Özet

Kullanıcıların kendi kasasını oluşturup o kasaya istediği türde dosyaları güvenli bir bulut sunucusunda saklayabildiği programdır.

Amaç – Kapsam

Günümüzde çoğu kişi gizliliğe önem vermektedir. Bu yüzden de bilgisayardaki dosyaları şifrelemeye çalışmaktadırlar. Fakat bir süre sonra sadece dosyayı şifrelemek yetersiz kalmakta olup dosyaların şifreleri kolay bir şekilde kırılabilmektedir. Bu soruna çözüm olarak kullanıcıların programımız ile kendine ait bir dosya oluşturduktan sonra bu dosyaya attığı her dosya tüm bilgileri ile birlikte şifrelenmektedir. Sadece programımız ile açıldığında dosyalar görüntülenebilecek, aksi takdirde dosyalar herhangi bir anlam ifade etmeyecektir.

Planlama Çözümleme

Proje Kaynakları

Donanım Kaynakları

Ana Bilgisayar

Yerel Alan Ağı (LAN)

Kullanıcı Bilgisayarları (PC)

Yazılım Kaynakları

İnsan Kaynakları

Abdülaziz SÖNMEZ

Mehmet Ali CAFER

Şifrelemede Kullanılan Yöntem

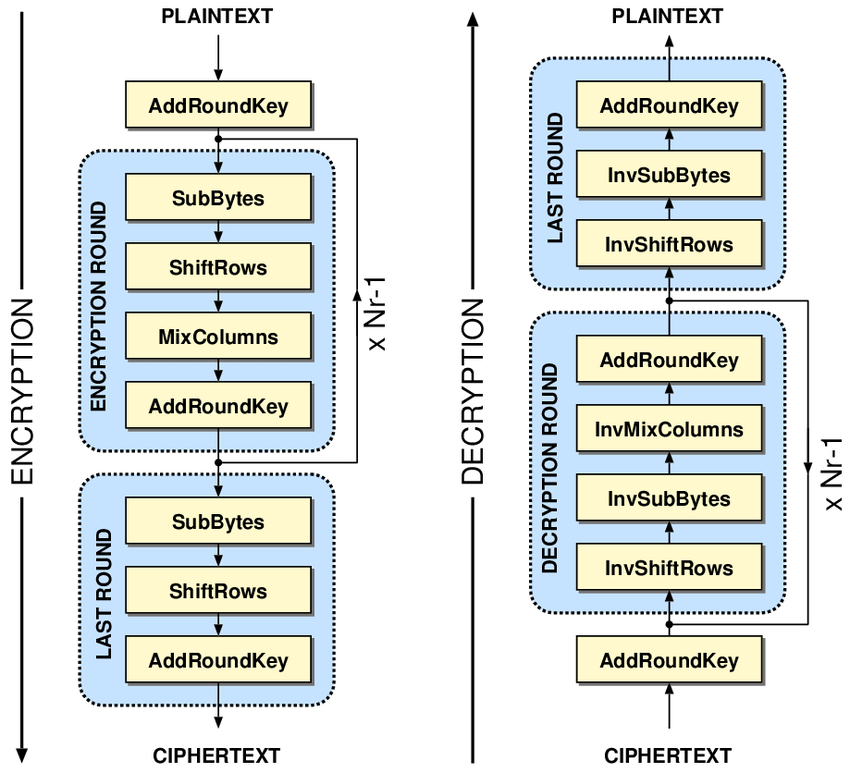
AES (Advanced Encryption Standard) kullanılmıştır.

AES bir simetrik blok şifreleme algoritmasıdır. Simetrik blok şifreleme algoritması gerçek metini şifrelerken ve şifreyi çözerken aynı anahtarı kullanan algoritmalardır.

AES’in çalışma yapısı



Şifreleme İşlemi

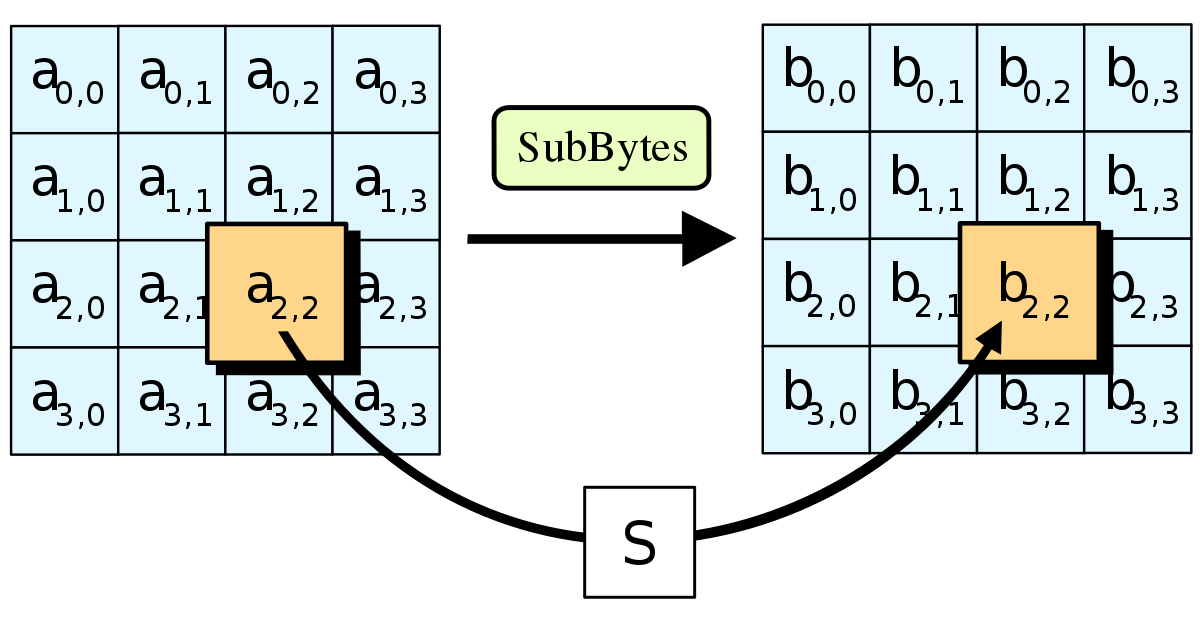


4 adımı vardır.

1. Bayt değiştirme

S: Sbox Tablosu: 256 sayısının 8 bitlik permütasyonlarını içeren 16x16 matristir.

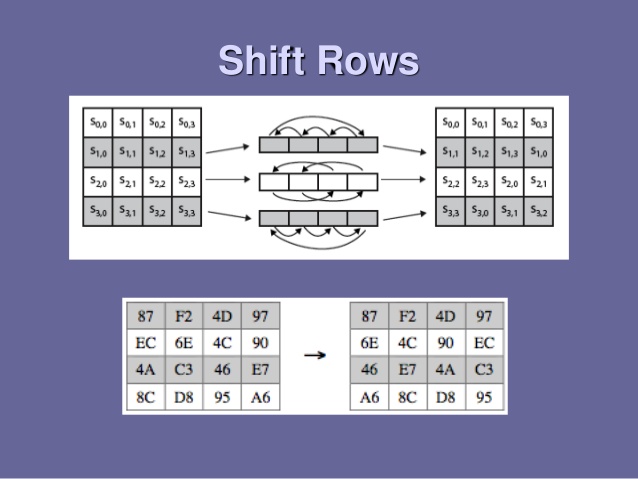
Karedeki her elemanın sbox daki değeri bulunup onunla değiştirilmesidir.



1. Satır kaydırma

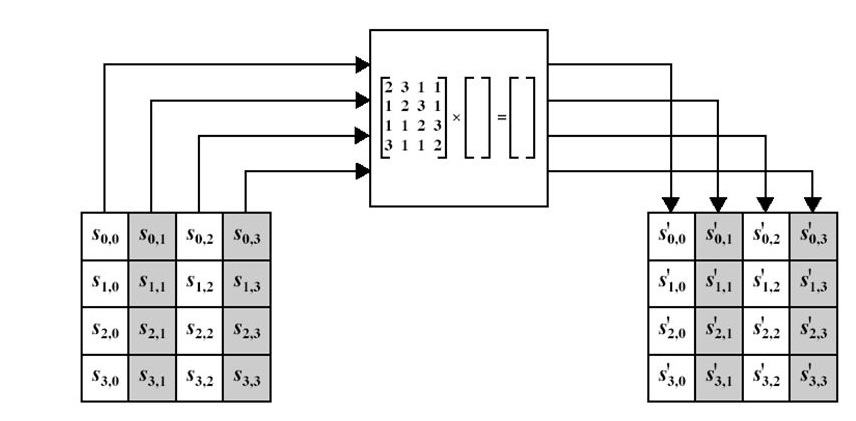
Oluşturulan matrisdeki her satır sola kaydırılır. Satır taşması durumunda tekrardan dizinin en sağına eklenir. Aşağıdaki işlemler uygulanır;

* İlk satır kaydırılmaz.
* 2. satır 1 kere (byte) sola kaydırılır.
* 3. satır 2 kere sola kaydırılır.
* 4. Satır 3 kere sola kaydırılır.
* Sonuç olarak çıkan matris aynı matrisin satırlarının yer değiştirilmiş halidir.



1. Sütun karıştırma

Bu işlemde eski sütunlar kullanılarak yeni sütunlar elde edilmektedir. Bu yapılırken de yeni sütunun elemanlarını eski sütunun her elemanı hesaba katılarak tek tek hesaplanır.



1. Tur anahtarı ile toplama

Her turda daha önce yapılan işlemlerle birlikte bir de tur anahtarı oluşturma işlemi yapılır. Her turda sonuçta oluşan durum ile o tur için hazırlanmış olan yeni anahtar ile xor işlemi yapılır.

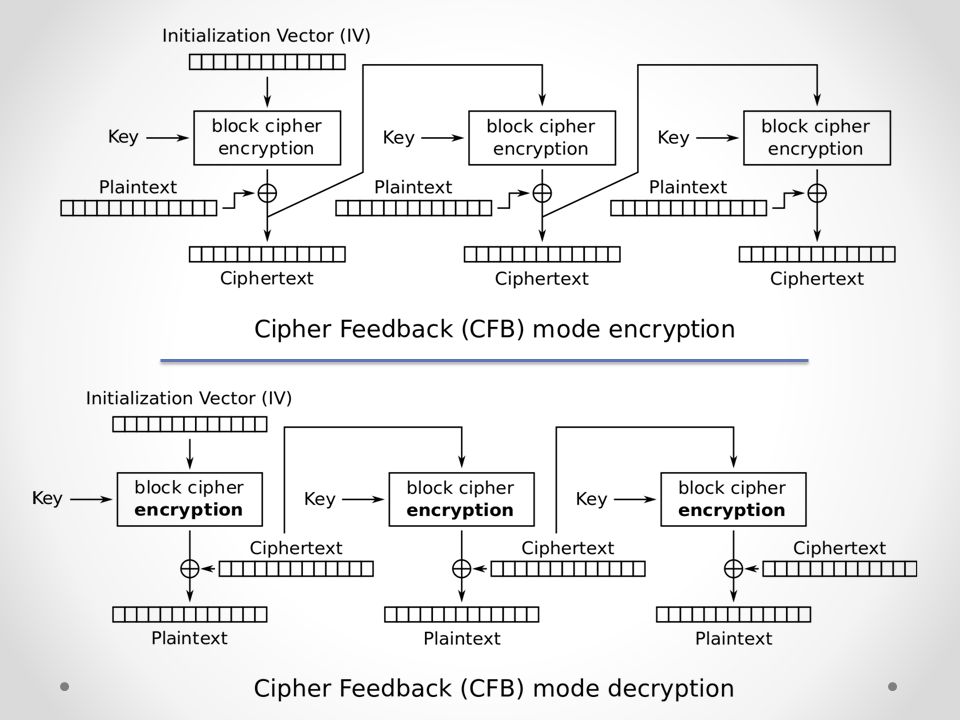
Bizim sistemimizde;

Key Size = 256

Block Size = 128

Cipher Mode = CFB olacaktır.

Cipher Mode:



Initialization Vector(IV)

Tekrarlı kelimeleri veya cümleleri şifrelerken şifrelerin farklı olmasını sağlayan rastgele rakamlardan oluşan vektördür.

Cipher Text: Şifreli metin

Plain Text: Ana metin

Kasa şifresinin hashlenmesi için SHA512 algoritması kullanılmıştır.