1fd75c3872a94e26ad68c7fa7667bdc82c07dd4ba85f4a6793f7a2b4e943b8fd

**T.C.**

**SAKARYA ÜNİVERSİTESİ**

**BİLGİSAYAR VE BİLİŞİM BİLİMLERİ FAKÜLTESİ**

**BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ**

Kriptolojiye Giriş

PROJE ÖDEVİ RAPORU

**G151210042 – Hüseyin SADE**

**SAKARYA**

**KASIM, 2018**

Kriptolojiye Giriş Dersi

İÇİNDEKİLER

BÖLÜM 1.

1.1 BLOWFİSH ALGORİTMASI NEDİR?.................................................... 3

1.2. ALT ANAHTARIN BULUNMASI……………………………............. 5

1.3. GİZLİ KUTULARIN BULUNMASI (S BOX)........................................ 6

1.4. F - FONKSİYONU…………………...,................................................... 7

1.5. AVANTAJLARI - DEZAVANTAJLARI................................................ 8

1.6. ÇIKTILAR………………………………................................................ 8

BÖLÜM 2.

KAYNAKÇA…………………………………….......................................... 9

**BÖLÜM 1.**

**BLOWFİSH ALGORİTMASI**

1.1 Blowfish Algoritması Nedir?

Blowfish, 1993 yılında Bruce Schneier tarafından tasarlanmış olan bir öbek şifreleyicidir. Feistel ağı kullanan bir blok şifreleme yöntemidir Birçok açığı tespit edilmiş olan DES algoritmasının yerine kullanılmak üzere tasarlanmıştır.

Blowfish ile ilgili olarak şu ana kadar etkin bir şifre çözme analizi var olmasa da, artık AES ya da Twofish gibi daha büyük ebatlı öbek şifreleyicilerine daha fazla önem verilmektedir.

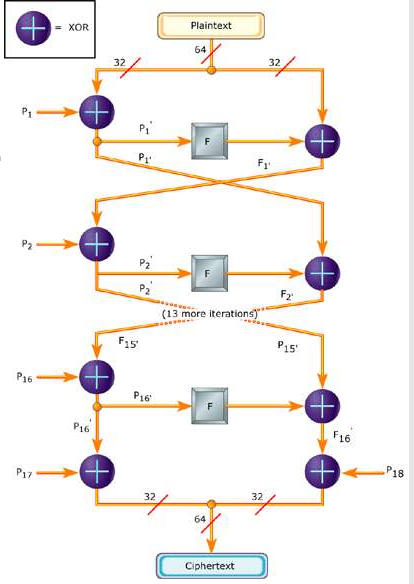
Tasarımın belirgin özellikleri anahtar-bağımlı S-boxes ve oldukça karmaşık anahtar çizelgesini içerir.

Özellikleri:

* Simetriktir.
* Blowfish’te veriler 64 bitlik bloklar halinde şifrelenir
* 32 bitten 448 bite kadar uzunluklu bir anahtar yardımıyla çalışır.
* F fonsiyonu için 4 adet S-Box kullanılır.
* Veriler, basit bir fonksiyonun 16 kez kullanılmasıyla şifrelenir. Her turda anahtar bağımlı permutasyon ve veriye bağımlı yer değiştirme işlemleri yürütülür
* Yaratıldığı zamanda kullanılmakta olan şifreleme algoritmaları lisanslı ve paralı satılmasına rağmen, Blowfish tamamen ücretsizdir.

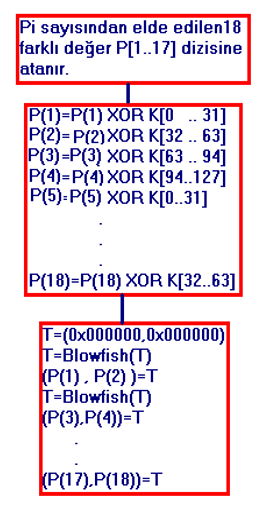
**Algoritma**

* 64 bitlik açıkveri 32 bitlik iki parçaya ayrılır.
* Sol taraftaki 32 bitlik blok ile P dizisinin ilk elemanı XOR işlemine girer. Buradan çıkan sonuç P’ değeri olur ve F fonksiyonuna gönderilir.
* F fonksiyonundan dönen değer ile 32 bitlik sağ taraftaki blok XOR işlemine girer. Buradan çıkan sonuç F’ değerini alır.
* Son olarak sol taraftaki P’ değeri yeni turda sağ blok, sağ taraftaki F’ değeri de sol blok kabul edilerek, aynı işlemler 15 tur daha tekrar edilir.



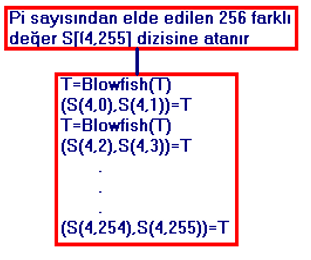
1.2 ALT ANAHTARIN BULUNMASI

* Blowfish algoritması 18 farklı alt anahtar (P) kullanmaktadır.
* P dizisinin başlangıç değerleri pi sayısının ilk 3 rakamı hariç hexadecimal dijitlerinden türetilen değerlerle elde edilir. (Örn:0x243f6a88)
* Daha sonra 128 bitlik gizli anahtarımız 32 bitlik olmak üzere 4 farklı blok haline getirilir. Bunlara (K1,K2,K3,K4) diyelim.
* K dizisi elemanları sırası ile P dizisi elemanları ile XOR lanır. Bu işlemden çıkan sonuçlar ise yine P dizisi elemanlarını ifade eder.
* Daha sonra sadece ‘0’ lardan oluşan bir metin(T) Blowsifh algoritmasına sokulur. Bu algoritma sonucunda gelen 64 bitlik metin (T) 32 bit, 32 bit olmak üzere 2 parçaya ayrılır. İlk 32 bitlik dizi P(1) in, ikinci 32 bitlik dizide P(2) nin yeni değerleridir.
* T metni tekrar algoritmaya gönderilir, fakat bu sefer algoritmada yeni P elemanları kullanılır, algoritmadan dönen değerler P dizisinin 3. ve 4. elemanlarıdırlar.
* Bu işlem P dizisi tamamlanıncaya kadar (P=18) tekrarlanır.



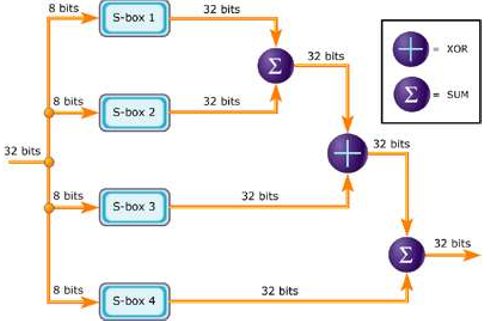
1.3 GİZLİ KUTULARIN BULUNMASI (S BOX)

* Gizli kutular 4 adettir ve 8\*32 boyutlarındadır.
* İlk değerleri Pi sayısından elde edilen değerleri içerir.
* P dizisinde son iki elemanı (T) yine algoritmaya gönderilir. Buradan dönen sonuç 1. gizli kutunun ilk iki elemanını ifade eder.(S(0,0) ve S(0,1))
* İlk elemanı oluşturan metin (T) tekrar algoritmaya gönderilir bu sefer algoritmada yeni S değerleri kullanılır ve bu işlem sonucunda dönen değer 3. ve 4. elemanları oluşturur.
* Bu işlem 1. kutu tamamlanıncaya kadar devam eder. (256 deger)
* Bu döngü geriye kalan diğer 3 gizli kutu içinde gerçekleştirilir.Tek farkı ilk gönderilicek metin (T) bir önceki kutunun son iki elemanın değerleridir.
* Tüm bu döngü işlemleri sonunda pi sayısından elde edilen geçici değerlerin yerini asıl değerler alacaktır.



1.4 F - FONKSİYONU

F-fonksiyonunun değeri;



((S1(B1) + S2(B2))XOR S3(B3))+ S4(B4) olur.

Toplama işlemi burada mod ye göre yapılır.

**DEŞİFRELEME**

* Blowfish algoritmasında deşifreleme işlemi, şifreleme işleminin tamamen aynısının adım adım tersten uygulanmış halidir.
* Deşifreleme algoritması Blowfish algoritmasının alt anahtarlarının tersten kullanılmış şeklidir. Yani deşifreleme algoritmasındaki P(1) değeri şifreleme algoritmasındaki P(18) değerine eşittir.

1.5 AVANTAJLARI – DEZAVANTAJLARI

Avantajları:

* Şu ana kadar bilinen bir Blowfish şifre kırıcı mevcut değildir.
* Piyasada kullanılan en hızlı öbek şifreleyicilerdendir.
* İçerdiği karmaşık anahtar çizelgesi şifrenin kırılmasını zorlaştırmıştır.
* Herkesin kullanımına açıktır. Kullanmak için lisans alma problemi yoktur.

Dezavantajları:

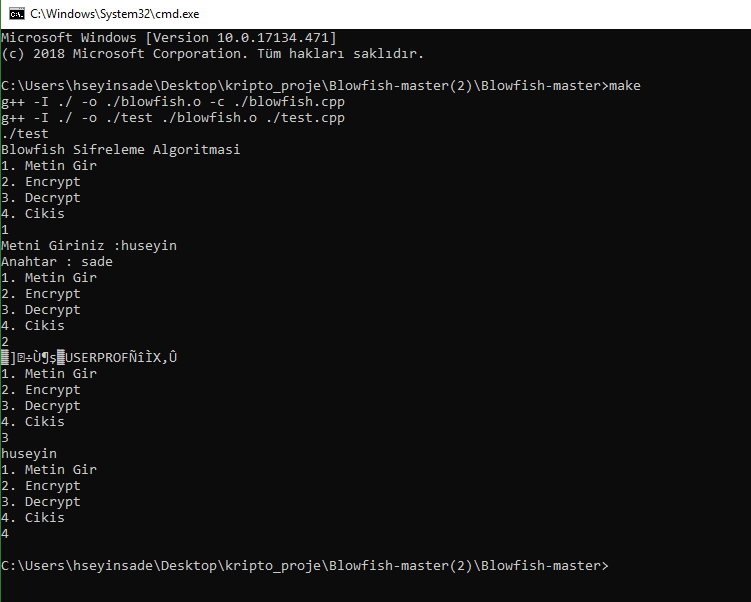
* Çalışmak için 4 kilobyte RAM'den daha fazla belleğe ihtiyaç duyarlar. Bu nedenle ilk akıllı kartlar gibi en küçük gömülü sistemlerde kullanılamazlar.
* 232'den fazla veri öbeğini şifrelemek, Blowfish'in zayıflayıp doğum günü saldırılarıyla bilgi sızdırılmasına sebep olabilir.

Başlıca kullanım alanları:

* E-posta gibi rutin uygulamalar
* Gömülü sistemler

Günümüz .NET teknolojisinde Blowfish öbek şifreleyici algoritmaya ait bir sınıf yer almamaktadır. Bu sebepten dolayı dışarıdan hazır alınan veya yazılımcıların kendi yazdığı sınıf yapıları kullanılmaktadır.

**ÇIKTI**



**BÖLÜM 3.**

KAYNAKLAR

* <https://bidb.itu.edu.tr/seyir-defteri/blog/2013/09/08/blowfish-algoritmas%C4%B1>
* <https://www.slideshare.net/enescaglar/blowfish-ifreleme-algoritmas?from_action=save>

© 2018 Sakarya Üniversitesi.

Bu rapor grubun özgün çalışmasıdır. Faydalanmış olduğumuz kaynakları belirttim. Her hangi bir kopya işleminde sorumluluk bize aittir.

Anahtar Kelimeler: Blowfish Algoritması, Şifreleme, Deşifreleme, S Box, F-Fonksiyonu