İSTANBUL AYDIN ÜNİVERSİTESİ DERGİSİ (İAÜD)
Yıl 5, Sayı 17, Sayfa (47 - 60)

MODERN BLOK ŞİFRELEME ALGORİTMALARI

Fatih ŞAHİN
e-mail: fsahin1976@yahoo.com

ÖZET

Şifreleme, Sezar'dan başlayarak gelişmekte, verinin her türlü iletiminde verinin gizlenmesi ve güvenli bir şekilde iletilmesi için kullanılmaktadır. Şifreleme işlemini sağlayan şifreleme algoritmaları bir kripto sistemin temel öğesidir. Bir kripto sistem; şifreleme algoritması, anahtar, açık metin ve şifreli metinden oluşmaktadır. Günümüzde kullanılan modern şifreleme algoritmaları üç ana kategoriye ayrılmaktadır. Bunlardan ilki simetrik şifreleme algoritmalarıdır. Blok şifreleme algoritmaları bu kategoriye girer. Bu tür algoritmalarda şifreleme ve deşifreleme işlemeleri aynı anahtarı kullanır. Kullanılan anahtara gizli anahtar denir. İkinci karma şifreleme algoritmaları üçüncüsü ise asimetrik şifreleme algoritmalarıdır ve şifreleme için gizli anahtarı kullanırken deşifreleme için açık anahtarı, yani herkesin erişebileceği anahtarı, kullanır. Blok şifreleme algoritmaları günümüzde kriptografide önemli bir yer taşımaktadır. Blok şifreler modern şifreleme algoritmaları için oldukça önemlidir. Bundan dolayı veri iletişimindeki güvenlik düşünüldüğünde şifreleme algoritmalarının gücü oldukça önemli bir kriterdir. Diğer yandan, blok şifreler onlara gücünü veren önemli özelliklere sahiptir. Bu çalışmada blok şifrelerin gücünün bir analizini sunduk ve bu amacı gerçekleştirmek için AES (Rijndael), DES ve 3DES algoritmaları incelendi.

Anahtar Kelimeler: DES, 3DES, AES, Blok Şifreleme

1. GİRİŞ

Şifreleme teknikleri her türlü iletişim ve veri depolamada önemli bilgilerin güvenliğini sağlamak için kullanılır. En yaygın ve önemli uygulamalardan biri de Internet üzerinde aktarılan bilginin güvenliğini sağlamak için kullanılan şifreleme işlemleridir [1,2].

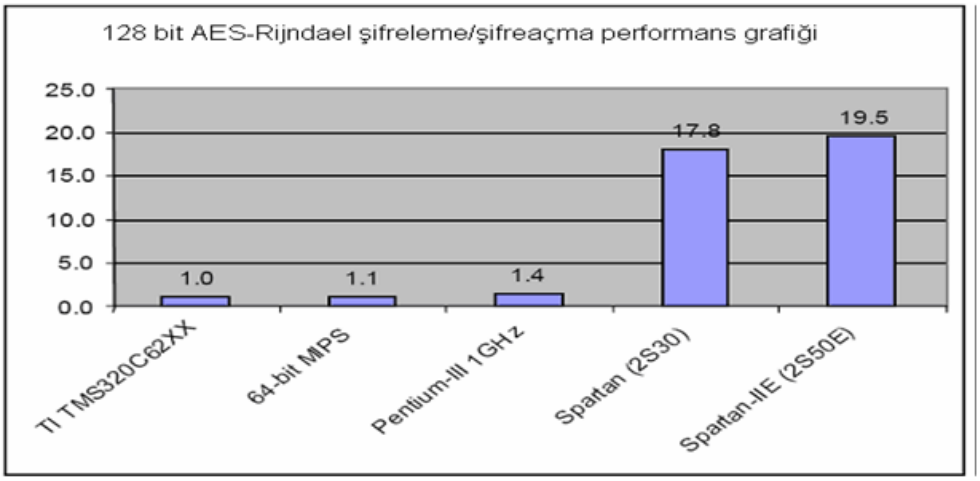
Şifreleme işlemi, şifreleme ve şifre açma olmak üzere iki aşamadan oluşur. Şifreleme, bir metnin asıl içeriğinin herhangi başka bir metne dönüştürülmesi işlemidir. Bu işlem şifreleme anahtarı ile gerçekleştirilir. Şifre açma işlemi ise şifreli metni asıl içeriğine dönüştürme işlemidir. Bu işlem bir şifre açma anahtarı ile gerçekleştirilir.

Bazı şifreleme uygulamaları özel bir donanıma gerek duymaktadır. Özellikle askeri ve aşırı önemli ticari uygulamalar donanım ile şifrelemeyi tercih etmektedir. Donanım ile şifreleme yaklaşımının seçilmesi için üç önemli neden vardır: hız, yüksek güvenlik ve kurulum/kullanım kolaylığıdır. Özel tasarlanmış donanımlar yazılımlardan

daha hızlı şifreleme yapabilmektedir. Bir bilgisayarda şifreleme yapan yazılıma farkında olunmadan kötü amaçlı kişiler/yazılımlar tarafından müdahale mümkündür. Fakat donanımlar bu probleme karşı daha iyi bir fiziksel koruma sağlamaktadır. Açılması zor olan kutular sayesinde saldırganları uzak tutmak mümkündür. Ayrıca entegre devrelerde algoritma anahtarını okuyacak saldırganlara karşı koruma tedbirleri geliştirilmiştir.

Bu konuda donanım ve yazılım ile gerçekleştirilen şifreleme algoritmalarının karşılaştırmalarına ait sonuç grafiği Şekil 1'de verilmiştir [3].

Şekil 1. AES algoritmasının değişik platformlarda performans grafiği.



Modern şifreleme algoritmalarının gücü söz konusu olduğunda algoritmanın kullandığı anahtarın uzunluğu, algoritmanın döngü sayısı, yapısı, kriptanaliz yöntemlerine karşı dayanıklılığı büyük önem taşımaktadır. Blok şifreleme algoritmaları günümüzde kriptografide önemli bir yer taşımaktadır. Bu algoritmalara örnek olarak DES (Data Encryption Standard) [4], AES (Advanced Encryption Standard) [5,6,] verilebilir. Çalışmamızda günümüzde yaygın kullanılan modern şifreleme algoritmaları araştırılmıştır.

2. ŞİFRELEME ALGORİTMALARI

Kriptografide şifreleme için kullanılan anahtarın özellikleri ve çeşidine göre temel olarak iki çeşit şifreleme algoritması bulunmaktadır. Bunlar;

1. Simetrik şifreleme algoritmaları,
2. Asimetrik şifreleme algoritmaları,
3. Karma Şifreleme Algoritmaları,

Bu algoritmada şifreleme ve şifre çözmek için bir tane gizli anahtar kullanılmaktadır. Kullanılan anahtar başkalarından gizlidir ve şifreleme yapan ile şifrelemeyi çözecek

kişilerde arasında anlaşılmış ortak bir anahtardır. Gönderilecek gizli metinle beraber üstünde anlaşılmış olan gizli anahtar da alıcıya gönderilir ve şifre çözme işlemi gerçekleştirilir. Simetrik şifrelemenin en önemli avantajlarından birisi oldukça hızlı olmasıdır. Asimetrik şifrelemeyle karşılaştırıldığında hız konusunda simetrik algoritmalar çok daha başarılıdır. Bununla birlikte simetrik algoritmayı içerdiği basit işlemlerden dolayı elektronik cihazlarda uygulamak çok daha kolaydır. Ayrıca simetrik algoritmalarda kullanılan anahtarın boyu ve dolayısıyla bit sayısı çok daha küçüktür.

Kuvvetli Yönleri;

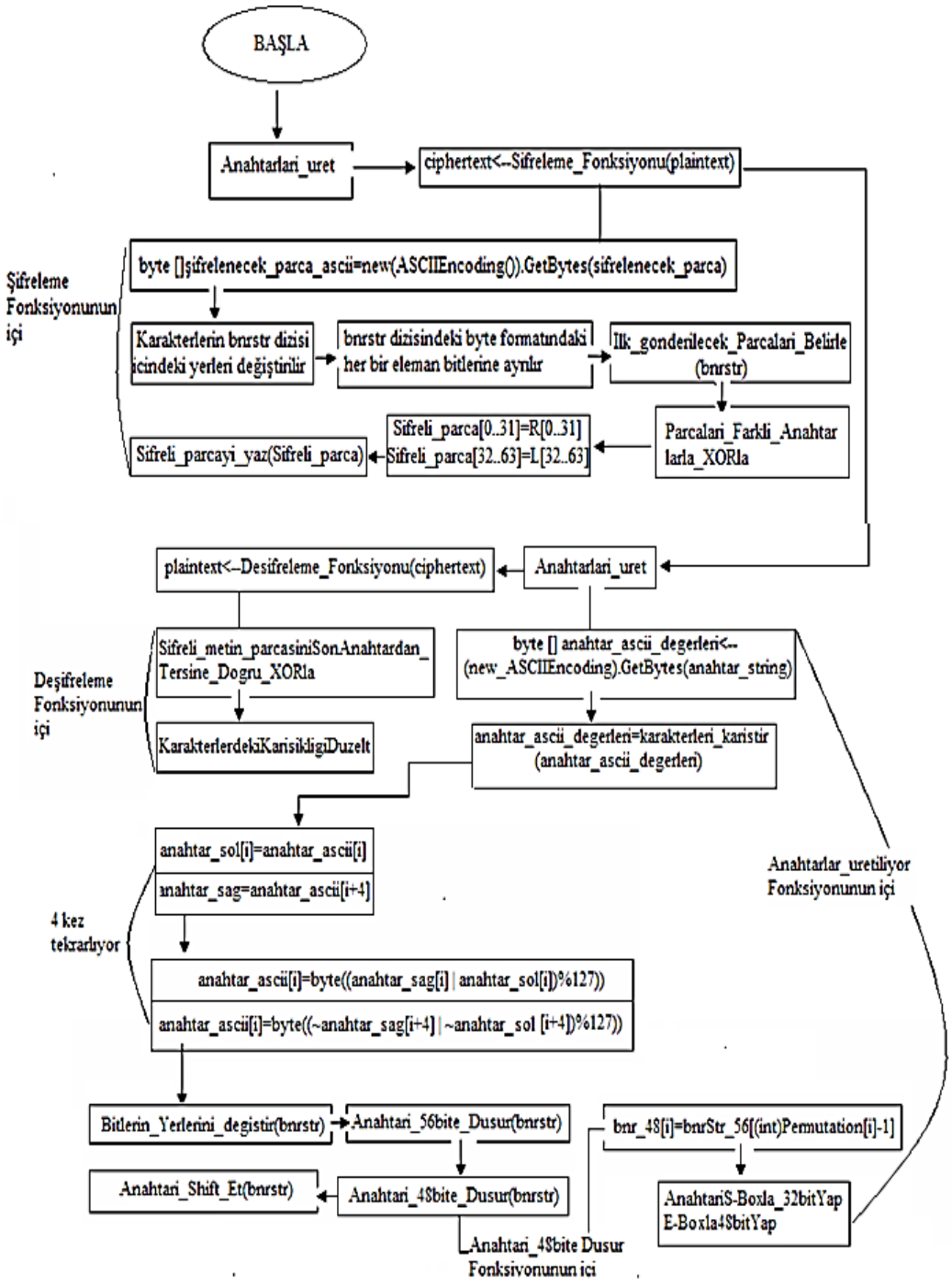
- Algoritmalar olabildiğince hızlıdır.
- Donanımla birlikte kullanılabilir.
- "Gizlilik" güvenlik hizmetini yerine getirir.
- Anahtarın boyu ve dolayısıyla bit sayısı çok daha küçüktür.

Zayıf Yönleri;

- Güvenli anahtar dağıtımı zordur.
- Kapasite sorunu vardır.
- Kimlik doğrulama ve bütünlük ilkeleri hizmetlerini güvenli bir şekilde gerçekleştirmek zordur.

2.1. Asimetrik Şifreleme Algoritmaları

1976 yılında Stanford Üniversitesinden Diffie ve Hellman adlı araştırmacılar iki farklı anahtara dayalı şifreleme sistemi önermiştir. Bu sistemde bir tane şifreleme için (public key) ve bundan farklı olarak bir tanede şifre çözmek için (private key) anahtar bulunur. private key, public key' den elde edilemez. Asimetrik şifreleme algoritmalarında çok büyük asal sayılar kullanılmaktadır.



Şekil 2. Algoritmanın Şematik Gösterimi [7]

Asimetrik Şifreleme Algoritmaların Sınıfları:
Açık Anahtar Dağıtım Şeması: Bilginin bir kısmının güvenli olarak değiştirilmesi için kullanılır. Değer iki tarafa bağlıdır. Bu değer gizli anahtar şeması için bir oturum anahtarı olarak kullanılır.
İmza Şeması: Sadece sayısal imza üretmek için kullanılır, burada gizli anahtar imzayı üretmekte, açık anahtar ise doğrulamakta kullanılır.
Açık Anahtar Şeması: Şifrelemek için kullanılır. Burada açık anahtar mesajları şifreler, gizli anahtar mesajların şifresini çözer.
Kuvvetli Yönleri;

- Kriptografinin ana ilkeleri olarak sayılan; bütünlük, kimlik doğrulama ve gizlilik hizmeti güvenli bir şekilde sağlanabilir.
- Anahtarı kullanıcı belirleyebilir.

Zayıf Yönleri;

- Şifrelerin uzunluğundan kaynaklanan algoritmaların yavaş çalışması,
- Anahtar uzunlukları bazen sorun çıkarabiliyor olması.

2.1.1. Asimetrik Şifreleme Algoritmalarının Avantajları:

- Asimetrik şifrelemenin kırılması simetrik şifrelemeye göre daha zordur.
- Bu yöntem private-keylerin karşılıklı aktarılmasını gerektirmez. Böylece simetrik şifrelemedeki anahtar dağıtım problemi çözülmüş olur.
- Public Keylerin bize şifreli mesaj göndermek isteyenler tarafından bilinmesi gerektiğinden bu anahtarlar internette bir sunucu ile rahatça dağıtılmaktadır.
- İki anahtarla şifrelemeden dolayı inkar edememeyi sağlayan sayısal imza gibi yeni yöntemler geliştirilmiştir.

2.1.2. Asimetrik Şifreleme Algoritmalarının Dezavantajları:

- Anahtarları kullanarak bilgileri çözme işlemlerinde CPU zamanının çok fazla olması.
- Bu zaman ileti uzunluğu ile üssel olarak artmaktadır.

Asimetrik şifreleme algoritmaları aşağıdaki gibidir;

1. Diffie Helman
2. RSA (Ronald L.Rivest, Adi Shamir ve Leonard Adleman)
3. DSA (Digital Signature Algorithm)
4. Eliptik Eğri Algoritması (ECC)

2.2. Simetrik Algoritmalar

a. Blok Şifreleme,
b. Dizi (akış) Şifreleme Algoritmaları, olarak ikiye ayrılmaktadır.

Simetrik şifreleme algoritmaları aşağıdaki gibidir;

1. AES (Advanced Encryption Standard- Gelişmiş Şifreleme Standartı)
2. DES (Data Encryption Standard- Veri Şifreleme Standartı**)**
3. Triple DES (3DES)
4. IDEA (International Data Encryption Algorithm)

5. Blowfish
6. Twofish
7. IRON
8. RC4
9. MD5 (Message-Digest Algorithm 5)
10. SHA (Secure Hash Algorithm – Güvenli Özetleme Algoritması)

2.3. Karma Şifreleme Algoritmaları

Günümüzde simetrik ve asimetrik şifreleme algoritmalarını birlikte kullanarak hem yüksek derecede güvenlik hem de yüksek hızlı sistemler şifrelenebilmektedir. Bu gibi sistemlere melez sistem adı verilir. Anahtar şifreleme, anahtar anlaşma ve sayısal imza işlemleri genellikle asimetrik şifrelemeyle, yığın veri işlemleri ve imzasız veri bütünlüğü korumaysa simetriklerle gerçekleştirilir.

3. BLOK ŞİFRELEME ALGORİTMALARI

Blok Şifreleme Algoritmaları veriyi bloklar halinde işlemektedir. Bazen bağımsız bazen birbirine bağlı olarak şifrelemektedir. Blok şifreleme şifrelenecek bir blok bilgiyi alır (genelde 64 bit) ve tek anahtarı ile seçilmiş fonksiyonu kullanarak onu aynı boyuttaki başka bir bloğa dönüştürür. Bu algoritmalarda iç hafıza yoktur, bu yüzden hafızasız şifreleme adını da almıştır. Bütünlük kontrolü gerektiren uygulamalarda genellikle blok şifreleme algoritmaları tercih edilir. Blok şifreler [8], Shannon'un önerdiği karıştırma (confusion) ve yayılma (diffusion) tekniklerine dayanır. Karıştırma şifreli metin ve açık metin arasındaki ilişkiyi gizlemeyi amaçlarken, yayılma açık metindeki izlerin şifreli metinde sezilmemesini sağlamak için kullanılır. Karıştırma ve yayılma, sırasıyla yerdeğiştirme ve lineer transformasyon işlemleri ile gerçeklenir. Feistel ağları ve Yerdeğiştirme-Permütasyon ağları olmak üzere iki ana blok şifreleme mimarisi vardır. Her ikisi de yerdeğiştirme ve lineer transformasyonu kullanır. Ayrıca her iki mimari ürün şifrelerinin örneklerindendir. Yani birden fazla şifreleme işleminin birleşmesi ile oluşturulurlar. Tekrarlanan şifreler yine ürün şifreleridir ve aynı şifreleme adımının tekrarlanan uygulamasını içerir ve her şifreleme adımına döngü denir. Bir döngü birden fazla şifreleme adımı içerebilir. Genellikle her döngüde farklı anahtar materyali kullanılır.[9]

Blok şifrelerin gücünü belirleyen bazı faktörler aşağıdaki gibidir:

- **Anahtar:** Blok şifrelerde anahtarın uzunluğu saldırılara karşı güçlü olacak şekilde seçilmelidir. Anahtarın uzun olması şifrenin kaba kuvvet (brute-force) saldırısına karşı kırılabilirliğini zorlaştırır.
- **Döngü sayısı:** Blok şifreleme algoritmalarında döngü sayısı iyi seçilmelidir. Böylelikle doğrusal dönüşüm ve yerdeğiştirme işlemleri ile şifreleme algoritması daha da güçlenmektedir. Ayrıca şifrenin karmaşıklığının arttırılmasında çok önemli bir etkendir. Böylelikle saldırılara karşı açık metin iyi derecede korunabilir.

- **S-kutuları (Yerdeğiştirme kutuları):** Blok şifreleme algoritmalarının en önemli elemanı S-kutularıdır. Algoritmanın tek doğrusal olmayan elemanıdır. Bu yüzden iyi bir S-kutusu seçimi şifrenin karmaşıklığını doğrudan etkiler. [10]

3.1. Blok Şifreleme Algoritmalarının Özellikleri

3.1.1 Anahtar

Blok şifreleme algoritmalarında anahtarın uzunluğu yada bit sayısı en temel saldırı olan geniş anahtar arama saldırısına karşın güçlü olmalıdır. Örneğin DES algoritması 56-bit anahtar kullanırken AES, algoritması DES'in bu zaafını örter niteliktedir ve 128, 192, 256 bit anahtar seçenekleri mevcuttur. Ayrıca anahtarın rastlantısal olması gerekmektedir.

3.1.2 Döngü Sayısı

Blok şifreleme algoritmalarında döngü sayısı iyi seçilmek zorundadır. Çünkü lineer transformasyon ve yerdeğiştirmelerin bu seçilen değerle algoritmaya yeterli gücü vermesi gerekmektedir. Ayrıca yapılan saldırıların başarısız olması için en önemli şartlardan biridir. Bu sayı için herhangi bir teorik hesaplama olmamasına rağmen Lars Knudsen'e göre kabaca döngü sayısı;

$$r >= dn/w \qquad (1)$$

(1) deki gibi olmalıdır. Burada r döngü sayısını, d yerdeğiştirme durumuna bir word'ü almak için gerekli maksimum döngü sayısını, n blok genişliğini, w ise tüm şifrede yerdeğiştirme durumuna giriş olan minimum word genişliğini temsil etmektedir. (1) de yayılma tekniği ihmal edilmiştir. *Şekil 2,* Lars Knudsen'e göre bazı algoritmaların döngü sayılarının neler olması gerektiğini göstermektedir. [6)

Şekil-3. Bazı Şifreleme Algoritmaları için Döngü Sayıları

Algoritma	**Döngü sayısı**	**(1)'e göre olması gereken döngü sayısı**
DES	16	21
IDEA	8	8
BLOWFISH	16	16
AES(Rijndael)	10	16

3.1.3 S Kutuları

S kutuları bir blok şifreleme algoritmasının en önemli ana elemanıdır. Çünkü algoritmadaki tek non-lineer yapıdır ve dolayısıyla algoritmaya gücünü vermektedir. S

kutuları için üç önemli nokta vardır. Bunların belirlenmesinde lineer kriptanaliz, diferansiyel kriptanaliz, Davies [11] saldırıları etkili olmuştur. Bunlar;

SAC (Strict Avalance Criteria); 1 bit giriş değişimi sonucunda her çıkış bitinin değişme olasılığı ½ olur.

S kutularının genişliği; Kriptanaliz saldırıları düşünüldüğünde büyük bir kutu küçüğüne oranla daha iyi olacaktır. Ayrıca diferansiyel saldırılardan korunmak için büyük sayıda çıkış bitleri ve lineer saldırılardan korunmak için büyük sayıda giriş bitleri gereklidir.

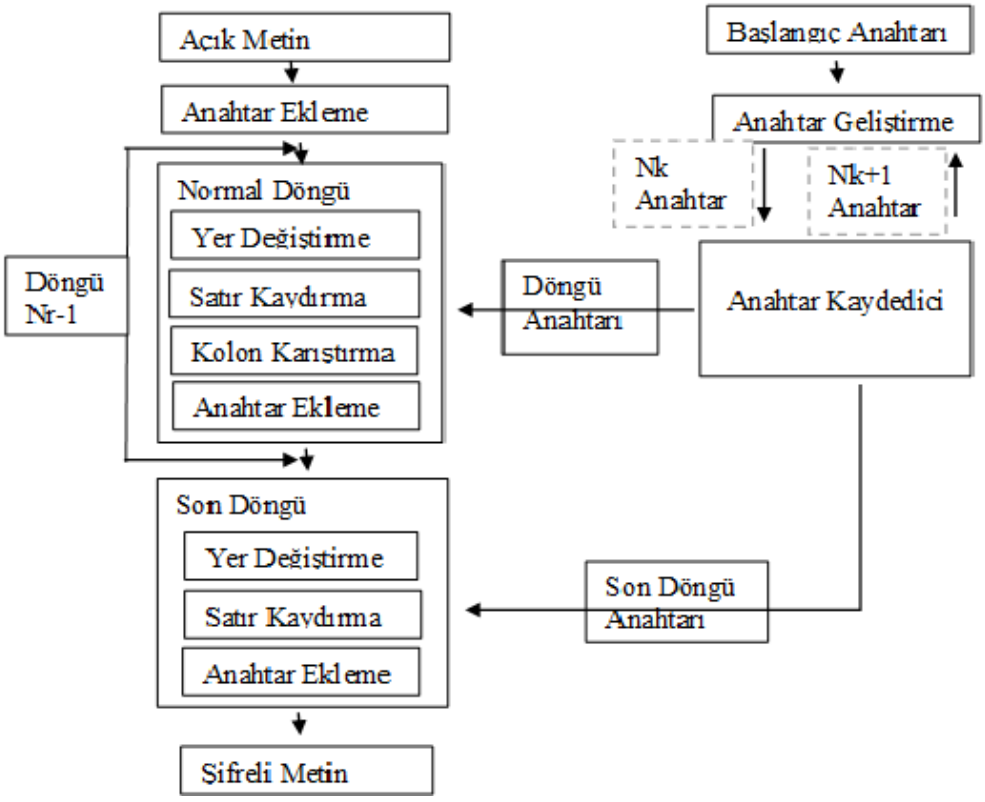
S kutusu gereksinimleri; Çıkışların dağılımları Davies saldırısına karşın kontrol edilmeli, çıkışlar girişe göre lineer olmamalı, S kutusunun her sırasındaki değerler tek olmalıdır. Daha güçlü S kutuları yaratmak için çeşitli çalışmalar da yapılmıştır [12,13,14,15].

4. AES (Advanced Encryption Standard- Gelişmiş Şifreleme Standartı)ALGORİTMASI

En yaygın olarak kullanılan simetrik şifreleme algoritmasıdır. AES, John Daemen ve Vincent Rijmen tarafından Rijndael adıyla geliştirilmiş ve 2002 yılında standart haline gelmiştir. AES uzunluğu 128 bitte sabit olan blok ile uzunluğu 128, 192 ya da 256 bit olan anahtar kullanır. Kullanılan tekniklerden bazıları baytların yer değiştirmesi, 4x4' lük matrisler üzerine yayılmış metin parçalarının satırlarına uygulanan kaydırma işlemleridir. SPN algoritmasının geniş bir çeşididir. Square [16] ve Crypton [17] şifreleri AES benzeri SPN şifrelerdir. Döngü sayısı anahtar genişliğine göre değişmektedir. 128 bit anahtar için 10 döngüde şifreleme yapılırken 192 ve 256 bit anahtarlar için sırasıyla 12 ve 14 döngüde şifreleme yapılmaktadır. AES algoritmasında her döngü dört katmandan oluşur.

4.1. AES Döngü Yapısı

Algoritmanın genel yapısı; AES algoritmasında giriş, çıkış ve matrisler 128 bitliktir. Matris 4 satır, 4 sütun (4×4), 16 bölmeden oluşur. Bu matrise 'durum' denmektedir. Durumun her bölmesine bir bytlık veri düşer. Her satırda 32 bitlik bir kelimeyi meydana getirir. Şifreleme işleminde ilk olarak 128 bit veri 4x4 byte matrisine dönüştürülür. Daha sonra her döngüde sırasıyla byte'ların yerdeğiştirmesi, satırların ötelenmesi, sütunların karıştırılması ve anahtar planlamadan gelen o döngü için belirlenen anahtar ile XOR'lama işlemleri yapılır. Byte'ların yerdeğiştirilmesinde 16 byte değerinin her biri 8 bit girişli 8 bit çıkışlı S kutusuna sokulur. S kutusu değerleri, Galois cisiminde (Galois Field-GF) GF(2^8), 8 bitlik polinom için ters alındıktan sonra doğrusal bir dönüşüme sokularak elde edilmiştir. Satırların ötelenmesi işleminde 4x4 byte matrisinde satırlar ötelenir ve sütunların karıştırılması işleminde herhangi bir sütun için o sütundaki değerler karıştırılır. Döngünün son katmanında ise o döngüye ait anahtar ile XOR'lama yapılmaktadır.



Şekil 4. AES şifreleme algoritmasının genel yapısı.

Metin uzunluğu: 128, 192, 256 bit olabilir.
Anahtar uzunluğu: 128, 192, 256 bit olabilir.
Döngü sayısı: Anahtar uzunluğu ve metin uzunluğuna göre değişiklik göstermektedir. Tablo1'de metin ve anahtar uzunluklarına göre döngü sayıları gösterilmiştir. Satırlar metin uzunluklarını, sütunlar anahtar uzunluklarını göstermektedir.

Tablo 1. AES anahtar uzunlukları ve döngü sayıları.

Metin Uzun.	Anahtar uzunluğu		
	128	192	256
128	10	12	14
192	12	12	14
256	14	14	14

Döngü sayıları

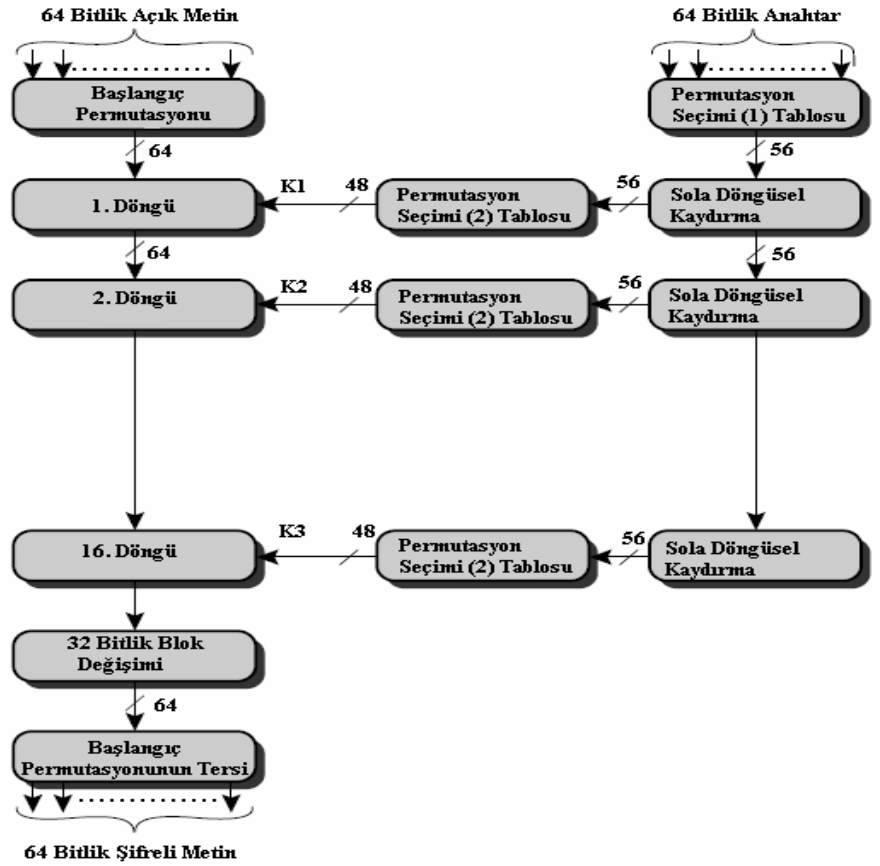
5. DES (Data Encrytion Standard - Veri Şifreleme Standartı) ALGORİTMASI

DES algoritması blok şifreleme (block cipher) mantığına göre çalışır, yani veriler bir anahtar yardımıyla bloklar halinde şifrelenir. Anahtar ne kadar uzunsa şifreyi çözmekte o kadar zor olacaktır. Des algoritmasında anahtar uzunluğu 56 bittir. Bu anahtar özellikle günümüz işlemci hızları göz önüne alındığında, brute force saldırılarına belli bir süre dayanabilir. DES yapısı itibari ile blok şifreleme algoritmasıdır. Yani basitçe şifrelenecek olan açık metni parçalara bölerek (blok) her parçayı birbirinden bağımsız olarak şifreler ve şifrelenmiş metni açmak içinde aynı işlemi bloklar üzerinde yapar. Bu blokların uzunluğu 64 bittir. Şifrelemeyi metin uzunlukları belli olan bloklar halinde gerçekleştirir. DES, IBM tarafından geliştirilmiştir. 1975 yılında "Federal Register" tarafından yayınlanmıştır. Ayrıca klasik Feistel Ağı kullanılarak temelde şifreleme işleminin deşifreleme işlemiyle aynı olması sağlanmıştır. DES algoritması 64 bitlik anahtar uzunluğuna sahip olmasına rağmen 56 bit uzunluğunda simetrik kriptolama tekniği kullanan bir sistemdir. Her kullanımında o kullanıma özel yeni bir anahtar yaratması DES'in güçlü yanı olup, günümüz teknolojisi için algoritmasının yavaş ve 56-bit'lik anahtar uzunluğunun yetersiz kalması DES'in zayıf yönleridir. 2000'li yılların başında kırılmasıyla günümüz teknolojisi için yetersiz kaldığı görülmüştür ve itibarını kaybetmiştir. DES"in algoritmasından kaynaklanan bu sorunlar "Triple DES" ya da "DES-3" olarak bilinen yeni bir algoritma ile düzeltilmiştir. SSH gibi günümüzde kullanılan çoğu uygulama 3DES"i kullanmaktadır. 3DES algoritması DES şifrelemesinin 3 kere art arda yapılması şeklinde çalışır. Bu yüzden DES'e göre 3 kat daha yavaştır. Bununla birlikte 3DES şifreleme yapmak için uzunluğu 24 bayt olan bir anahtar kullanılır. Her bayt için 1 eşlik biti vardır. Dolayısıyla anahtarın uzunluğu 168 bittir. AES'in geliştirilmesiyle etkinliğini kaybetmiştir çünkü daha gelişmiş bir algoritmaya sahip olan AES şifreleme yöntemine göre 6 kat daha yavaş çalışır.[18]

5.1. DES Algoritmasının Çalışma Prensibi

- DES şifreleme algoritmasının genel blok diyagramından da görülebileceği üzere algoritmanın genel çalışması aşağıdaki sıra düzenine göre özetlenebilir.[19]
- 64 bitlik data başlangıç permutasyonu olan IP (initial Permutation)'ye tabi tutulur.
- 64 bitlik data eşit uzunluktaki sağ ve sol parçalara ayrılır. Bunlar L ve R olarak adlandırılırlar. Ayrılan bölümlerin her biri 32 bit uzunluğundadır. İlk döngü durumu olduğu için bu yarılar L0 ve R0 olarak kullanılır.
- f fonksiyonu ile, ilgili döngü için oluşturulmuş alt anahtar ile işlem yapılır. Yapılan bu işlemler 16 döngü boyunca tekrarlanır.
- 16 döngü sonunda sol yarı ile sağ yarı değiştirilir.
- Son olarak 64 bitlik data üzerine başlangıç permutasyonun tersi uygulanır.

5.2. DES Şifreleme Algoritmasının Genel Blok Diyagramı



6. 3DES ŞİFRELEME TEKNİĞİ

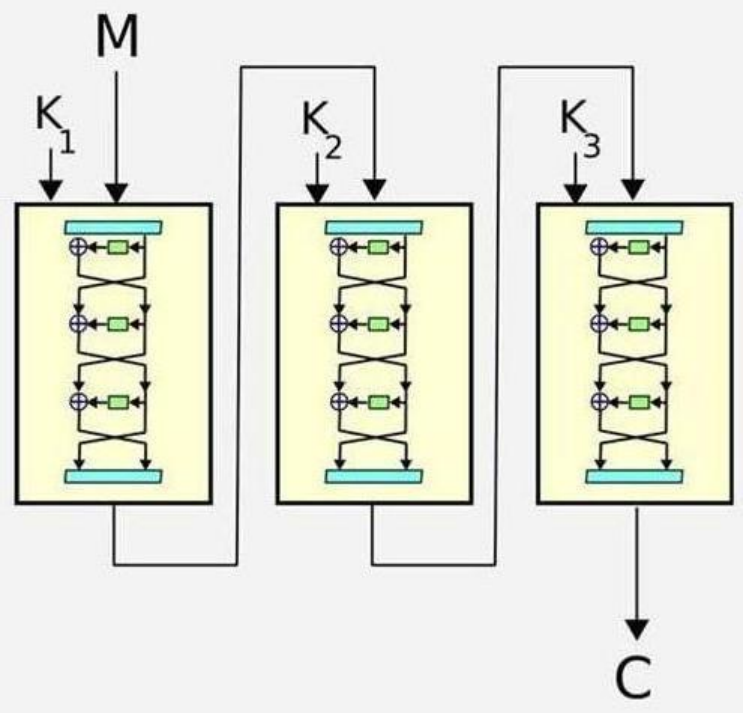
3DES algoritması, DES algoritmasının ardarda üç kez çalıştırılması ile elde edilmiştir. 3DES, DES`in daha çok güvenlik sağlayan bir çeşididir. Bu metot kriptolama anahtarındaki bitleri 3 katına çıkaran, DES`in 3 kez kullanımına dayalı bir şifreleme tekniğidir. 3DES kullanımı DES kullanımına göre 2 kat daha fazla güvenlik sağladığına inanılmaktadır. Bu 112 bitlik koda sahip olunması demektir. Ayrıca kodlama süresince de doğru orantılı olarak arttırmaktadır.

6.1. 3DES Şifreleme Tekniğinin Özellikleri

- Çift yönlü çalışır. Şifrelenmiş veri geri çözülebilir.
- DES şifrelemesinin 3 kere art arda yapılması şeklinde çalışır.
- DES şifreleme yöntemine göre 3 kat daha yavaş çalışır.

- Şifreleme yapmak için uzunluğu 24 bayt olan bir anahtar kullanılır. Her bayt için 1 eşlik biti vardır. Dolayısıyla anahtarın uzunluğu 168 bittir.
- Veri, 3DES anahtarının ilk 8 baytı ile şifrelenir. Sonra veri anahtarın ortadaki 8 baytı ile çözülür. Son olarak anahtarın son 8 baytı ile şifrelenerek 8 bayt bir blok elde edilir.
- Algoritmanın akış diyagramı aşağıdaki gibidir.

Şekil 5. 3DES Algoritmasının Akış Diyagramı



Avantajları:

- Çift yönlü çalıştığından şifreli bir şekilde veriler saklanabilir, istenildiği zaman geri çağrılarak şifresi çözülebilir.
- Bilgisayarın donanımsal açıklarını kapatır. (örnek: VPN, veri haberleşme ağları)

Dezavantajları:

- Güvenlik tamamen kullanılan anahtara dayanmaktadır. Anahtarın zayıflığı, şifrenin çözülmesini kolaylaştırır.
- Daha gelişmiş bir algoritmaya sahip olan AES şifreleme yöntemine göre 6 kat daha yavaş çalışır.

Kullanıldığı Yerler:

- Bankacılık sistemi
- Ciddi güvenlik programları
- Elektronik ödeme sistemi (kredi kartıyla internetten alışveriş yapma)

SONUÇ

Günümüzde blok şifreleme algoritmaları, şifrelemenin gerektiği birçok alanda kullanılmaktadırlar. Dolayısıyla bu algoritmaların gücüde güvenlik açısından çok önemlidir. Blok şifreleme algoritmalarının gücü, anahtar uzunluğuna, yapılan saldırılara karşı dayanıklılığına bağlıdır. Bunun yanında saldırıların başarılı sayılabilmesi için geniş anahtar arama saldırısı da bir kıstas olarak kullanılmaktadır. Yani anahtar arama saldırısından daha az maliyete mal olan saldırlar başarılı sayılmaktadır. Dolayısıyla algoritmanın tasarımında kullanılan anahtar yönetimi, yani bir ana anahtardan döngülere giriş olan anahtarlar elde etme yöntemi, S kutuları ve döngü sayısı algoritmanın yapılan saldırılara dayanıklılığını da etkilemektedir. Buna ek olarak algoritmaya yapılan saldırı da kullanılacak açık metin/şifreli metinlerin sayısı da, birçok gelişmiş saldırı yöntemleri bu verileri gerektirmekte, algoritmanın gücünü ortaya koymaktadır. Her ne kadar yukarıda bahsedilen teknikler geniş anahtar arama saldırısından daha etkili olsa da daha az açık metnin ve şifreli metnin kullanıldığı saldırı yöntemleri geliştirmek gereklidir. AES algoritmasında olduğu gibi yeni saldırı tipleri demek yeni algoritmalarda bu saldırı tiplerinin dikkate alındığı daha güçlü şifreleme algoritmaları demektir.

KAYNAKÇA

[1] Lincoln D. S., "Web Security: A Step-by-Step Reference Guide", Addison Wesley Professional , Boston,32-48, 60-82 (1997).

[2] Dworkin M. "Computer Security: Recommendation for Block Cipher Modes of Operation, Methods and Techniques" NIST Special Publication, Gaithersburg, 800-838 (2001).

[3] www.xilinx.com (Erişim Tarihi: 04.12.2014)

[4] FIPS 46-3, Data Encryption Standard, Federal Information Processing Standard (FIPS), Publication 46-3, National Bureau of Standards, U.S. Department of Commerce, Washington D.C., October 25, 1999.

[5] FIPS 197, Advanced Encryption Standard, Federal Information Processing Standard (FIPS), Publication 197, National Bureau of Standards, U.S. Department of Commerce, Washington D.C., November 26, 2001

[6] Bir Blok Şifreleme Algoritmasına Karşı Square Saldırısı, M. Tolga SAKALLI, Ercan BULUŞ, Andaç ŞAHİN, Fatma BÜYÜKSARAÇOĞLU, Trakya Üniversitesi, 22100 Edirne

[7] Tek Anahtarlı Yeni Bir Şifreleme Algoritması Daha, Gökhan DALKILIÇ, Gülşah YILDIZOĞLU, Dokuz Eylül Üniversitesi, Bilgisayar Mühendisliği, İzmir.

[8] Keliher L., Linear Cryptanalysis of Substitution-Permutation Networks, Ph.D. Thesis, 2002.

[9] Modern Blok Şifreleme Algoritmalarının Gücünün İncelenmesi, Andaç ŞAHİN, Ercan BULUŞ, M. Tolga SAKALLI, Trakya Üniversitesi, 22100 Edirne

[10] andacmesut.trakya.edu.tr/ag/Ders2.ppt (Erişim Tarihi: 27.11.2014)

[11] Biham E., Biryukov A., An Improvement of Davies' Attack on DES, JOURNAL OF CRYPTOLOGY, no. 3, 1997.
[12] Adams C., Tavares S., The Use of Bent Sequences to Achieve Higher-Order Strict Avalanche Criterion in S-Box Design, Technical Report TR 90-013 (Ontario, Canada) 1990.
[13] Biham E., Biryukov A., How to Strengthen DES using Existing Hardware, ASIACRYPT: International Conference on the Theory and Application of Cryptology, 1994
[14] Kwangjo K., Construction of DES-like S-boxes based on Boolean Functions Satisfying the SAC, ASIACRYPT'91, 1991.
[15] Adams C., Tavares S., Designing S-boxes, Conclusions.
[16] Daemen J., Knudsen L., Rijmen V., The block cipher SQUARE, Fast Software Encryption (FSE'97), LNCS 1267, pp.149-165, Springer-Verlag, 1997.
[17] Lim C. H., CRYPTON: A new 128-bit block cipher, The First Advanced Encryption Standard Candidate Conference, Proceedings, Ventura, California, 1998.
[18] http://bidb.itu.edu.tr/seyirdefteri/blog/2013/09/07/%C5%9Fifreleme-y%C3%B6ntemleri (Erişim Tarihi: 25.11.2014)
[19] PETRE, I., 2006, Cryptography and Network Security Lecture 3: Block ciphers and DES, [Online], Abo Akademi University, http://web.abo.fi/~ipetre/crypto/lecture3.pdf (Erişim Tarihi:15.11.2007)

Biyografi

Fatih ŞAHİN 1976 yılında Nevşehir'de dünyaya geldi. İlk ve ortaokulu burada okuduktan sonra 1990 yılında Kuleli Askeri Lisesine girdi. 2000 yılında Kara Harp Okulunu Jandarma Muhabere subayı olarak mezun olduktan sonra sırasıyla; İzmir, Tokat, Şırnak Ve İstanbul'da muhabere sistemleri (telli, telsiz, bilgisayar ve kripto hizmetleri) branşında görev yaptı. 2012 yılında Sakarya Üniversitesi, Bilişim Teknolojiler ve Bilgisayar Mühendisliğinde yüksek lisans derecesi yaptı. Halen İstanbul Aydın Üniversitesinde Bilgisayar Mühendisliği bölümünde doktora eğitimine devam etmektedir.
Evli ve iki çocuk sahibi olup, İngilizce bilmektedir.