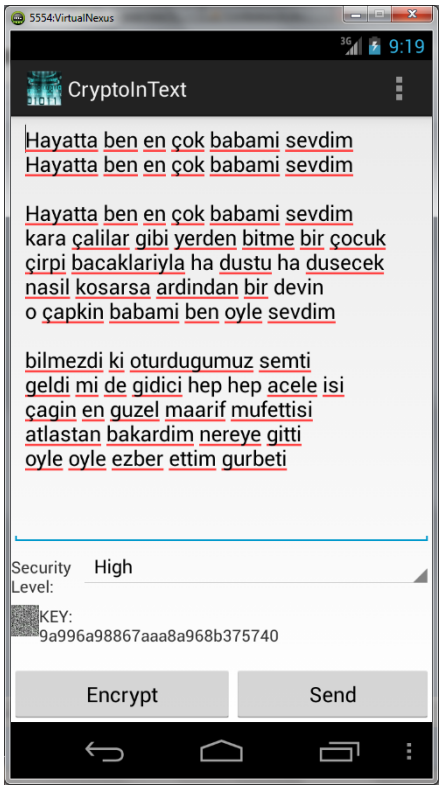
Şekil-12: "convertBitmapImageToText"alt metodu Akış Diyagramı



Şekil-13: convertBinaryStringListToMessageMatrix Akış Diyagramı



Şekil-14: "getTextFromMessageMatrixes" metodu akış diyagramı



Şekil-15: Örnek mesaj

5.1 Arayüz

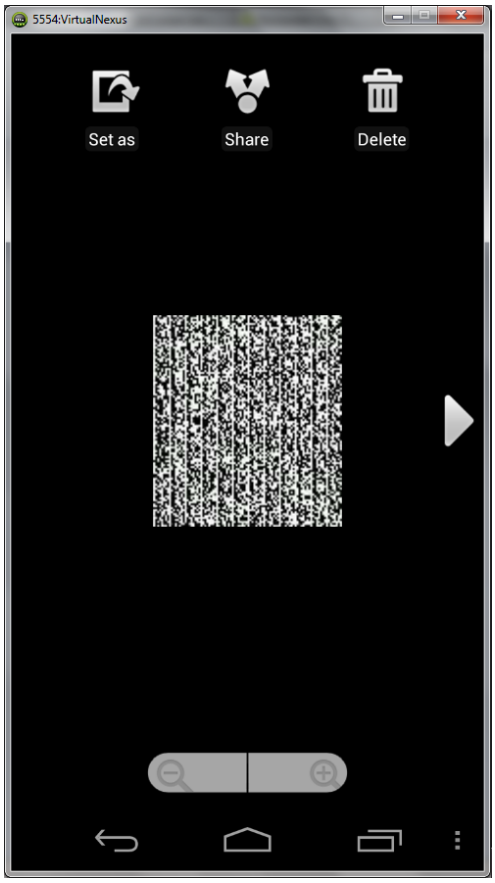
Geliştirdiğimiz şifreleme yöntemini kullanarak mesajlarını göndermek isteyenler için iki arayüz hazırlamamız gerekmiştir. Gönderen taraf için geliştirilen arayüzde, metin yazma alanı ve yazılan metni şifrelemek için bulunan bir düğme,

"Encrypt"düğmesi bulunmaktadır. Şifreleme düğmesine basmadan önce, kullanıcı şifreleme seviyesini seçebilmektedir. Şekil-15'te gönderen tarafa ilişkin arayüz verilmiştir

Kullanıcını belirlediği şifreleme seviyesi ile anahtarın uzunluğu da belirlenmiş olmaktadır. Anahtar ne kadar kısa olursa o kadar güçlü şifreleme gerçekleştirilecektir. Şifreleme seviyesine göre 12x12 matriste 26, 18 ve 12 delikten oluşan anahtar üretilmektedir.

Şifrelenmiş metin, daha önce anlatıldığı gibi resim kalıbına dönüştürülmektedir. Resim kalıbına dönüşmüş mesajın görüntüsü Şekil-16'da verilmiştir.

Alan tarafın arayüzünde ilk olarak Şekil-16'da görülen resim görülecektir. Çözümle seçeneği seçildiğinde, mesaj metni Şekil-15'teki gibi görülmektedir.



Şekil-16: Şifreleme sonrası

6 Sonuç ve Öneriler

Metinleri şifrelemek için geliştirilmiş çok sayıda şifreleme yöntemi bulunmaktadır. Bu yöntemlerin bazıları simetrik bazılar asimetriktir. İki kişi tarafından cep telefonu üzerinden mesajlaşma için simetrik bir yöntemin kullanılmasının uygun olacağı düşünülmüştür.

Yakın dönem şifreleme yöntemlerinde, doğrusal şifreleme yöntemleri kullanılmamaktadır. Geliştirilen şifreleme yöntemi de bu nedenle doğrusal değildir.

Şifreleme algoritması, bu çalışmada anlatıldığı gibi açıktır ve analizi yapılmıştır. Gizli olan şifreleme sırasında kullanılan anahtardır. Anahtarın boyu şifrelemenin gücünü değiştirmektedir. Değişik boyda anahtar kullanarak elde edilecek çözüm olasılıkları hesaplanmıştır.

Bir şifreleme algoritmasından beklenen şifreleme gücü, iletilmek istenen bilginin ne kadar süreyle gizli tutulması gerektiğine bağlıdır. Cep telefonu üzerinden gönderilecek kısa mesajın devlet sırrı olmayacağı düşünüldüğünden, geliştirilen yöntemin sağladığı gizliliğin yeterli olacağı açıktır.

Geliştirilen algoritmanın güvenliğini ilerletilmek istenirse; oluşturulan resim için görüntü şifreleme yöntemleri de uygulanabilir. Resme görsel şifreleme yöntemi uygulanabilir ve bu amaç ile oluşturulan iki farklı resim üst üste getirilerek alıcı tarafa gönderilebilir.

7 Kaynaklar

[1] “The History of Polybius”, penelope.uchicago.edu/tayer/E/Roman/texts/Polybius/

[2] “Tabula Recta”, Wikipedia

[3] J. Robert Buchanan, “An Introduction to Cryptography, Spotlight on Science”, http://banach.millersville.edu/~BobBuchanan/presentations/Spotlight.pdf, 2008

[4] B. Schneier, *Applied Cryptography*, John Wiley & Sons, Inc., 1996.

[5] Mike Knee, “The Basic of Cryptography”, *http://www.snellgroup.com/documents/white-papers/white-paper-Good-Old-Mathematics.pdf ,2008.*

[6] The components of the Enigma machine, http://www.codesandciphers.org.uk/enigma/enigma2.htm

[7] İTÜ/BİDB, “Şifreleme Yöntemleri”, http://www.bidb.itu.edu.tr/?d=1002, 2009.

[8] Sourav Mukhopadhyay, http://www.facweb.iitkgp.ernet.in/~sourav/DES.pdf

[9] Android Development with Eclipse – Tutorial http://www.eclipse.org/resources/resource.php?id=516, 2012.

[10] An Adroid Developers, http://developer.android.com/index.html, 2012.

[11] R. L. Schaffer, M. Mulekar and J. T. Mcclave, *Probability and Statistics for Engineers*, 2010, pp. 170-172.

[12] WolframAlpha Computational Knowledge Engine, http://www.wolframalpha.com/ , 2012.

[13] Feza Buzluca, "Lecture Notes of Object Oriented Modelling and Design", http://ninova.itu.edu.tr/tr/dersler/bilgisayar-bilisim-fakultesi/2097/blg-468e/ekkaynaklar?g197952, 2012.