Blok Şifreleme Modları

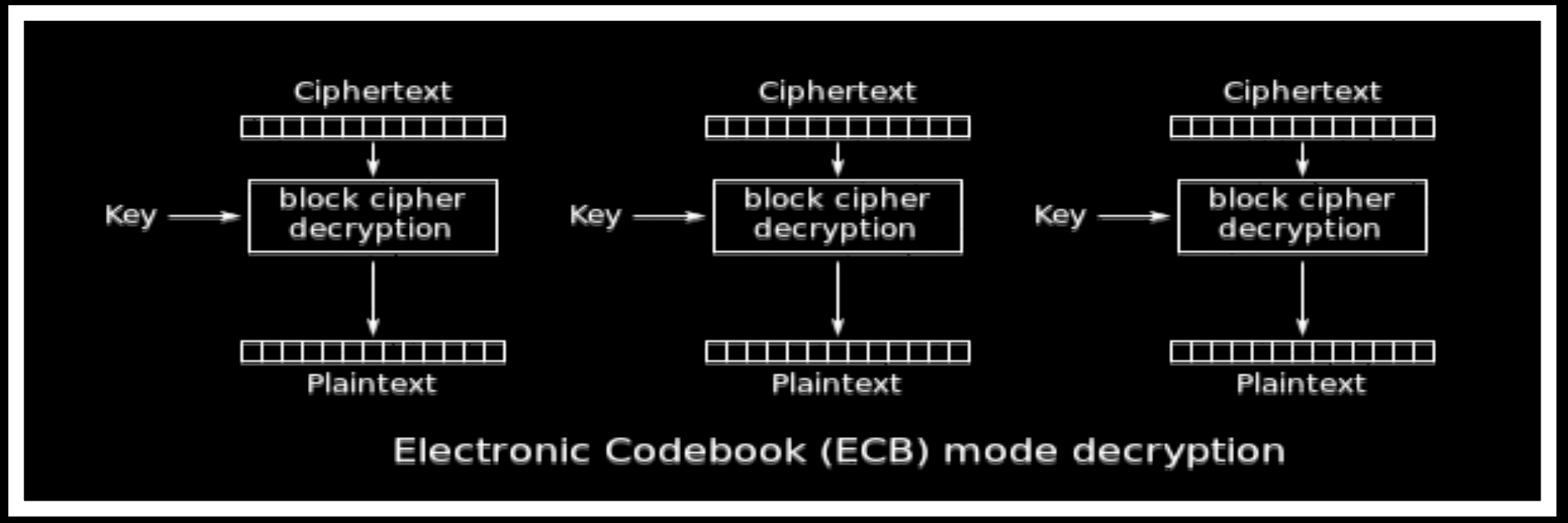
Oluşturan: Furkan Sergen Dayıoğlu

Blok Şifreleme Modları

- Elektronik Kod Defteri (ECB: Electronic Code Book)
- Şifreli Blok Zincirlemesi (CBC: Cipher Block Chaining)
- Yayılımlı Şifre Blok Zincirlemesi (PCBC: Propagating Cipher Block Chaining)
- Şifre Geri Beslemeli (CFB: Cipher FeedBack)
- Çıktı Geri Beslemeli (OFB: Output FeedBack)
- Sayıcı Modlu Şifreleme(Counter Mode Encryption CTR)

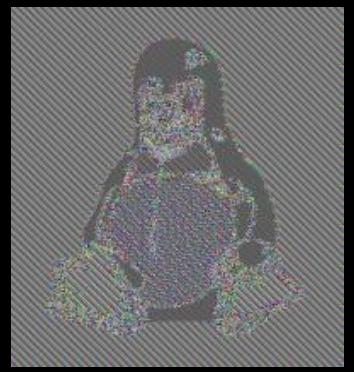
Elektronik Kod Defteri

- En basit şifreleme şekli.
- Data bloklar halinde ve her bir blok diğerlerinden bağımsız olarak şifrelenir.



ECB PENGUIN

- ECB şifreleme modu datayı bloklar halinde şifreler.
- Dolayısıyla aynı data bloğu şifrelendiğinde aynı çıktıyı verir.
- Ve dolayısıyla bu da verinizin data örüntüsünü belli eder.
- Örnek olarak , aşağıda ecb mod ile şifrelenmiş resim gösterilebilir.

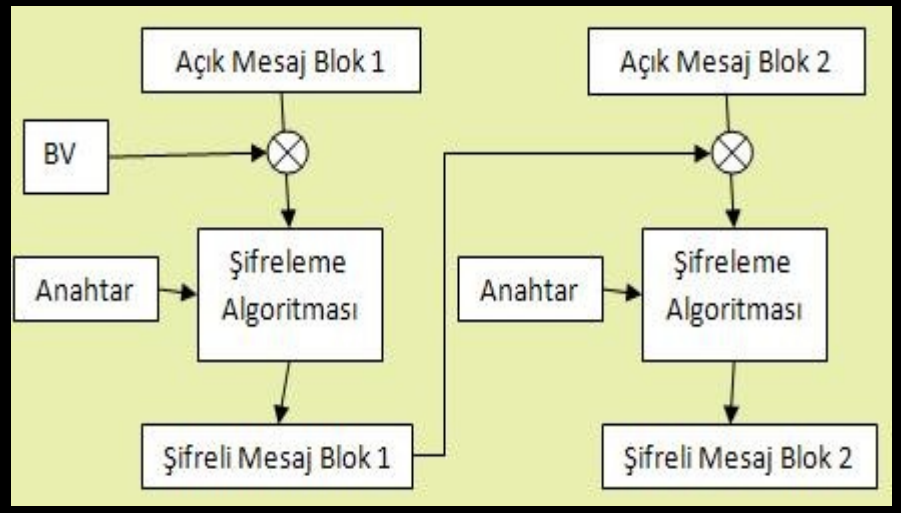


ECB Modun Avantajve Dezavantajları

- Avantaj olarak;
- Basit bir mod. Hızlı ve uygulanabilir.
- Dezavantaj olarak;
- Çözümü basit. Tekrar eden parça varsa veya bir parçası biliniyorsa çözülebilir.
- Aynı data için aynı çıktıyı verir.

Şifre Blok Zincirlemesi

- Data bloklara bölünür.
- İlk blok, bir başlangıç vektörüyle XOR işlemine tutulur.
- Bu işlemin sonucu anahtar değerle şifrelenir.
- Şifreli blok bir sonraki bloktaki data ile XOR işlemine sokulur.

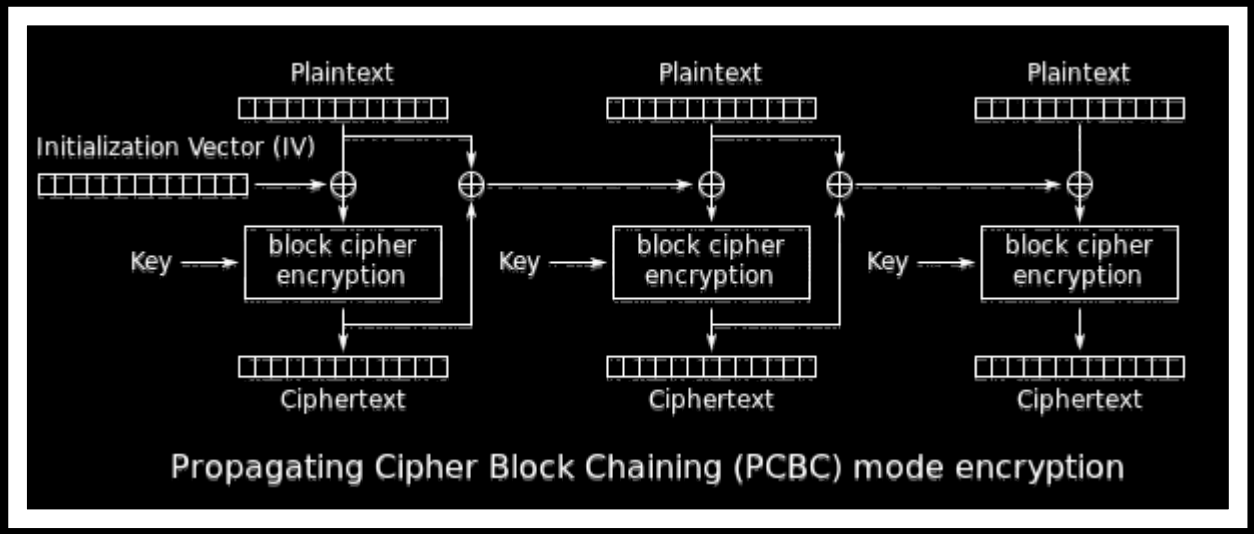


CBC Modun Avantajve Dezavantajları

- Avantaj olarak;
- ECB modun çözülebilirliğini azaltması
- Çözüm olarak aldığı datanın bir bölümü yanlış olacaktır.
- Dezavantaj olarak;
- XOR işlemi

Yayılım Şifre Blok Zincirleme

- İlk blok aynı CBC modunda olduğu gibi şifrelenir.
- Daha sonra ikinci bloğa XOR işlemi için gönderilecek data;
- İlk blok sonucu oluşan şifreli mesaj ile açık mesajın XOR işleminin sonucudur!!

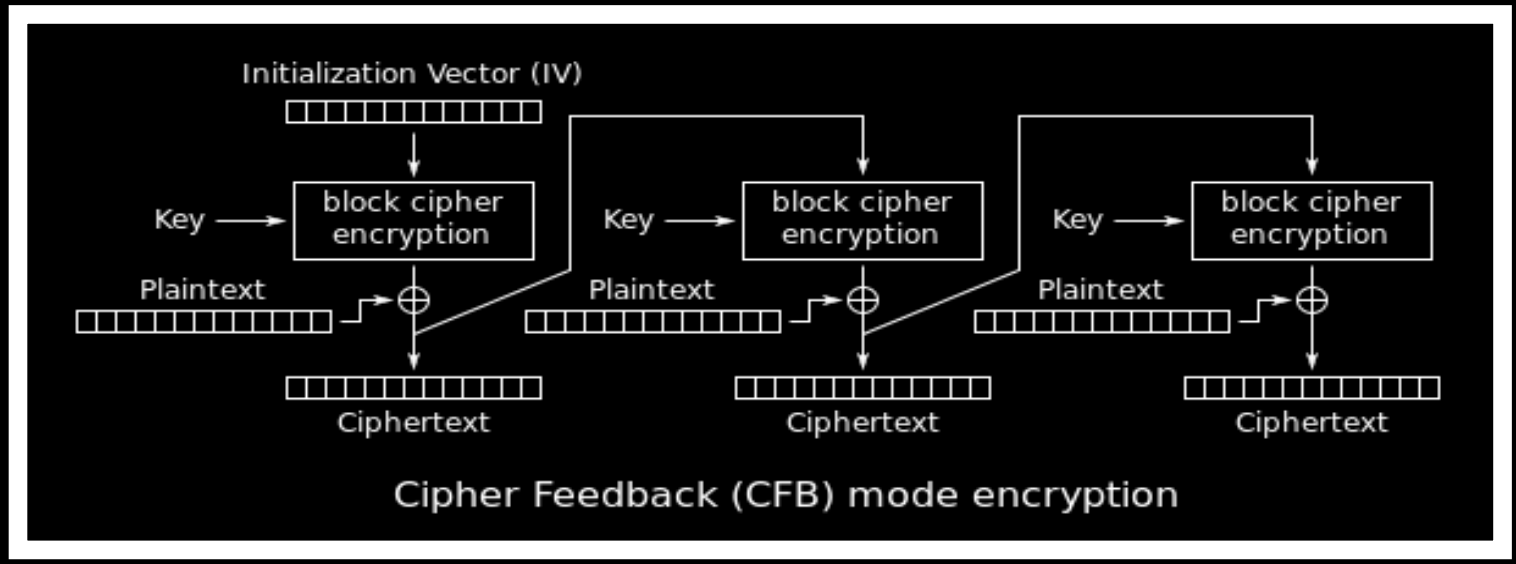


PCBC Modun Avantajve Dezavantajları

- Avantaj olarak;
- Şifrelenen içerik sayısı
- Şifreleme sayısı
- Dezavantaj olarak;
- Arada XOR işleminin kullanılması
- Nispeten yavaş olması

Şifre GeriBeslemeli

- Burada da aynı CBC ve PCBC modlarında olduğu gibi şifrelenmiş blok, bir sonraki blok için giriş değeridir.
- En başta başlangıç vektörü , anahtarla şifrelenir.
- Sonucu ilk(açık) blok ile XOR işlemine sokulur.
- Bu işlemin sonucu oluşan şifreli metin , bir sonraki blok için giriş değeridir.!

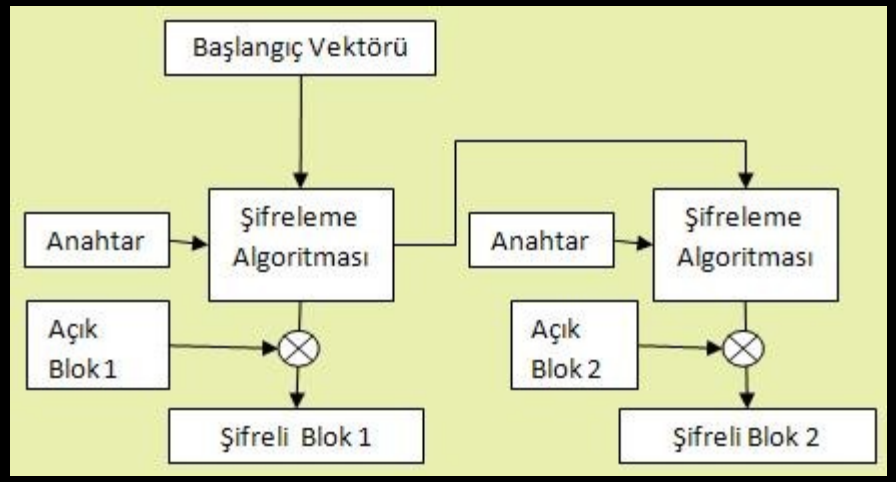


CFB Modun Avantajve Dezavantajları

- Avantaj olarak;
- Bir bir değiştiğinde, bütün datanın çökmesi
- Dezavantaj olarak;
- OFB moda göre yavaş

Çıktı Geri Beslemeli

- CFB modundan farklı olarak burada;
- Anahtar ve İlk vektörün sonucu bir sonraki bloğa girdi olarak gönderilir.

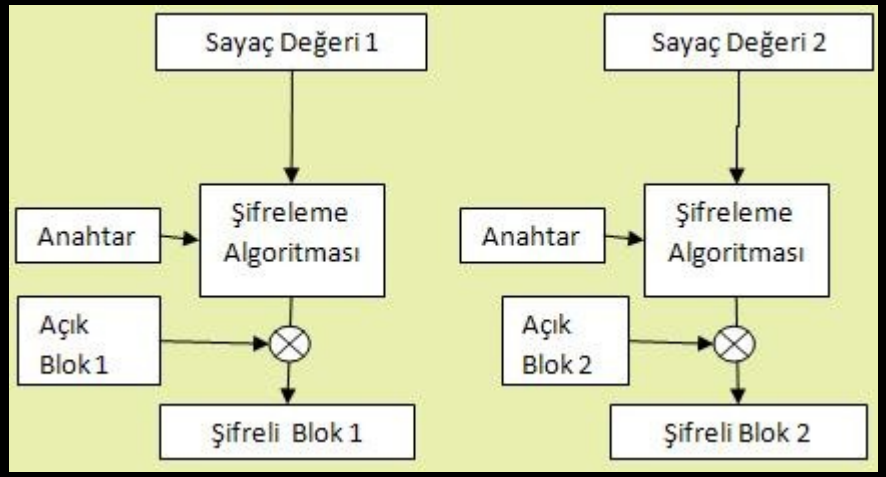


OFB Modun Avantajve Dezavantajları

- Avantaj olarak;
- Hızlı olması
- Şifreleme sayısının fazla oluşu;
- Tahmin edilebilirliği az
- Dezavantaj olarak;
- Aynı anahtar ve aynı başlangıç vektörü kullanıldığında, aynı çıktı
- Ara işlemlerde XOR kullanılması.
-

Sayaç Modlu Şifreleme

- ECB modundaki gibi her blok kendi içinde şifrelenir.
- Her blok , sayaçtan giriş değeri alır.
- İdeal koşullarda sayaç ,tahmin edilemez ve tekrar etmez değerler ürettiği varsayılır.
- Sayaçtan gelen değer ve anahtar şifrelenir.
- Sonucu açık blok ile XOR işlemine sokulur.



CTR Modun Avantaj ve Dezavantajları

- Avantaj olarak;
- Mükemmel (ideal) bir sayaçda çözülmesi zor
- Çünkü tekrar yoktur ve tahmin edilebilirliği neredeyse yoktur
- Dezavantaj olarak;
- Mükemmel sayaç yok.
- Sonuçlar belli bir süre sonra tahmin edilebilir
- Değerler tekrar edebilir.

Karşılaştırmalar

	Enc. Parallelizable	Dec. Parallelizable	Random Read Access
ECB	Evet	Evet	Evet
CBC	Hayır	Evet	Evet
PCBC	Hayır	Hayır	Hayır
CFB	Hayır	Evet	Evet
OFB	Hayır	Hayır	Hayır
CTR	Evet	Evet	Evet

Tavsiye !!!

- https://blog.filippo.io/the-ecb-penguin/
- https://github.com/pakesson/diy-ecb-penguin
- ECB sonucunda penguene ne olduğunu denemek isteyenler için!!

Kaynakça

- http://crypto.stackexchange.com/questions/14487/can-someone-explain-the-ecb-penguin
- https://blog.filippo.io/the-ecb-penguin/
- https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation
- http://bilgisayarkavramlari.sadievrenseker.com/2008/06/07/blok-sifreleme-block-cipher
- https://secgroup.dais.unive.it/teaching/cryptography/block-cipher-modes/