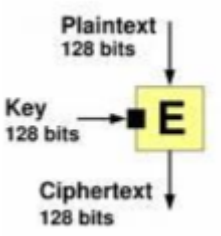
BLOK ŞİFRELEME

Anahtar temelli simetrik algoritmaları iki gruba ayrılır; blok şifreleme (block cipher) ve dizi şifreleme (stream cipher)'dir. Blok şifreleme sistemlerinde şifrelenmesi istenen veri eşit uzunlukta bloklara ayrılır.Blok şifreleme, her blok üzerindeki verinin zamanla senkron bir biçimde tek tek şifrelenmesini sağlar.

$$E: \{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^n$$

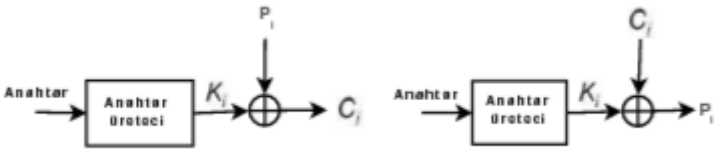
$$E(k, P) = E_k(P) = C$$

Blok şifre sisteminin matematiksel tanımlanması bu şekilde yapılabilir. k-bitlik bir anahtar ile (Aes 'de 128,192,256 bitlik anahtarlar söz konusu) n-bitlik açık veriyi girdi olarak alır. Yine bu n-bitlik açık veriye karşı n-bitlik şifreli veriyi çıktı olarak döndürür.



Her bloktaki şifreleme işlemi kendi içerisinde yapılır. Blok ile yapılan şifreleme sisteminin gücü algoritmada tercih edilen S kutuları, döngü sayısı (Aes'de anahtar uzunluğuna göre değişir), blok uzunluğu, anahtarın uzunluğu ve özelliği ile doğru orantılıdır. Gücünün ölçülmesinde başka önemli unsur ise özellikle günümüz için saldırılara karşı ne kadar dayanaklı olduğudur.

Dizi şifreleme sistemlerinde şifreleme anahtarının üretilip, her bir bitinin sırasıyla verinin her bir bitinin exor"lanması işlemiyle gerçekleşir. Şifrelenmiş verinin çözülmesinde yine anahtarın her bir biti ile verinin her bir bitinin ex-or'lanması sonucu veriyi döndürür.



BLOK ŞİFRE MODLARI

Blok şifrelemede bloklar arasındaki ilişkiye göre çeşitli şifreleme yöntemleri oluşturulmuştur.

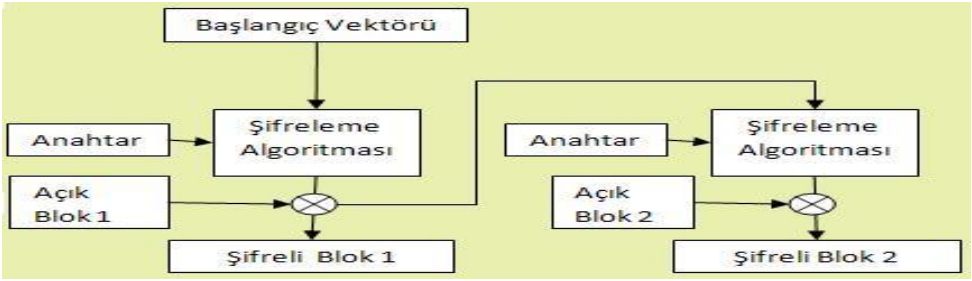
Elektronik Kod Kitabı(Electronic Code Book-ECB): En basit yöntemdir. Veri blok boyutlarına bölünüp birbirinden bağımsız şifrelenir.Düz metin aynı karakterleri içeriyorsa şifrelemiş metinde de bu karakterlere denk düşen yerler aynı olur.

Şifre Blok Zincirleme (Cipher Block Chaining-CBC): ECB'deki basit yöntemin aksine şifrelenecek olan ilk düz metin bloğu rastgele bir sayı ile ex-or işlemine sokulur. Daha sonra takip eden bloklarda bir önceki bloktan gelen şifrelenmiş metnin ex-or'lanması sonucu elde edilir. Bu sayede aynı düz metin aynı şifreli metine sahip olması engellencektir.

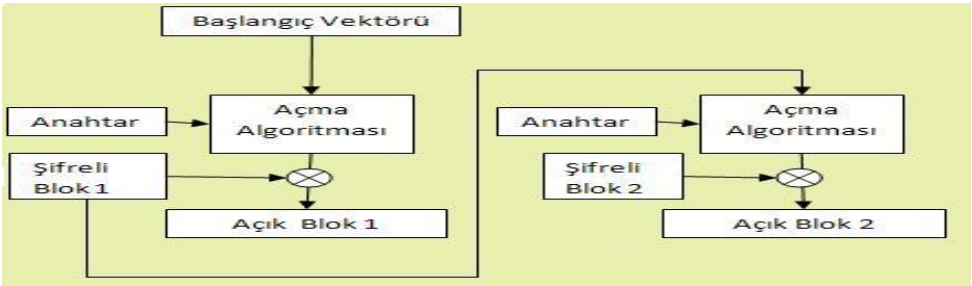
• **Çıktı Geribesleme Modu (Output Feedback Mode-OFM):** OFM'de şifreleme, bir bloğun şifreleme algoritmasından çıktısının bir sonraki bloğun beslemesini sağlayan algoritma sistemine dayanır. Başlangıçta başlama vektörü yer alır, bu vektörün de şifrelenmesiyle ilk OTP bloğu oluşturulur. Bu OTP bloğu, bir sonraki bloğun şifreleme algoritmasında girdi olarak kullanılır.

• **Sayaç Modu (Counter Mode-CM):** OFM'ye benzerdir ama bu yöntemde bir sonraki blok OTP blokları ile beslenmez. Her blok için bir vektör girişi vardır. Bu vektörler matematiksel bir fonksiyon ile birbirlerine bağlıdır. Bu fonksiyon sürekli sayı üretilmesine ve üretilen sayıların kendilerini tekrar etmemesini sağlar. Böylelikle üretilen sayılar, önceden kestirilemez rastgele bir yapıya sahip olur

• **Şifre Geribesleme Modu (Cipher Feedback Mode-CFB):** OFM benzer yapıdadır. OFM'de şifreleme algoritmasından çıkan blok ile sonraki bloklar işleme sokulurken CFB'de bir bloğun şifrelenmesinden elde edilen sonuç, sonraki bloklarla işleme sokulur. Aşağıdaki şekilde şifreleme akış diyagramı gösterilmiştir.



CFB yöntemi için şifre çözme akış diyagramı aşağıdaki gibidir.



BLOK ŞİFRELER – STANDARTLAŞTIRMA

Amerikan Milli Standartlar Bürosu (NBS) bilgi güvenliğinin sağlanması için 1973 yılında şifreleme algoritmasının geliştirilmesi için proje başlattı. 1974'te IBM tarafından geliştirilen finansal uygulamaları elverişli olan bir şifreleme ailesi (LUCIFER) duyuruldu. NBS 1977'de geliştirmiş olduğu ilk standart DES (Data Encryption Standard) şifreleme algoritmasını Federal Information Processing Standard (FIPS 46) olarak duyurdu.

DES, 64-bitlik blok boyutuna ve anahtar uzunluğuna sahiptir. 64-bitlik anahtar uzunluğuna sahip olmasına rağmen 56-bit'i işlevsellik özelliği taşımakta olan bir blok şifreleyicidir. DES her kullanışında ona özel yeni bir anahtar yaratır.Bu da DES'in saldırılara karşı güçlü olmasını sağlar. Fakat günümüz teknolojisi için algoritmasının56-bit'lik anahtar uzunluğuyla çalışması saldırılara karşı yetersiz kalmasına neden oluyor. Bu nedenle NIST 1997'de bir yarışma başlatır. Bunun üzerine 2001 yılında sona kalan 5 finalist algoritma arasından Rijndael Algoritması (Joan Daemen, Vincent Rijmen), DES'in yerine standart olarak atanır. DES'in zayıf yönleri tespit edilerek tüm saldırılara karşı önlemler alınmıştır. Kolay anlaşılabilir yapısı sayesinde birçok ortamda çalışmaya elverişlidir.

AES'in DES'in yerine tercih edilmesinin nedenleri: donanımda ve yazılımda hızlı olması, daha kolay uygulanabilir olması ve çok daha az hafızaya gerek duyması gösterilebilir. AES, 128-bit (16 byte) blok büyüklüğüne ve 128, 192 ve 256-bit gibi değişken anahtar uzunluğuna sahip bir algoritmadır.

Kriptografik Algoritmaların Güvenliği

İyi kriptografik sistemler saldırılara karşı dayanıklı olacak şekilde tasarlanmalıdırlar. Bu saldırı yöntemi, kaba kuvvet olarak adlandırılan olası tüm anahtarların denenmesi şeklinde olabilir.Herhangi bir anahtar boyutuna sahip kriptografik metot için gerekli hesaplama gücü anahtarın uzunluğu ile üstel olarak artar. N sembolüne anahtarın bit sayısı dersek; 2^N olabilecek bütün anahtar kombinosyanlarının sayısını verir.

Anahtar bit sayısı	Adım sayısı	Gereken Ortam
32	2^{32}	Ev Bilgisayarı
40	2^{40}	Ev Bilgisayarı-1hafta
56 **(ÖRN: DES)**	2^{56}	Çok sayıda Ev Bilgisayarının güç paylaşımı ile birkaç ay
80	2^{80}	Çok sayıda Ev Bilgisayarının güç paylaşımı ile birkaç yıl

128 bitli anahtarların kaba kuvvet ile kırılması zordur. Ancak saldırılar için anahtar uzunluğu tek önemli konu değildir. Pek çok şifreleme olası tüm anahtarlar denenmesine gerek olmadan da kırılabilir. Kriptanalistler için kullanılan ekstra yapıda işin içine girmektedir.