Mukayeseli Veri Şifreleme Algoritmaları

Comparision of Data Encryption Algorithms

Sıddık Said AYDOĞAN
Bilgisayar Mühendisliği Bölümü
Yıldız Teknik Üniversitesi
İstanbul, Türkiye
s.said@saidaydogan.com

***Özet*—Veri şifreleme algoritmalarının başarıları ne kadar çözülemez ve verimli olduğu ile alakalıdır. Bu makalede en çok kullanılan veri şifreleme algoritmaları olan DES,üçlüDES ve Blowfish incelenmiş ve performansları karşılaştırılmıştır.**

Anahtar Kelimeler—Kriptoloji; Şifreleme; DES; üçlüDES; Blowfish

***Abstract*— Data encryption algorithms that success is related to the difficulty of dissolution and efficiently. This article is the most widely used data encryption algorithms DES, Blowfish tribleDES and their performances are compared and analyzed.**

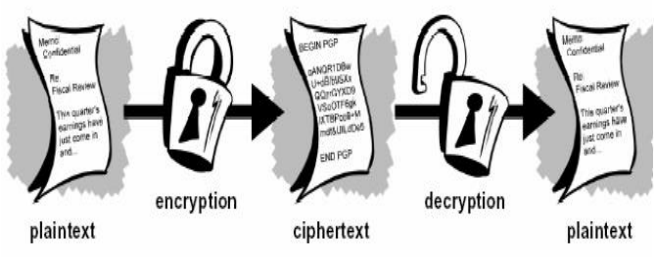
Keywords—Cryptology; Encryption; DES; TripleDES; blowfish

I. GİRİŞ

Kriptoloji, Yunanca crypto's (saklı) ve lo'gos (kelime) kelimelerinin birleştirilmesinden oluşturulmuştur ve iletişimde gizlilik bilimi olarak değerlendirilmektedir. Ticari ilişkilerde,devlet işlerinde, askeri işlerde ve personel ilişkilerinde güvenli iş çalışması yapmak büyük bir sorundur. Sistemler arası bağlantılarda ya da herhangi iki nokta arasındaki haberleşmede verinin güvenli bir şekilde gittiğinden emin olmak gerekir. Bunun sağlanması ise gönderilen verinin şifrelenmesi ile olur. Böylece açık haberleşme kanalları kullanılarak verinin güvenli bir şekilde ulaştırılması sağlanır. İletişimde, açık bir haberleşme kanalı (internet gibi) kullanılıyorsa gizli tutulmak istenen bilginin yetkisiz bir kişi tarafından dinlenebileceği veya haberleşme kanalına girip (araya girme) veriyi bozabileceği ya da değiştirebileceği (yanlış verinin gönderilmesi) düşüncesi her zaman için önemli bir problem oluşturur. Bu noktada, mesajların herkesin erişimine açık elektronik haberleşme kanallarından iletilebilmesi için bir takım dönüşümler sonucunda değişikliğe uğratılarak üçüncü şahıslar için anlaşılamaz bir hale getirilmesi gerekmektedir. Bu amaçla yapılan tüm işlemlere birden kriptografi ya da şifreleme adı verilir . Diğer bir tanımla kriptografi, en az iki kişinin güvenli olmayan bir kanal üzerinden üçüncü bir şahsa bilgi sızdırmadan haberleşmesini sağlamak amacıyla matematiksel tekniklerin geliştirilmesidir[1].

Kriptoloji esas olarak iki bölüme ayrılır: Kriptografi (şifreleme) ve kriptoanaliz (şifre çözme). Gönderilmek istenen orijinal mesaj açık mesaj (plaintext) ve bu mesajın şifrelenmiş hali şifreli mesaj (ciphertext - cryptograph) olarak adlandırılır.

Şifreleme, askeri ve diplomatik iletişimde (haberleşmede) güvenliği sağlamak için bin yıldır kullanılmaktadır. Ancak bugün artık özel sektörde de gereksinim duyulmaktadır. Sağlık hizmetleri, finansal işler (örneğin: kredi kart işlemleri) gibi konularda bilgisayarlar arasındaki haberleşmede açık kanallar kullanılarak yapılmaktadır. Bu açık kanalların kullanılması sırasında yukarıda sayılan işlerin güvenli ve gizli bir şekilde yapılabilmesi için şifrelemeye gerek duyulmaktadır.



Şekil 1

Bu makalede en çok kullanılan veri şifreleme algoritmaları incelenmiş ve performanslarından bahsesilmiştir. 2. bölümde şifreleme algoritmaları sınıflandırması hakkında bilgi verilmiştir. 3. bölümde DES algoritması,4. bölümde 3DES algoritması,5. bölümde blowfish algoritması incelenmiştir. Son bölümde ise elde edilen sonuçlar yorumlanmıştır.

II. ŞİFRELEME ALGORİTMALARININ SINIFLANDIRILMASI

A. Sınıflandırma Kriterleri

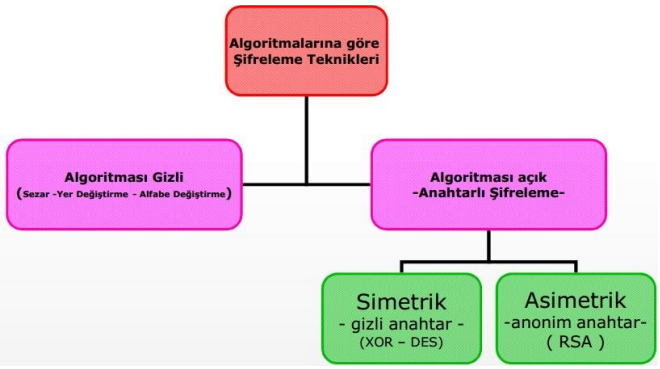
Şifreleme algoritmaları algoritmanın gizliliği ya da açıklığı, algoritmada kullanılan anahtar sayısı ve şifrelenen mesajın tipine göre çeşitli sınıflara ayrılırlar[2].

B. Algoritmalarına Göre Şifreleme Teknikleri

Algoritmaları gizli olan şifreleme algoritmaları şifrelemelerini anahtar kullanmadan yapmaktadır. Üretilen şifrenin çözülebilmesi algoritmanın bilinirliğine bağlıdır.Yani algoritma başka birinin eline geçerse kolaylıkla şifre çözme istenmeyen kişiler tarafından yapılabilir.Bu algoritmanın en bilinir örneği ilk Sezar Algoritmasıdır. Fakat Sezar algoritması daha sonraları anahtarlı olarak kullanılmıştır. Algoritması açık olan şifreleme algoritmalarına anahtarlı şifreleme algoritması

denilmektedir. Bu algoritmalar da kendi arasında "açık anahtarlı / asimetrik" ve "gizli anahtarlı / simetrik" olmak üzere 2'e ayrılmaktadır. gizli anahtarlı şifrelemede hem şifreleme için hem de şifre çözme işlemi için aynı anahtar kullanılmaktadır. Yani şifreleme işini yapan kişi şifreleme yaparken kullandığı anahtarı şifre çözene vererek şifreyi çözmesi sağlanır. Bu algoritmaların en bilinir örneği DES algoritmasıdır. Açık anahtarlı şifrelemede ise şifre ve şifre çözme işlemleri için farklı anahtarlar kullanılır. Bu iki farklı anahtardan birisi gizli anahtar diğeri ise herkes tarafından bilinebilir (umumi) anahtardır. Açık olan anahtardan matematiksel olarak çözülemeyecek düzeyde bir takım işlemlerle kapalı anahtar elde edilir ve sadece bu anahtarla çözülmesi garanti edilir[3,4,5].

Algoritmalarına Göre Şifreleme Teknikleri Şekil 2'de şematik olarak gösterilmiştir.



Şekil 2

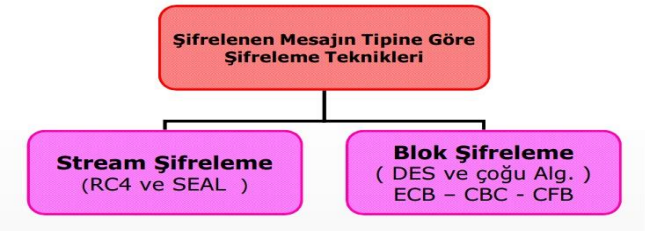
C. Şifrelenen Mesaj Tipine Göre Şifreleme Algoritmaları

Şifreleme algoritmaları kullandıkları mesaj tipine göre de sınıflandırılabilirler. Bu algoritmalar genelde akış şifrelemesi (stream chipper) şifrelemesi ve blok şifrelemesi(block chipper) olmak üzere 2'e ayrılırlar.

Akış şifrelemede, her şifreleme işlemi bir önceki adımdaki çıktıya bağlı olarak değişebilir.Şifreleme genelde küçük (örneğin : 1 bit) boyutlar için yapılır. En bilinir örneği RC4 algoritmasıdır.

Blok şifrelemede, şifrelenecek mesaj belli bir uzunlukta(örneğin : 128 bit) bloklara bölünerek şifreleme işlemi gerçekleştirilir. Birçok şifreleme algoritması bu yöntemi kullanır. En bilinen örneği : DES algoritmasıdır.

Bu sınıflandırma Şekil 3'te şematik olarak gösterilmiştir.



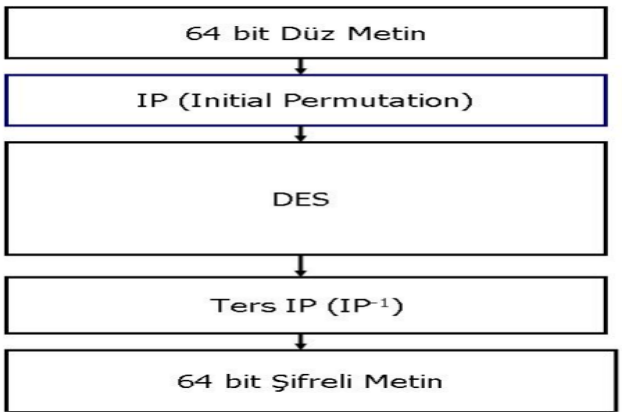
Şekil 3

III. VERİ ŞİFRELEME STANDARTI – DATA ENCRYPTION STANDART (DES)

En çok kullanılan şifreleme tekniği 1977'de şimdiki adı Ulusal Standart ve Teknolojiler Enstitüsü olan Ulusal Standartlar Bürosunda ortaya atılan Veri Şifreleme Standardıdır (DES). DES' de veri, 56-bitlik bir anahtar kullanılarak 64-bitlik bloklar halinde şifrelenir. Algoritma, 64-bitlik bir girişi bazı aşamalar sonucu 64-bitlik bir çıktı oluşturacak şekilde dönüştürür. Şifrelemeyi geri almak için aynı adımlar, aynı anahtar kullanılarak işlenir. Yani kapalı anahtarlı ve simetrik bir şifreleme tekniğidir[1].

A. DES Algoritması

Algoritmanın genel yapısı Şekil 4'te verilmiştir.



Şekil 4

1) Algoritma Adımları :

- 64 bitten oluşan bir metni öncelikle ilk permütasyon (initial permutation - IP) adında bir işlemden geçirir. Bu işlemde bitler bir tablo yardımıyla yer değiştirirler. İlk permütasyondaki bit değişim sırası şöyledir:

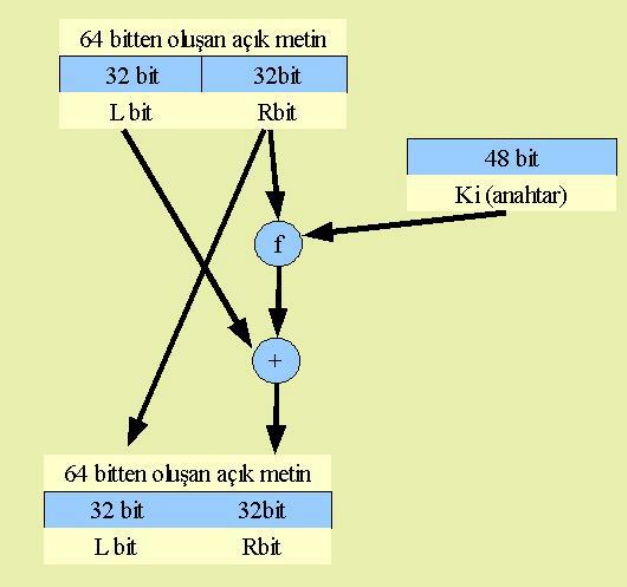
IP

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

- DES, İlk permütasyondan çıkan 64 bit veriyi 2 parçaya ayırarak sağdaki ve soldaki parçaları ayrı ayrı işlemektedir[6,7]. Soldaki parça xor işlemine tabi tutulur. Sağdaki parça çıktının sol parçasının en başından itibaren ters sırada yazılır. Ayrıca sağdaki parça bir f fonksiyonuna anahtar ile birlikte girer. f fonksiyonu giriş yapan anahtar(48 bit) ve sağ parça(32 bit) için işlem yaparak 32 bit çıktı üretir. Sağdaki parçadan çıktı olarak üretilen değer sol parçayla xor işlemine tabi tutulur. Xor işlemi diğer adıyla farklılık işlemi 0-1 ve 1-0 durumlarında 1 çıktısını vermektedir. Diğer

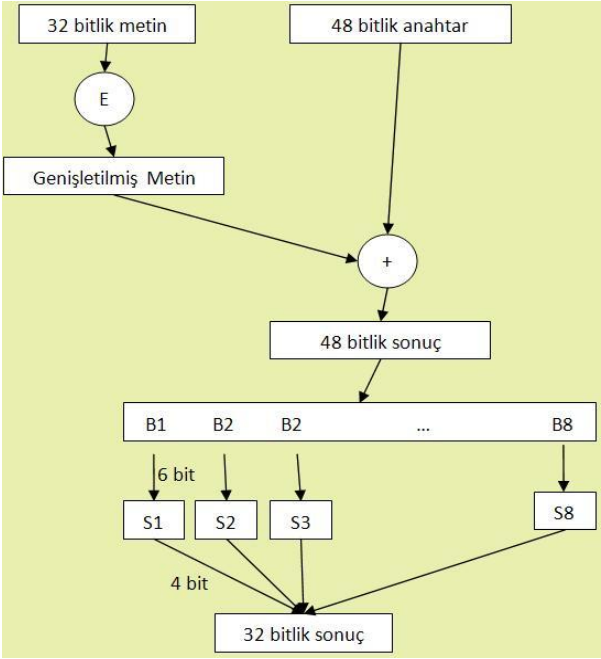
durumlarda 0 çıktısını verir[8]. Bu işlemler 16 defa birbiri ardınca tekrarlanır. Sağ ve sol parça değişerek ilerler.

Şekil 5'te DES kutusunun çalışma şekli gösterilmiştir.



Şekil 5

Şekil 6'ta f (Feistel) fonksiyonunun çalışma şekli gösterilmiştir.



Şekil 6

f fonksiyonunda bulunan E genişletme (expansion) işlemi sayesinde 32 bitlik sağ parça 48 bit haline getirilir (bazı bitleri 2 farklı yere yazarak)[9].

- 2. Adımdan üretilen 64 bit veri ters ilk permütasyona girer (IP-1). IP-1 ile bit değişim şırası şu şekildedir.

***IP*^{1}**

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

Yani giren değerin 40. biti ilk bit, 8. biti ikinci bit olmaktadır. İşlem buna benzer şekilde 64 bit için yapılır.

Yukarda bahsedilen 3 adım sonucunda 64 bit şifreli mesaj elde edilmiştir. Şifrelemede kullanılan anahtar yardımıyla aynı algoritma yardımıyla şifre çözülebilmektedir. Çözme işlemi için ters sırada gidilir.

2) Algoritma Değerlendirmesi

- Anahtar üzerinde değişikliklerle yeni anahtarlar üreterek kullanması güçlü yanıdır.
- DES'in en büyük dezavantajı anahtar uzunluğunun 56 bit olmasıdır. 1977 yılında yayınlanan bu algoritma günümüzde geliştirilen modern bilgisayarlar tarafından yapılan saldırılar karşısında yetersiz kalmaktadır.
- DES kırılabilir yapan en büyük etken Feistel fonksiyonunda bulunan S1,S2..S8 şeklinde gösterilmiş 6 bit veriyi 4 bit e çeviren s-kutuları (s-box) adı verilen yapılardır.

IV. ÜÇLÜ DES – TRIPLE DES (3DES)

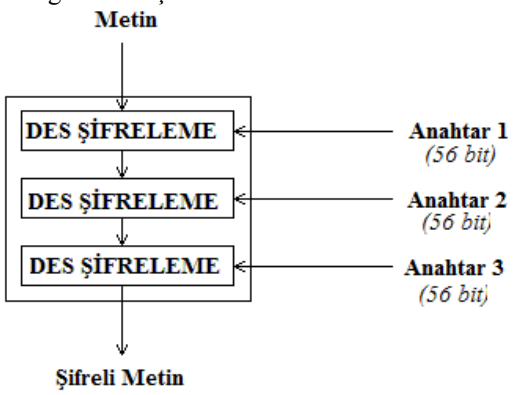
DES algoritmasının kırılabilirliğinin azaltılması üzerine üçlü des (3DES) algoritması geliştirilmiş ve kullanılmaya başlanmıştır. 3DES, DES algoritmasında anlatılan aşamaları aynen yapmakta fakat algoritmada kullanılan anahtar uzunluğu 3 anahtarlı 168 (3*56) bit ya da 2 anahtarlı 112(2*56) bit olacak şekilde geliştirilmiştir.

DES algoritmasında bulunan ilk permütasyon (IP) , DES kutusu aşaması ve ters ilk permütasyon (IP^{-1}) işlemleri 3DES'te de yer almaktadır.

1) Algoritma Adımları:

- A1,A2 ve A3 anahtarlar olsun. Metin A1 anahtarı kullanılarak DES şifreleme algoritmasına gönderilir. Burdan çıkan şifreli mesaj ile A2 anahtarı DES şifre çözme algoritmasına gönderilir bu metni karmaşıklaştırmayı sağlamaktadır. Enson çıkan şifreli mesajla da A3 anahtarı kullanılarak DES şifreleme algoritmasıyla son çıktı elde edilir.

Şekil 7'de 3DES algoritmasının genel çalışma şekli gösterilmiştir.



Şekil 7

2) Algoritma Değerlendirmesi

- 3DES 168 bit anahtar kullanabilme kabiliyeti sayesinde oldukça güvenli olmaktadır.
- DES gibi simetrik çalışma özelliğine sahip olması avantaj sağlar.
- 3DES algoritması DES algoritmasına göre 3 kat yavaş olması dezavantajıdır[12].

V. BLOWFİSH

Blowfish, Bruce Schneier tarafından 1993 yılında tasarlanmış, çok sayıda şifreleyici ve şifreleme ürününe dahil olan; anahtarlanmış, simetrik bir blok şifreleyici (block chipper) dir. Blowfish, 64-bit blok büyüklüğüne ve 32 bit'ten 448 bit'e kadar anahtar uzunluğuna sahiptir. 16-tur Feitel fonksiyonu ve anahtar-bağımlı S-boxes kullanır[13].

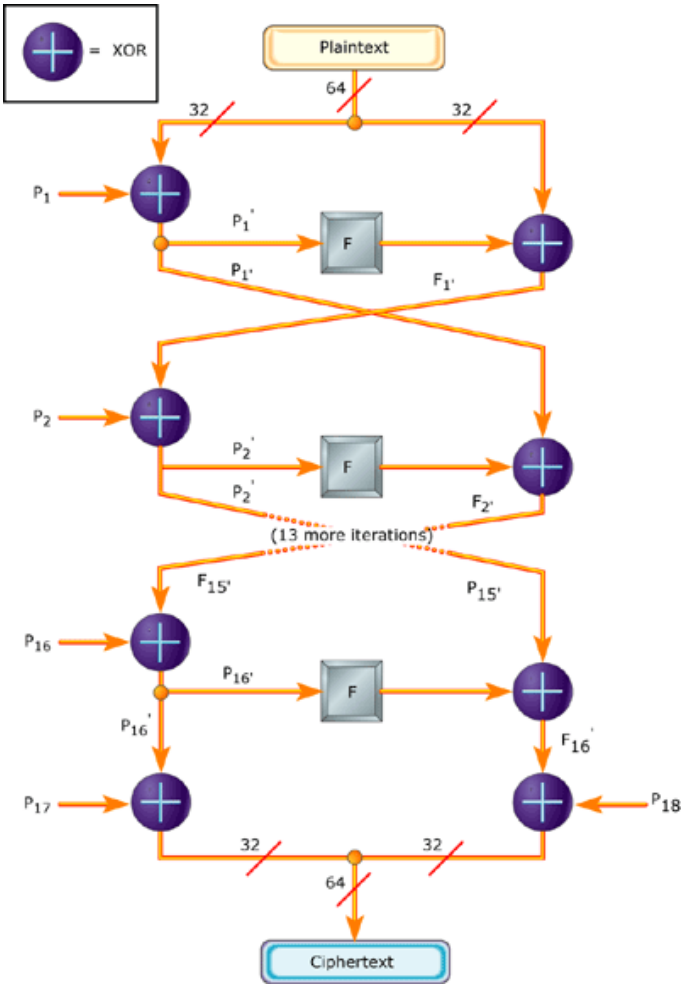
Schneier; Blowfish'i bir genel kullanım algoritması olarak, eskiyen DES'ın yerini alması için ve diğer algoritmalarla yaşanan sorunlara çözüm olarak tasarlamıştır. O zamanlarda, birçok diğer tasarım lisanslı, patentle korunmakta ya da devlet sırrı olarak saklanmaktaydı. Ancak blowfish, patentsiz ve herkes tarafından özgürce kullanılabilir olarak doğmuştur.

A. *Blowfish Algoritması*

1) Algoritma Adımları:

- Her biri 32 bitten oluşan 18 adet alt anahtar elde edilir. Bu alt anahtarlar şöyle elde edilir; 128 bitlik gizli anahtarımız 32 bitten oluşan 4 parçaya bölünür. (K1,K2,K3,K4). Her bir parça da alt anahtarla xor işleminden geçilir ve yeni P değerleri bulunur
- 64 bitlik veri 32 bitten oluşan 2 parçaya ayrılır. sol ve sağ olarak 2 parçaya bölünen metinin sol kısmı 1. alt anahtar olan P1 ile xor işleminden geçirilir ve P' değeri elde edilir. Bu P' değeri de F fonksiyonuna gönderilir. Bu fonksiyondan çıkan değerle verinin sağ kısmı xor işlemine sokulur. Buradan çıkan sonuç F2 sonraki adımda sol kısma , daha önce oluşturulan P' değeri de sağ kısma gelecek şekilde yer değiştirilir.Bu işlemler P16 üstü ve F16 üstü elde edilinceye kadar yapılır yani 16 kez tekrarlanır. Daha sonra kalan 2 alt anahtar yer değiştirme işlemi yapılmadan uygulanır.

Şekil 8'de blowfish algoritmasının genel çalışma şekli gösterilmiştir:



2) Algoritma Değerlendimesi

- Blowfish 3DES ve DES algoritmalarıyla kıyaslandığında daha hızlı çalışmaktadır.
- Blowfish 32 bitten 448 bit' e kadar anahtar uzunluğu ile yüksek güvenlik sağlamaktadır.
- DES ve 3DES gibi simetrik çalışma özelliğine sahip olması avantaj sağlar.
- Tüm alt anahtarları oluşturmak için 521 kez çalışması gerektiği için 4 KB dan daha büyük veri alanlarına ihtiyaç duyması dezavantajı olarak görülmektedir.

VI. SONUÇ

Algoritmalar değerlendirilirken Tablo 1'deki değerler kullanılmıştır.

TABLO I. KULLANILAN ALGORITMALAR

Algoritma İsmi	Anahtar Boyutu (bit)	Blok Boyutu (bit)
DES	64	64
3DES	192	64
Blowfish	448	64

Değerlendirme sonuçlarına göre incelediğimiz veri şifreleme algoritmalarından blowfish , DES ve 3DES e göre hem daha güvenilir hem de daha hızlı çalışmaktadır[15,16]. 3DES ise DES e göre daha yavaş fakat daha güvenilir çözümler sunmaktadır.

Blowfish algoritması anahtar üretme zamanı dışarıda bırakıldığında çok hızlı çalışmasına rağmen 4 KB 'tan daha fazla yere ihtiyaç duyduğu için akıllı kart gibi çok küçük gömülü sistemler içerisinde kullanılamayabilir dolayısıyla bu tür durumlarda 3DES ya da DES iyi bir alternatif olmaktadır.

KAYNAKÇA

[1] T. Yerlikaya, E. Buluş, and N. Buluş, "Kripto algoritmalarının gelişimi ve önemi", Akademik Bilişim Konferansları 2006-AB2006, Denizli-Türkiye, Şubat-2006.

[2] E. Gülaçtı, "Elektronik imza ve güvenlik",Tubitak Uakae,Haziran 2009

[3] "Symmetric-key algorithm", Wikipedia, 2013, https://en.wikipedia.org/wiki/Symmetric-key_algorithm

[4] S.E. Şeker, "Açık anahtarlı şifreleme", 2008, http://www.bilgisayarkavramlari.com/2008/03/19/acik-anahtarli-sifreleme-public-key-cryptography/

[5] "Gizli anahtarlı şifreleme", Wikipedia, 2012, http://tr.wikipedia.org/wiki/Gizli_anahtarl%C4%B1_%C5%9Fifreleme

[6] J. Orlin Grabbe, "The DES algorithm illustrated", Laissez Faire City Times, 1992.

[7] O. Aktaş, "Des algoritması – kriptoloji yazı dizisi 4", 2012, http://acikfikir.org/2012/04/des-algoritmasi-kriptoloji-yazi-dizisi-4/

[8] "Xor chipper", Wikipedia, 2013, http://en.wikipedia.org/wiki/XOR_cipher

[9] S.E. Şeker, " DES (Veri Şifreleme Standardı, Data Encryption Standard)", 2008, http://www.bilgisayarkavramlari.com/2008/03/13/des-veri-sifreleme-standardi-data-encryption-standard/

[10] FIPS 46-3, Data Encryption Standard. National Institute of Standarts and Technology, NIST, 1999.

[11] J. Thakur, N. Kumar, "DES, AES and Blowfish: symmetric key cryptography algorithms simulation based performance analysis", UETAE, 2011.

[12] İ.T.Ü. B.İ.D.B, "3DES Algoritması", 2008, http://www.bidb.itu.edu.tr/?d=891

[13] "Blowfish", Wikipedia, 2013, http://tr.wikipedia.org/wiki/Blowfish

[14] E. Erdem, "Blowfish algoritması", 2013, http://elvanerdem.blogspot.com/2013/03/blowfish-algoritmas.html

[15] A. Nadeem, M.Y. Javed, "A Performance Comparison of Data Encryption Algorithms", IEEE 2005.

[16] A.K. Al Tamimi, Performance analysis of data encryption algorithms, Washington University in St. Louis,2005.