KRİPTOLOJİ TAKIMI GRUP ÇALIŞMASI

BLOWFİSH ŞİFRELEME İNCELEME RAPORU

SALİH ÖZTÜRK

ZONGULDAK 2020

İÇİNDEKİLER

BÖLÜM 1

BLOWFİSH NEDİR

Blowfish, Bruce Schneier tarafından 1993 yılında tasarlanmış, çok sayıda şifreleyici ve şifreleme ürününe dahil olan; anahtarlanmış, simetrik bir blok şifreleyicidir. Blowfish ile ilgili olarak şu ana kadar etkin bir şifre çözme analizi var olmasa da, artık AES ya da Twofish gibi daha büyük ebatlı blok şifreleyicilerine daha fazla önem verilmektedir.

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.

Bruce Schneier, bunu şu şekilde ortaya koymaktadır:

> “ *Blowfish, patentsizdir ve tüm ülkelerde bu şekilde yer alacaktır. Algoritma genel kamusal alanda bulunmakta olup, herkes tarafından özgürce kullanılabilir.*

BÖLÜM 2

BLOWFİSH ŞİFRELEME ÖZELLİKLERİ

- Simetriktir bir şifreleme kullanılır.
- Veri 64 bit bloklara ayrılır.
- Her biri 32 bitlik olan 18 alt anahtardan oluşur.
- 4 adet S-Box tan oluşan fonksiyon kullanılır.
- 16 kez tekrarlanır, bu adımlardan alt anahtarlarla XOR işlemi uygulanır.
- 32 bitten 448 bite kadar uzunluklu bir anahtar yardımıyla çalışır.
- Yaratıldığı zamanda kullanılmakta olan şifreleme algoritmaları lisanslı ve paralı satılmasına rağmen, Blowfish tamamen ücretsizdir.
- Şu ana kadar bilinen bir Blowfish şifre kırıcı mevcut değildir.
- Piyasada kullanılan en hızlı blok şifreleyicilerdendir.
- İçerdiği karmaşık anahtar çizelgesi şifrenin kırılmasını zorlaştırmıştır.
- Herkesin kullanımına açıktır. Kullanmak için lisans alma problemi yoktur.
- Çalışmak için 4 KB RAM’dan daha fazla belleğe ihtiyaç duyarlar. Bu nedenle ilk akıllı kartlar gibi en küçük gömülü sistemlerde kullanılamazlar.

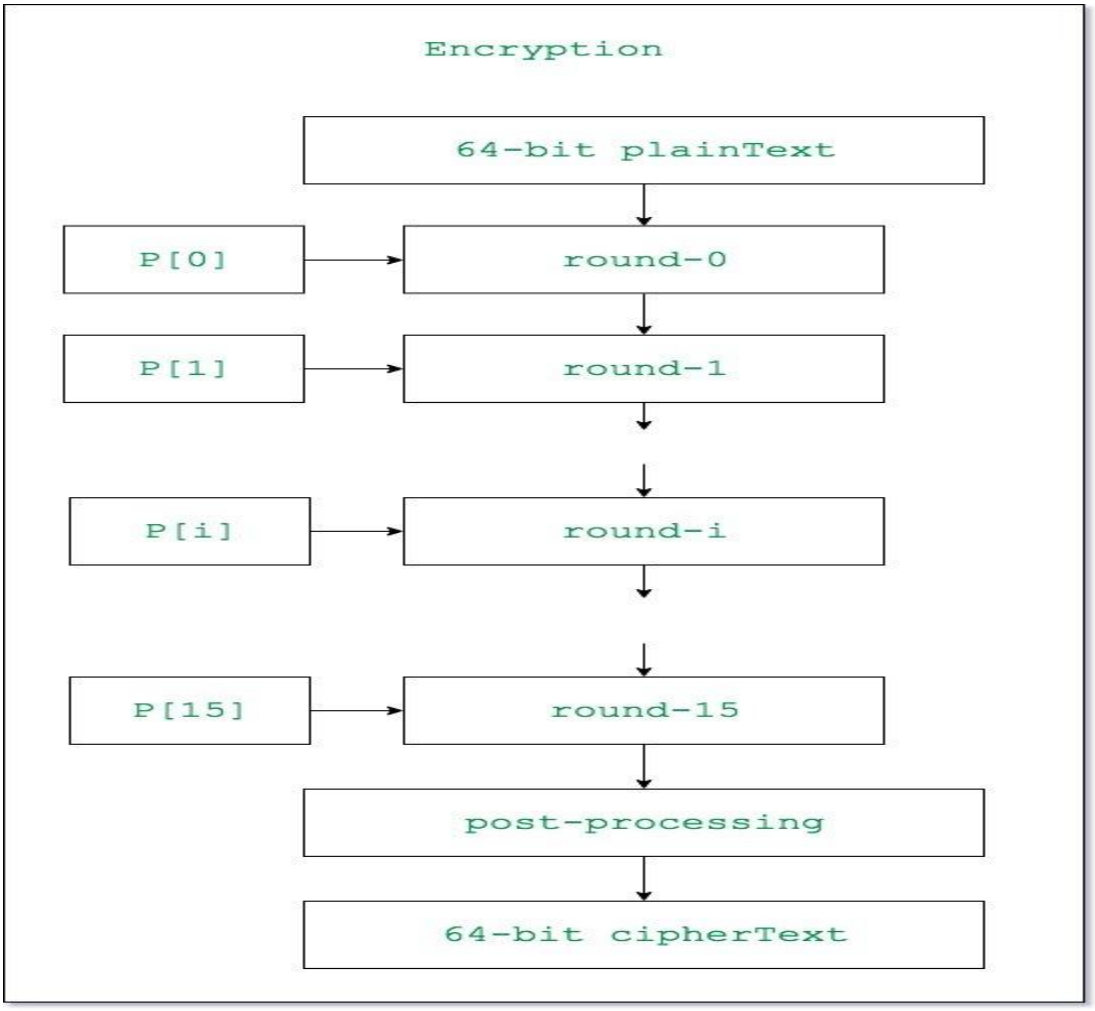
BÖLÜM 3

BLOWFİSH ÇALIŞMA PRENSİBİ

Çalışma prensibine geçmeden önce bilgileri tazelemekte fayda var.

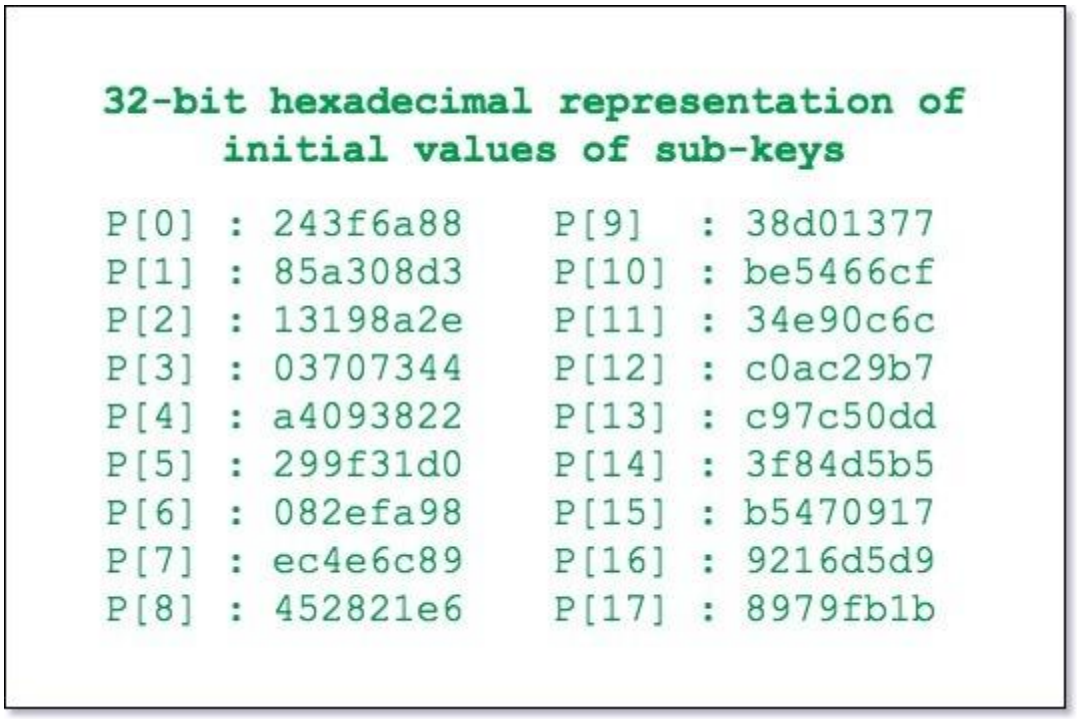
1. **Blok boyutu** : 64 bit
2. **Anahtar boyutu** : 32 bit ila 448 bit değişken boyutu
3. **Alt anahtar sayısı** : 18 [P-dizisi]
4. **Tur sayısı** : 16
5. **S-box sayısı** : 4 [her biri 32 bitlik 512 girişe sahiptir]

Ana hatlarıyla çalışma şekli bu şekildedir.

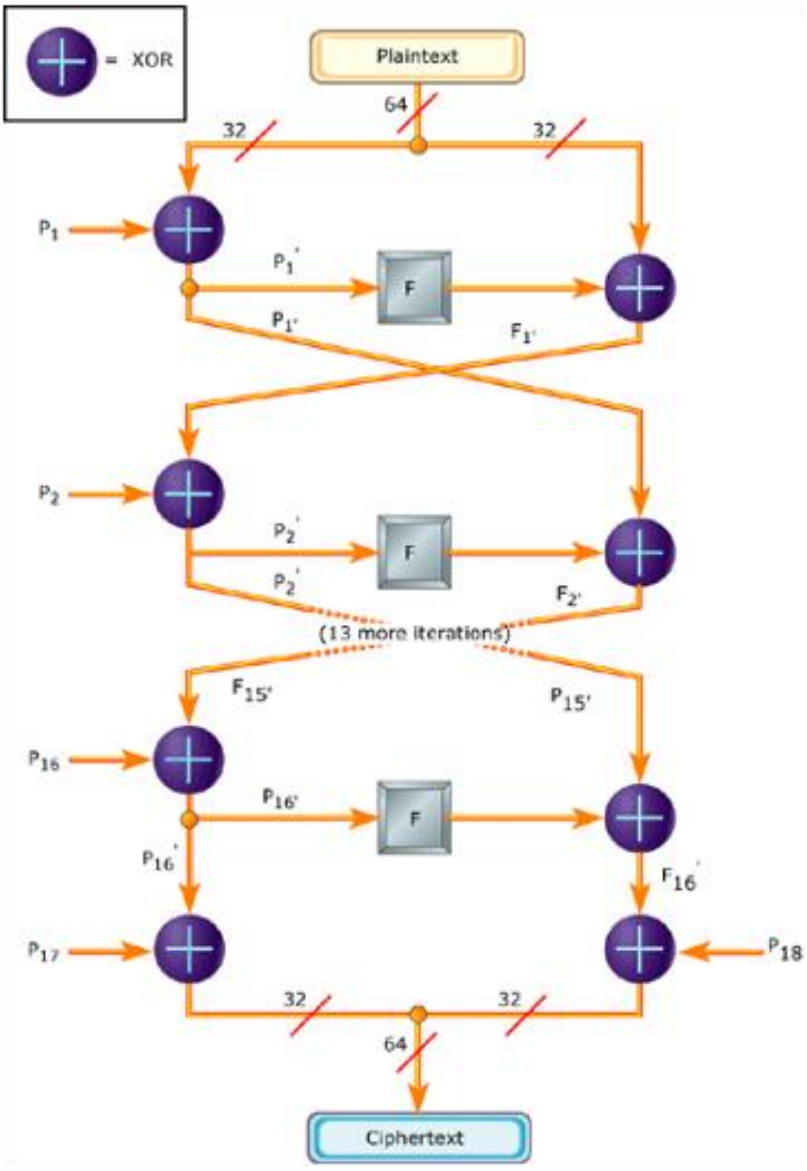


Alt anahtarların oluşturulması:

- Hem şifrelemede hem de şifre çözme işlemi için 18 alt anahtar {P [0]… P [17]} gereklidir ve her iki işlem için aynı alt anahtarlar kullanılır.
- Bu 18 alt anahtar, her dizi öğesinin 32-bit giriş olduğu bir P-dizisinde saklanır.
- Anahtar Pi sayısının ilk 3 rakamı hariç, basamaklarından türetilerek oluşur ve hexadecimale çevrilir.
- Alt anahtarların her birinin onaltılık gösterimi şu şekilde verilir:
- P[0]=”243f6a88”
- P[1]=”85a308d3”
- .
- .
- .
- P[17]=”8979fb1b”



Detaylı olarak çalışma şekline bakacak olursak;

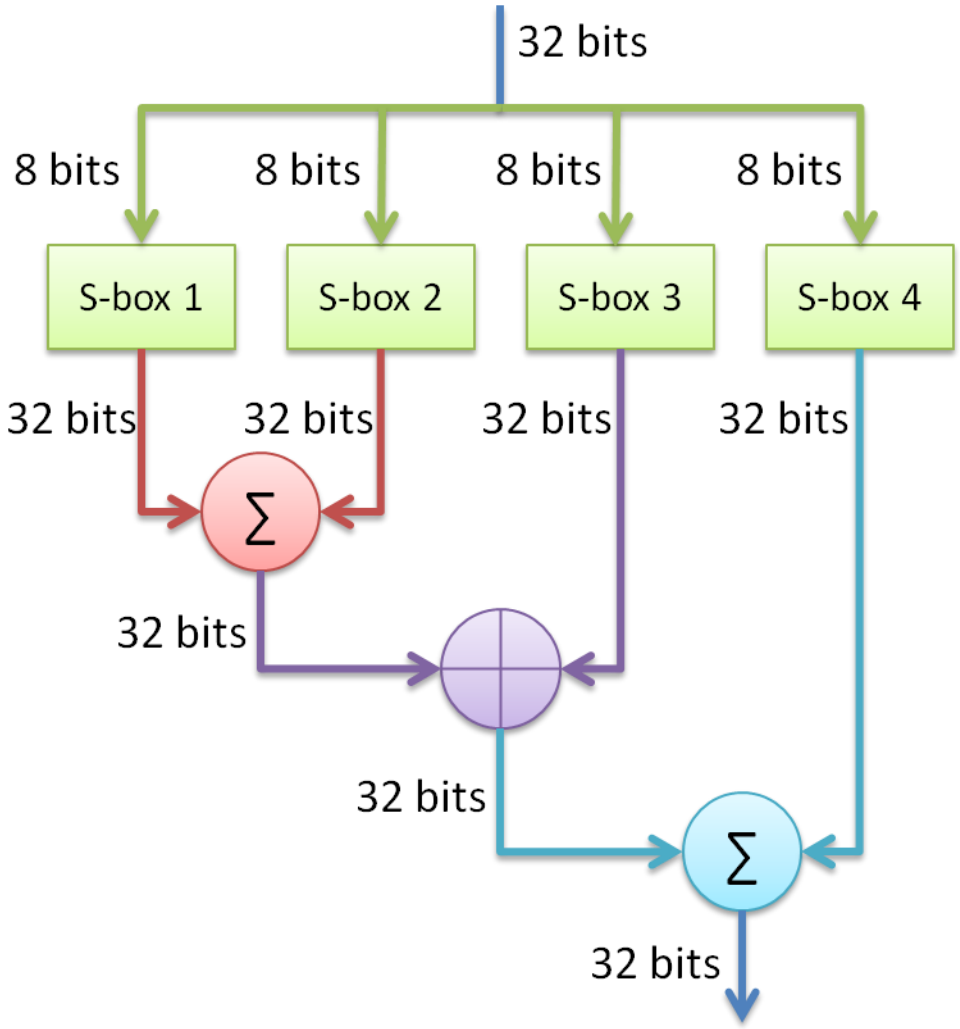


64 bitlik açık veri 32 bitlik iki parçaya ayrılır. Sol taraftaki 32 bitlik blok ile P dizisinin ilk elemanı XOR işlemine girer. Buradan çıkan sonuç P1' değeri olur ve F fonksiyonuna gönderilir. F fonksiyonundan çıkan değer ile 32 bitlik sağ taraftaki blok XOR işlemine girer. Buradan çıkan sonuç F1' değerini alır. Son olarak sol taraftaki P1' değeri yeni turda sağ blok, sağ taraftaki F1' değeri de sol blok kabul edilerek, aynı işlemler 15 tur daha tekrar edilir.

Sonuçta P' ve F'ler P dizisinin en son 2 girişine(17. ve 18. Giriş) kadar fonksiyona değer olarak gönderilir. Son turda yer değiştirme işlemi gerçekleşmez. P16' değeri ile P17 değeri XOR işlemine sokulur. F16' değeri ile de P18 değeri XOR işlemine sokulur. Son olarak sol taraftaki 32 bit veri ile sağ taraftaki 32 bit veri birleştirilerek 64 bit şifrelenmiş veri elde edilir.

F FONKSİYONUNUN AKIŞ ŞEMASI

F fonksiyonunun değeri ; ((S1(B1) + S2(B2)) XOR S3(B3)) + S4(B4) olur. Toplama işlemi burada mod 2^32 ye göre yapılır.



BÖLÜM 4

KAYNAKÇA

https://medium.com/ltunes/si%CC%87metri%CC%87k-blok-%C5%9Fi%CC%87freleme-algori%CC%87tmalari-ve-yapisi-c76fbe80ed4

https://www.slideshare.net/enescaglar/blowfish-ifreleme-algoritmas

https://www.geeksforgeeks.org/blowfish-algorithm-with-examples/

https://tr.wikipedia.org/wiki/Blowfish

https://www.morf.lv/introduction-to-data-encryption