Modern Blok Şifreleme Algoritmaları

doi: 10.17932/ IAU.IAUD.m.13091352.2015.7/26.15-21

***Fatih ŞAHİN*[1]**

Özet

Günümüzde duyulan en büyük ihtiyaçlardan birisi "bilginin doğru ve güvenli bir şekilde saklanıp, gerektiği yer ve zamanda ilgili kişiler tarafından" kullanılmasıdır. Bu kapsamda karşımıza "Kripto" yani "Şifreleme" çıkmaktadır. Şifreleme en eski tarihten beri kullanılan bir sistemdir. Tarihte şifrelemeyi ilk kullanan bilinen kaynaklarda Sezar'dır. Şifreleme; verinin, bilginin her şartta istenilen kişilere verinin güvenli bir şekilde iletilmesi için kullanılmaktadır. Şifreleme işlemi yaparken kullandığımız temel algoritmalar ise kriptosistemi oluşturur ki, bu algoritmalar kriptosistemin temel yapı taşlarıdır.

Bu kullanılan algoritmalar ise; anahtar, şifreleme algoritması, şifreli metin ve açık metinden oluşmaktadır. Gelişen teknoloji ile birlikte kullanılan modern şifreleme algoritmaları üç gruba ayrılmaktadır. Bunlardan birincisi, blok şifreleme algoritmalarının da içinde bulunduğu simetrik şifreleme algoritmalarıdır. Bu grup algoritmalar şifrelemede ve şifre çözmede (deşifreleme) aynı anahtar kullanılır. Bu kullanılan anahtara ise "gizli anahtar " denir. Şifreleme algoritmalarının ikincisi karma şifreleme algoritmaları ve üçüncüsü ise üçüncüsü ise asimetrik şifreleme algoritmalarıdır. Asimetrik şifreleme algoritması da simetrik algoritmalar gibi "gizli anahtar" kullanırken deşifreleme için ise açık anahtar kullanmaktadır. Bu saydığımız şifreleme algoritmaları özellikle de

[1] *e-mail: fsahin1976@yahoo.com*

modern blok şifreleme algoritmaları, günümüzde kullanılan kriptografide başrol görevi üstlenmektedir. Kullanılan blok şifreler güvenlik açısından düşünüldüğünde çok önemli bir ölçüttür. Sizlere sunulan bu çalışmada AES (Advenced Encryption Standard, Gelişmiş Şifreleme Standartı), DES (Data Encryption Standard, Veri Şifreleme Standartı) ve 3DES algoritmalarını inceleyerek bilgi sunulmuştur.

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

Abstract

One of the greatest needs nowadays is "keeping the information correct and secure and that it is used by the respective people when and where needed". In this respect we encounter the term "Crypto", i.e.the "Ciphering". Ciphering is a system which is used since the ancient history. According to sources, Caesar is known to be the one who used the cipering first. Cipering is used for transmitting the data and information to the required people in a secure manner under all circumstances. The basic algorithms which we use while performing the cipher process,constitute the cryptosystem. These algorithms are the basic units of the cryptosystem.

These used algorithms consist of key,cipher algorithm, ciphered text and public text. Modern cipher algorithms which are used with the developing tecnology, are divided into theree groups. First one is the symmetric sipher algorithms. The same key is used for ciphering and for decoding (deciphering) the algorithms in this group. This key is called as the "secret key". Second one is hybrid ciphering and the third one is asymmetric cipper algorithms. The asymmetric cipher algorithms use "secret key" as the symmetric algorithms, however it uses a "public key" for deciphering. These above mentioned ciphering algorithms and especially the modern block cipher algorithms, play the leading role in the cryptography currently used. Used block ciphers are very important criteria from the point of security. Within this work which is presented to you, AES (Advanced Encryption Standard), DES (Data Encryption Standard) and 3DES algorithms are examined and information are offered.

Keywords: *DES, 3DES, AES, Block Ciphering.*

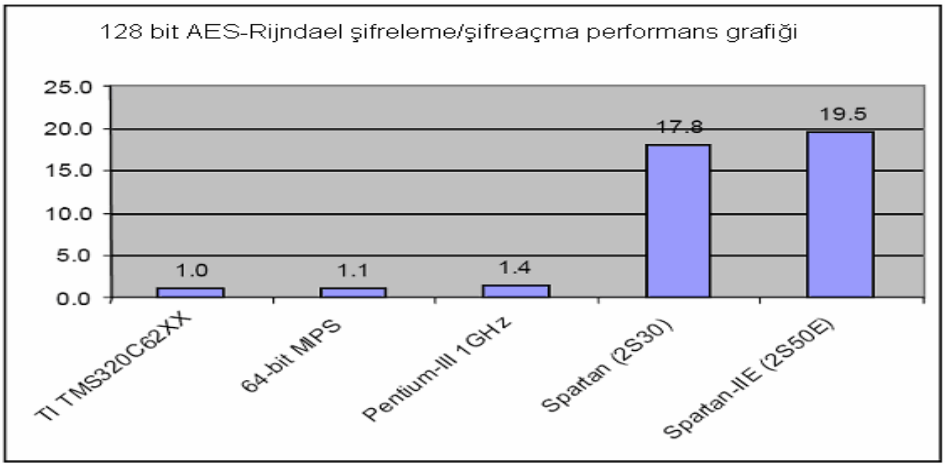
1. Giriş

Günümüzde kullanılan şifreleme ve deşifreleme teknikleri her türlü verinin iletişimi ve bu verilerin saklanıp depolanmasında, bu bilgilerin güvenliğini sağlanmasında kullanılmaktadır. Bütün bunların arasında en çok kullanılan ve yaygın olan uygulamaların başında internette kullanılan bilgiler gelmektedir. Bu verilerin güvenli bir şekilde aktarılması ise şifrelemenin görevidir ve kullanılan şifreleme işlemleridir [1,2].

Şifreleme denildiğinde aklımıza verilen verinin veya metnin şifrelenmesi ve şifresinin açılması gelmektedir. Şifreleme; iletmek istediğimiz metnin içeriğinin başka bir metne dönüştürülmesi işlemidir. Dönüştürme işlemi ise bizim oluşturduğumuz veya taraflarca bilinen bir anahtar ile gerçekleştirilir. Kullanılan tekniğe göre ya aynı anahtar kullanarak ya da farklı anahtar ile bu metni açabiliriz.

Şifreli metin ve verileri açarken bir kısım uygulamalar özel donanıma gerek duymaktadır. Ulusal güvenlik konularında ve ekonomisi büyük şirketlerde bu donanımları görmekteyiz. Donanım ve şifreleme tekniklerinin aynı anda kullanılmasının başlıca sebepleri ise; güvenlik ihtiyacı, hız ve kullanım kolaylığıdır. Kullanılan bu özel üretim donanımlar, kullanıcılara yazılımın yanısıra daha fazla ve hızlı olanak sağlayarak şifreleme yaptırmaktadır. Kullanılan yazılımlara kötü niyetli insanlar tarafından zararlı yazılımlar ile müdahale edilebileceği için, özel tasarlanmış bu donanımlar ve entegre devrelerle daha iyi fiziksel bir güvenlik sağlamaktadırlar.

Yazılım ile birlikte donanımın da kullanılması kapsamında yapılan inceleme kapsamında şifreleme algoritmalarının karşılaştırılması Şekil 1'de verilmiştir [3].



Şekil 1. *AES Algoritmasının Değişik Platformlarda Performans Grafiği.*

Şekil 1' de görüldüğü üzere modern şifreleme algoritmalarının gücü kullanılan anahtarların uzunluğuna, algoritmanın yapısı ve döngü sayısına, kriptanaliz ve sisteme yapılacak saldırıları yöntemlerine karşı direnci önem arzetmektedir.

Günümüzde kriptografide güvenlik kriterleri düşünüldüğünde blok şifreleme algoritmaları, hem güvenlik hem de hız hususları olarak değer kazanmaktadır. Blok şifreleme algoritmalarına DES (Data Encryption Standard) [4], AES (Advanced Encryption Standard) [5,6,] örnek olarak verilebilir. Çalışmamızda günümüzde yaygın kullanılan modern şifreleme algoritmaları araştırılmıştır.

2. Şifreleme Algoritmaları

Şifrelemede kullanılan anahtarların özelliklerine ve kullanılan algoritmanın çeşitlerine göre incelendiğinde üç ana gruba ayrılmaktadır. Bunlar;

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

2.1. Asimetrik Şifreleme Algoritmaları

İlk kez 1976 yılında Stanford Üniversitesinden araştırmacı olarak görev yapan Diffie ve Hellman 'a göre şifreleme sisteminde kullanılan iki farklı anahtar vardır. Bu araştırmacılar şifrelemede (private key) ayrı, deşifreleme için ise ayrı (public key) anahtar kullanmışlardır. Bu anahtarlar birbirinden bağımsız olarak üretilirler.

Asimetrik şifreleme algoritmalarının bölümleri:
Açık Anahtar Dağıtım Şeması: İletilecek bilginin güvenli bir şekilde değiştirilmesinde kullanılır.

İmza Şeması: Sayısal imza elde etmek için kullanılır. Burada kullanılan "gizli anahtar" imzayı üretmek için kullanılırken, "açık anahtar" ise imzayı doğrulamak için kullanılır.

Açık Anahtar Şeması: Bilgiyi şifrelemede kullanılır. Kullanılan "açık anahtar" gönderilen mesajları şifrelerken, "gizli anahtar" da gönderilen mesajları deşifrelemede kullanılır.

2.1.1. Asimetrik Şifreleme Algoritmalarının Avantajları:

- Şifrelerin kırılması nispeten daha zordur,
- Kimlik doğrulama, bütünlük ve gizlilik ilkelerini gerçekleştirmek için güveli bir yoldur,
- Kullanılacak olan anahtarı kullanıcı kendisi belirleyebilir,
- Şifreleme için kullanılan private-keylerin karşılıklı aktarılması gerekli değildir,
- Deşifreleme için kullanılan public keylerin internetteki bir sunucu tarafından dağıtılabilir,
- Şifrelemede iki anahtar kullanıldığı için sayısal imza ile inkar edememeyi sağlar.

2.1.2. Asimetrik Şifreleme Algoritmalarının Dezavantajları:

- Şifreler uzundur, bundan dolayı algoritmalar yavaş çalışır,
- Anahtarlar uzun olduğundan bit sayıları da uzundur.

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

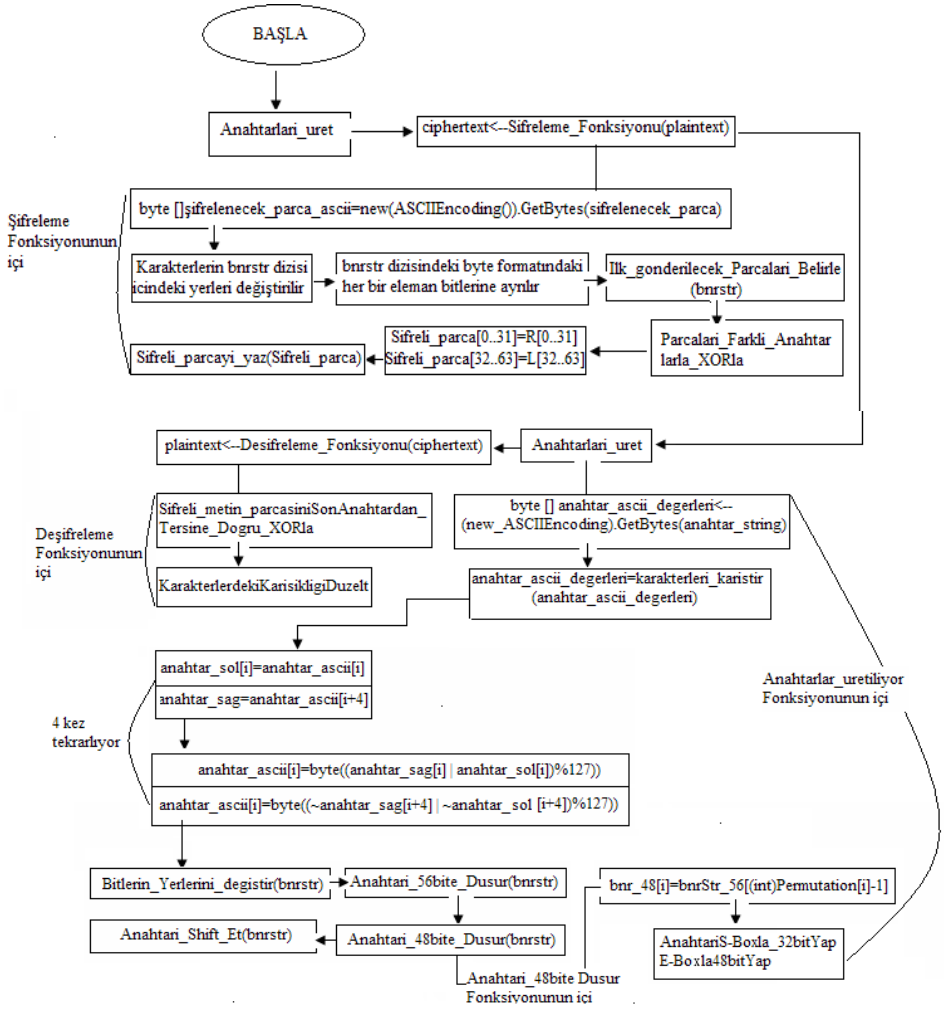
Simetrik şifreleme algoritmalarında, şifreleme ve deşifreleme için sadece bir tane gizli anahtar kullanılmaktadır. Kullanılan anahtar gizlidir ve şifreleme yapan ile şifrelemeyi çözecek (deşifreleme yapacak olan) kişiler arasında kullanılan ortak bir anahtardır. Gönderilecek gizli metinle birlikte gizli anahtar da metinin üstünde eklenerek önceden koordine edilmiş olan alıcıya birlikte, aynı anda gönderilir. Şifre çözme işlemi de bu anahtar kullanılarak gerçekleştirilir. İşlem süresinin hızlı olması simetrik şifreleme algoritmalarının en önemli avantajlarındandır. Diğer şifreleme algoritmaları ile kıyaslandığında simetrik algoritmalar hız konusunda diğer şifreleme algoritmalarına karşı oldukça başarılıdır. Ayrıca simetrik algoritmalarda kullanılan basit işlemlerden dolayı donanımlarda ve elektronik cihazlarda kullanılabilirliği ve uygulanabilirliği çok daha basittir. Bunun yanında simetrik algoritmalarda kullanılan anahtarın uzunluğu ve anahtarın bit sayısı yine diğer algoritmalara göre çok daha küçüktür ve daha az yer kaplarlar. Simetrik şifreleme algoritmaları; dizi (akış) ve blok şifreleme algoritmaları olmak üzere ikiye çeşittir.

Kuvvetli Tarafları;

- Diğer algoritmalara nazaran daha hızlıdır,
- Özel donanımla birlikte kullanılabilir,
- "Gizlilik" konusunda ve güvenlik konusunda daha başarılıdır,
- Bit sayısı düşük olduğundan dolayı anahtarın boyu nispeten daha küçüktür.

Zayıf Tarafları;

- Anahtarların güvenli bir şekilde dağıtımı zordur,
- Kapasitesi sınırlıdır,
- Bütünlük ve kimlik doğrulama hizmetlerini güvenli bir şekilde gerçekleştirmek zordur.



Şekil 2. *Algoritmanın Şematik Gösterimi [7]*

Simetrik Şifreleme Algoritmaları Çeşitler;

1. IRON
2. IDEA (International Data Encryption Algorithm)
3. DES (Data Encryption Standard- Veri Şifreleme Standartı**)**
4. 3DES (Triple DES)
5. AES (Advanced Encryption Standard- Gelişmiş Şifreleme Standartı)
6. Blowfish
7. Twofish
8. RC4

9. MD5 (Message-Digest Algorithm 5)
10. SHA (Secure Hash Algorithm – Güvenli Özetleme Algoritması)

2.3. Karma Şifreleme Algoritmaları

Günümüzde bilginin güvenli bir şekilde kullanılması, iletilmesi ve saklanmasının yanı sıra mesajın seri ve hızlı bir şekilde gönderilmesi de önem kazanmıştır. Bundan dolayıda simetrik ve asimetrik algoritma sistemleri birlikte kullanılmaya başlanmıştır. Bu gibi (melez sistemlerde) karma sistemlerde avantaj ve dezavantajları göz önüne aldığımızda; anahtar şifreleme, sayısal imza gibi işlemler asimetrik sistemlerle yapılırken; küme (yığın) veri işlemleri ve veri bütünlüğü koruma işlemleri de simetrik algoritma sistemleri kullanılarak yapılmaktadır.

3. Blok Şifreleme Algoritmaları

Adından da anlaşılacağı üzere Blok Şifreleme Algoritmaları, veriyi/bilgiyi bloklar halinde işlemektedir. Bloklar halinde işlerken de bazen birbirinden bağımsız, bazense birbirine bağımlı olarak şifrelemektedir. Bu sistemde, blok şifreleme bilgiyi şifrelenecek bloklara ayırır (genellikle 64 bit) ve kullandığı tek anahtar ile seçilen fonksiyonu kullanarak bilgi bloğunu boyutunu değiştirmeden başka bir bloğa dönüştürür. Bu algoritmaların hafızası olmadığı için "hafızasız şifreleme" de denilmektedir. Dolayısıyla bütünlük ihtiyacı gerektiren uygulamalarda genellikle blok şifreleme algoritmaları tercih edilmektedir.

Blok şifreler [8], Shannon'un önerdiği karıştırma (confusion) ve yayılma (diffusion) tekniklerine dayanmaktadır. Bu tekniklerden karıştırma; gönderilecek olan açık metin ile alınan şifreli metin arasındaki bağlantıyı gizlemek için kullanılır. Yayılma tekniği ise; gönderilecek açık metindeki geride bıraktığı izleri iletim ortamındaki şifreli metinde anlaşılmamasını sağlar. Yerdeğiştirme ve lineer transformasyon işlemleri karıştırma tekniği ve yayılma tekniklerini gerçekleştirmek için kullanılır. Bu kapsamda karşımıza iki temel blok şifreleme yapısı karşımıza çıkmaktadır. Bunlar: Yerdeğiştirme-Permütasyon ve Feistel ağlarıdır. Bunlarda yine lineer transformasyon ve yerdeğiştirme tekniklerini kullanırlar. Bunlar, ürün şifreleme için kullanılan mimarilerdir. Başka bir deyişle; şifreleme işlemi yaparken birden çok işlemin birleşmesidir. Şifreler tekrar kullanırken ürün şifrelerini kullanırlar ve bu şifreleme adımlarına da döngü denmektedir.

Anlaşılacağı üzere her bir döngü birçok şifreleme adımından oluşur. Bu döngüler tekrarlanırken herbiri ayrı anahtar kullanırlar. [9]

3.1. Blok Şifreleme Algoritmalarının Özellikleri

3.1.1 Anahtar

Blok şifrelemede kullanılacak anahtarın uzunluğu veya bit sayısının seçimindeki dikkat edilecek husus; güçlü bir şifre seçilmesidir. Yani, saldırganların temel saldırısı olan geniş anahtar arama saldırısına karşı güçlü seçilmeli ve kaba kuvvet (brute-force) saldırısına karşı kırılabilirliği de zor olmalıdır. [10] Örnek olarak DES şifreleme algoritmaları 56-bit anahtar kullanırken, AES algoritması ise 128 bit, 192 bit ve 256 bitlik anahtar seçenekleri ile DES algoritmalarına göre daha avantajlıdır. Kullanılan anahtar random bir şekilde olması ise diğer bir özelliğidir.

3.1.2 Döngü Sayısı

Döngü sayısı blok şifreleme algoritmalarının seçimindeki en önemli hususdur. Şifrenin karmaşıklığının arttırılmasında lineer transformasyon ve yerdeğiştirme işlemleri öneli bir hususdur. Döngü sayısının hesaplanmasında herhangi bir standart olmamasına rağmen Lars Knudsen'e bir formül ile döngü sayısını hesaplamıştır;

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

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 giren minimum word genişliğini göstermektedir. (1) de yayılma tekniği ihmal edilmiştir., Lars Knudsen'e göre algoritmaların döngü sayılarının neler olması gerektiği Tablo-3gösterilmektedir. [6]

Tablo-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 (Substitution Box)

Blok şifreleme algoritmasının en önemli elemanlarından birisi S-kutularıdır. Çünkü algoritmadaki tek doğrusal olmayan elemandır. Bu özelliğinden dolayı S-kutuları kullanılacak şifrenin karmaşıklığını dolayısıyla da algoritmanın gücünü oluşturur. S-kutularının (S-Kutuları lineerliği engellerler) belirlenmesinde lineer kriptanaliz, diferansiyel kriptanaliz ve Davies saldırılarıdırı önemli yer tutmaktadır. [11] Bunlar;

SAC (Strict Avalance Criteria); Herbir giriş bit'inin değişmesi sonucunda çıkış bitinin değişme olasılığı ½ olur.

S-kutularının genişliği; S-kutunun büyüklüğü saldırılardan korunmamıza doğru orantılı olarak yansımaktadır. Sitemi hangi tür kriptanaliz saldırılarından korunacağımızı belirlemek önemlidir. Eğer diferansiyel saldırılardan korunmak istiyorsak, algoritmada büyük sayıda çıkış bit'leri kullanmalıyız. Eğer lineer saldırılardan korunmak istiyorsak da bu sefer giriş bit'lerini büyük sayıda kullanmalıyız.

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

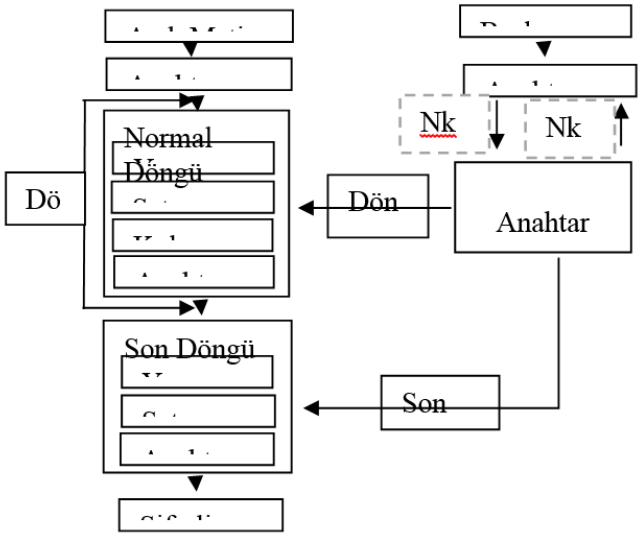
Blok şifreleme algoritmalarında en yaygın olarak kullanılan algoritma simetrik şifreleme algoritmasıdır. 2002 yılında şifreleme algoritmaları arasında kendisine yer bulmuştur. AES'in Rijndael adıyla anılması ise bu algoritmanın geliştiricileri olan Vincent Rijmen ve John Daemen'nın adlandırmasıdır. AES 128 bit uzunluğundaki blok ile, uzunluğu 128 bit, 192 bit ya da 256 bit anahtar alternatiflerini kullanır. Bayt'ların yer değiştirmesi ve kullanılan tekniklerden bazıları, 4x4' lük matrisler üzerindeki metinin satırlarına yapılan kaydırma işlemidir. SPN algoritmasının geniş bir çeşididir. Bu kullanılan şifreleme algoritmalarının yanında Square [16] ve Crypton [17] şifreleri AES tarzı şifrelerdir. Kullanılan anahtar uzunluğuna göre döngü sayısı değişmektedir. Şifrelemede, 10 döngü için 128 bit anahtar kullanırken, 192 bit anahtar için 12 döngü ve 256 bit anahtarlar için de 14 döngü ile şifreleme işlemini gerçekleştirmektedir.

4.1. AES Döngü Yapısı

AES algoritmasında her döngü dört katmandan oluşur. AES algoritmasının genel yapısında giriş, çıkış ve matrisler 128 bitliktir. Bu matrisler 4 satır ve 4 sütun (4×4) olmak üzere 16 bölmeden meydana gelir. Oluşan bu matrise 'durum' denilmektedir. Durumun herbir bölmesinde birer byte veri vardır. Şifrelemede ilk önce 128 bitlik veri 4x4 byte'lık matrise dönüştürülür. Sonrasında sırasıyla her döngüde;

- Byte'ların yerdeğiştirmesi,
- Satırların ötelenmesi,
- Sütunların karıştırılması ve
- Planlanan anahtar için o döngünün anahtarı XOR'lama işlemleri yapılır.

Byte'lar yerdeğiştirirken oluşturulan 16 byte 8 bit'i giriş ve 8 bit!i de çıkış olmak üzere S kutusuna gönderilir. S-kutusundaki değerler, Galois cisminde (Galois Field-GF) GF (28), 8 bitlik polinom için ters alındıktan sonra lineer bir dönüşümle oluşturulmuştur. Satırların ötelenmesi işleminde ise 16 bölümden oluşan matrisdeki satırlar ötelenir ve sütunların karıştırılması işleminde sütunlar kendi içinde karıştırılır. Son aşamada ise oluşturulan döngü anahtarı XOR'lama yapılarak işlem sonlandırılır. (XOR veriler anahtar bilgiler ekler)



Şekil 4. *AES şifreleme algoritmasının genel yapısı.*

Tablo-2'de şifrelenecek metin ve kullanılan anahtar uzunluklarına göre algoritmanın gireceği döngü sayıları verilmiştir.

Tablo-2. *AES'de metin ve anahtar uzunlukları ile 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 (kaba kuvvet) saldırılarına belli bir süre dayanabilir. Kısaca DES; şifrelenerek gönderilecek olan açık metni bloklara ayırarak oluşan bütün parçaları ayrı ayır şifreler. Sonuçta şifrelenmiş kapalı metni tekrar açabilmek için ise işlemi tekrar ederek yine ayrılmış olan bloklar üzerinde bağımsız ve ayrı ayrı yaparak çözer. Oluşturulan blokların 64 bit uzunluğuna sahiptir. DES şifreleme işlemini metin boyutu sabit olan bloklar olarak oluşturur. IBM tarafından geliştirililen DES, "Federal Register" tarafından 1975 yılında yayınlanarak dünyaya duyurulmuştur. Bu yayında bilinen Feistel Ağı kullanılmış ve şifreleme işlemi deşifreleme işlemi aynı şekilde kullanılmıştır. Fakat DES algoritmasındaki anahtar uzunluğunun 64 bit olmasına rağmen, 56 bit'lik simetrik kriptolama tekniğini kullanır. Her defasında o kullanıma mahsus farklı bir anahtar oluşturması DES algoritmasının avantajlı tarafı olup, modern teknolojide yavaş ve kullandığı 56 bit'lik anahtarının güvenlik ihtiyacını karşılayamaması da DES'in

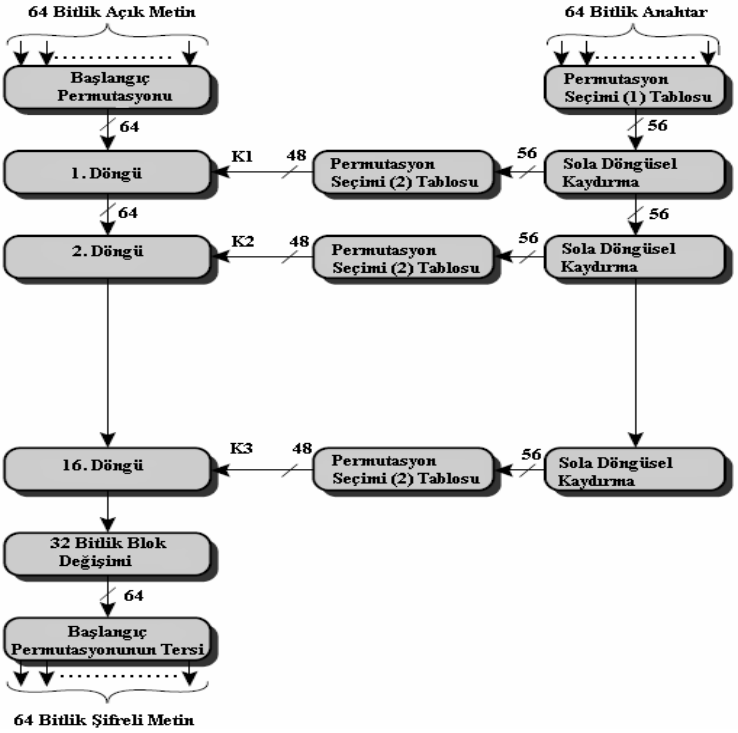
dezavantajlı tarafıdır. Bu zayıf yönü dolayısıyla da günümüzde itibarını kaybetmiştir ve yerini Triple DES" veya "3DES" olarak da adlandırılan yeni ve daha güvenlikli bir algoritmaya bırakmıştır. 3DES algoritması; DES algoritmasının arka arkaya 3 kere tekrar edilmesi suretiyle çalışmaktadır. Bu sebepten dolayı DES algoritmasına göre 3 kat daha yavaş çalışmaktadır. 3DES algoritması DES algoritmasının aksine şifreleme için 24 bayt'lık anahtar kullanır. Bu algoritmada kullanılan herbir bayt'ın bir (1) eşlik biti vardır ve bu da anahtarın uzunluğunu 168 bit yapmaktadır. 3DES algoritması da zamanla DES algoritması gibi günümüz teknolojisine ayak uyduramadığından ve yavaş kaldığından yerini, kendisine göre 6 kat daha hızlı çalışan AES şifreleme tekniğine bırakmıştır. [18]

5.1. DES Algoritmasının Çalışma Prensibi

DES şifreleme algoritmasının çalışması prensibi şu şekildedir.[19]

a. İlk olarak data başlangıç permutasyonu olan IP (İnitial Permutation) de çalıştırılır,
b. 64 bit'lik veri 32 bit'lik iki eşit parçaya ayrılır. Bunlar L (Left) ve R (Right) olarak adlandırılırlar. Başlangıç döngüsü olduğundan bu eşit parçalar L0 ve R0 diye adlandırılırlar.
c. Bu döngü için oluşturulmuş alt anahtar f fonksiyonu kullanarak döngüye sokulur, ve bu döngü 16 kere tekrarlanır.
d. 16 döngü sonrasında ayrılmış olan L ve R parçaları yerdeğiştir.
e. Son olarak da döngüye sokulmuş olan 64 bitlik dataya IP'nin ters işlemi uygulanarak algoritma tamamlanır.

5.2. DES Şifreleme Algoritmasının Genel Blok Diyagramı



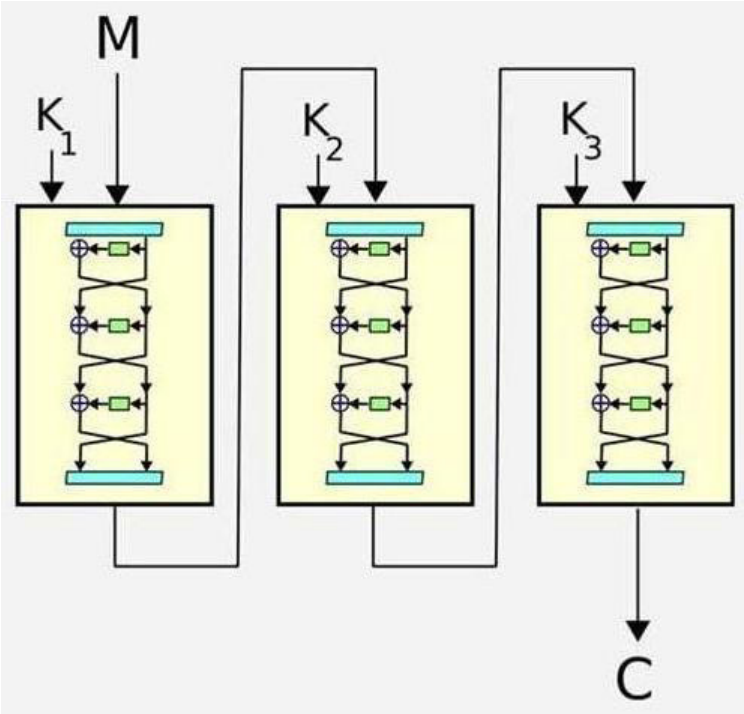
6. 3Des Şifreleme Tekniği

3DES algoritması, DES algoritmasının ardarda üç kez çalıştırılması ile elde edilmiştir. Dolayısıyla DES algoritmasına göre daha güvenlidir. 3DES iki ayrı anahtar kullanarak üçlü şifreleme yapmaktadır. Üç değilde iki anahtar kullanmasının nedeni ise Brute Force (Kaba Kuvvet) saldırılarına karşı yeterli olmasındandır. 3DES algoritması DES algoritmasına göre 2 kat daha fazla güvenlik sağlamaktadır ki bu da; 112 bitlik bir anahtara karşılık gelmektedir. Ve bu güvenlik bütün şifreleme işlemi boyunca da orantılı olarak artmaktadır.

6.1. 3DES Şifreleme Tekniğinin Özellikleri

- Şifrelenmiş bilgi tekrar çözülebildiğinden iki yönlü çalışabilmektedir.
- DES şifreleme algoritmasının 3 kez arka arkaya çalıştırılmasıyla oluşur.
- DES şifrelemesine nazaran 3 kat ağır işler.

- DES algoritmasının aksine şifreleme için 24 bayt'lık anahtar kullanır. Bu algoritmada kullanılan herbir bayt'ın bir (1) eşlik biti vardır ve bu da anahtarın uzunluğunu 168 bit yapmaktadır.
- Data, anahtarın ilk 8 baytı kullanılarak şifrelemeye tabii tutulur. Sonrasında, anahtarın ortasındaki 8 bayt'ı kullanılarak deşifrelenir. Son olarak da, anahtarın son 8 bayt'ı kullanılarak şifreleme yapılır ve tekrar 8 bayt'lık data oluşturulur.



Şekil 5. *3DES Algoritmasının Akış Diyagramı*

Kuvvetli Tarafları:

- İki yönlü çalışmasından dolayı veriler rahat bir şekilde saklanabilir ve dilediğinde tekrar çağırılarak data tekrar çözülebilir.
- Kullanılan cihazların (bilgisayarın) eksikliklerini giderir.

Zayıf Tarafları:

- Kullanılan anahtar sistemin güvenliğini oluşturur. Kullanılan anahtar ne kadar zayıfsa, şifrenin kırılması o kadar kolaydır.
- Günümüz teknolojisinde kullanılan daha gelişmiş AES algoritmasına

nazaran 6 kat ağır işler.

Kullanım Alanları:

- Finans sektörü (bankacılık)
- Önemli güvenlik faaliyetlerinde
- İnternet üzerinden alışverişlerde (e-ödeme)

Sonuç

Güvenlik ihtiyaçları insanoğlunun gereksinim duyduğu en başlıca ihtiyaçlarından birisidir. Bilginin iletilecek kişiye en güvenilir ve en hızlı bir şekilde iletilmesi günümüz yazılımlarının ve donanımlarının hedefi haline gelmiştir. Bu ihtiyaçları ise gidermek için şifreleme algoritmalarına gereksinim duyulmaktadır. Bu doğrultuda ise şifreleme tekniklerinin hangisini kullanacağımızı seçmek bize düşen bir tercih meselesidir. Şifrelemede kullanılan anahtarın gücü ne kadarsa sistemin gücü de o kadardır. Şifrelemede kullanılan anahtarların özelliklerine ve çeşitlerine göre iki temel şifreleme algoritması vardır: "Simetrik Şifreleme Algoritmaları" ve "Asimetrik Şifreleme Algoritmaları". Ayrıca herhangi bir girdi değeri olarak anahtar kullanmayan algoritmalara da "Anahtarsız Algoritmalar" denilmektedir. Anahtarsız algoritmalar herhangi bir sistemde tek başlarına kullanılmamaktadır. Sistemde kullanılan Simetrik veya Asimetrik Algoritmalara yardımcı olmak için kullanılmaktadırlar. Eğer sizin için önemli olan hız, donanımla uyumluluk ve güvenlik ise, kapasite sorununuz yoksa ve anahtar dağıtımında sorununuz yoksa, sizin için tek sistem Simetrik Şifreleme Algoritmalarıdır. Blok şifreleme algoritmaları da Simetrik Şifreleme algoritmalarının en yaygın kullanımlarından birisi ve günümüzün en gelişmiş şifreleme tekniği olarak görülmektedir. Algoritmanın gücü, kullanılan anahtarın uzunluğuna ve tabiki de sisteme uygulanan saldırılara karşı koyabilmesine bağlıdır. Bir saldırının başarısı geniş anahtar saldırısına bağlıdır. Diğer bir deyişle, saldırı ne kadar az maliyetli olursa ve sonuçta başarılı olursa o kadar amacına ulaşmış sayılır. Blok şifreleme algoritmaları sadece boyutu sabit olan metinler için kullanılmaktadır. Blok uzunluğundan büyük metinler için blok şifreleme algoritmaları kullanılmaktadır. Blok şifreleme algoritmalarını seçerken vazgeçemeyeceğimiz tek husus güvenlik ise bunu AES şifreleme algoritması ziyadesiyle yerine getirmektedir. Günümüz teknolojisi ile uyumlu olması gerek kapasite gerekse de hafıza olarak en optimum çözüm AES şifreleme algoritmalarıdır. Şimdiye kadar AES şifreleme

algoritmalarında herhangi bir güvenlik açığı ile karşılaşılmadı, fakat önümüzdeki günlerde de karşılaşılmayacağı anlamına gelmemektedir

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)