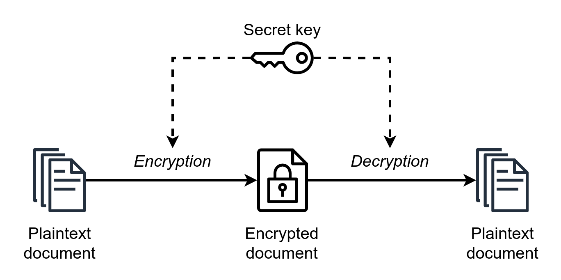
**MODERN SİMETRİK ŞİFRELEME**

Simetrik şifreleme bir gizli anahtar ile birlikte hem şifreleme hem de deşifreleme işleminin gerçekleştirilebildiği bir mantıktadır. Yani bir anahtar yardımıyla şifrelenen mesaj için karşı taraf yine o anahtarla mesajı açılabilmektedir.

 Yanda da verildiği gibi bir gizli anahtar bir metini hem şifrelemek hem de deşifre etmek için kullanılır. Bu yüzden ortak anahtar alıcı ve gönderici tarafta olduğu zaman şifreli haberleşme sağlanmış olur. Fakat asimetrik şifrelemeye göre daha az güvenli bir şifre sistemidir.

**Blok ve Akış Şifreleme Kavramları**

Blok ve akış şifreler simetrik şifreleme altında bulunan iki veri şifreleme yoludur. Her ikisi de düz metni şifreli hale getirebilen simetrik şifreleme algoritması olsa da çalışma şekilleri farklıdır.

Blok şifreleme isminden de anlaşıldığı gibi verileri bloklar halinde işler. Genellikle 64 bit veya 128 bit uzunluğunda blokları ayrı ayrı şifreleme mantığındadır. Blok şifrelemenin uygulanabilmesi için

* Ayrı işlenecek her bloğun uzunluğu aynı olmalı ve aynı anahtar tüm blokları şifreleyebilmelidir.

Bu kuralla birlikte blok şifrelemeyi kullanan yaygın algoritmalar:

* AES (Advenced Encription Standard)
* DES (Data Encription Standard)
* Blowfish

Bazı kullanım modları da bulunur 🡪 ECB, CBC, CFB, OFB

Bu şekilde blok şifrelemeler kullanıldığı algoritmalarda matematiği kullanarak şifreleme yaparken ses ve video şifrelemeleri için bu algoritmalar uygun olmayabilir.

Akış şifrelemeye gelecek olursak, bu şifreleme yönteminde de verilerin şifrelenmesi bitler ve baytlar ile ayrılır. Her bit veya bayt XOR işleminde şifrelenerek bir anahtar akışı oluşturur. Sürekli bir akışta işlenen verilerin senkronize olabilmesi için keystream jeneratörü kullanılır. Bu jeneratör şifreleme ve şifre çözme işlemi için sahte rastgele bir bit dizisi üretmede kullanılır. Bu oluşturulan diziler bit bit veya byte byte biçiminde XOR işlemine tabi tutularak şifreli metin oluşturur. Akış şifreleme algoritmaları:

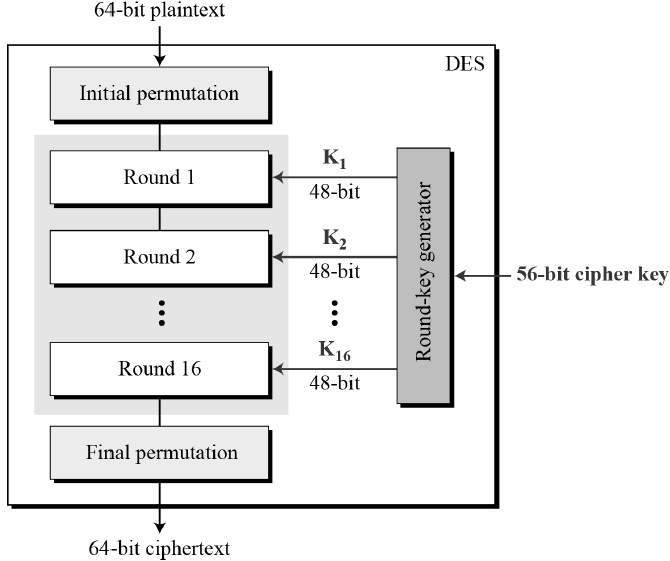
* RC4
* Salsa20/ChaCha20

Akış şifrelemenin avantajı gerçek zamanlı (örn: video, ses) gönderiler için uygun olması ve blok şifrelemeye göre düşük donanımlı sistemlerde daha hızlı çalışmasıdır.

!!! Dosya ve veri bütünlüğünün önemli olduğu yerlerde blok şifreleme tercih edilmeli, gerçek zamanlı ve hızın daha önemli olduğu aktarımlarda ise akış şifreleme tercih edilmelidir.

**Data Encryption Sistem (DES)**

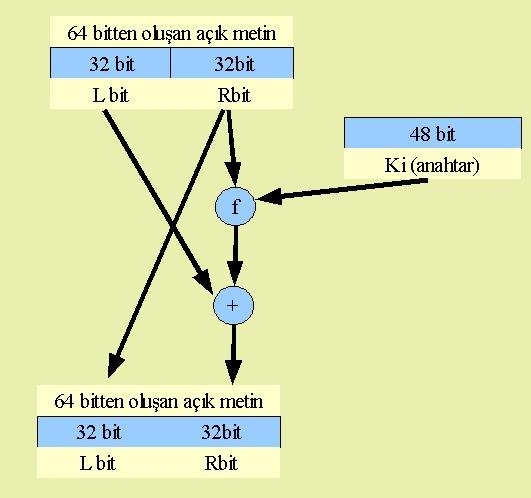
Blok şifreleme algoritması olması sebebiyle DES, şifrelenecek metni parçalara bölerek işler ve her bir parça birbirinden bağımsız olarak şifrelenir. Bu şifrelemeyi geri çözmek istersek de yine bloklar üzerinden aynı anahtar ile bu işlemi yapabiliriz.



>> DES şifreleme blok boyutları 64 bit (8 byte) olacak şekilde verilerin ayrılmasıyla işlenir.

>> Anahtar uzunluğunda 64 bit uzunluğunda olmalıdır. Burada 64 bitin sadece 56 biti şifreleme için kullanılırken geriye kalan 8 bit hata ayıklama için kullanılır

>> 16 round içinde her tur anahtar ile birlikte giren blok kendi içinde yer değiştirme yaparak karıştırılır.

 >> 64 bitten oluşan bir metin önce ikiye ayrılır. Sonrasında sağdaki ve soldaki parçalar ayrı ayrı anahtar ile yer değiştirme yapar.

>> R kısmı f fonksiyonuna gönderilir. Bu fonksiyon 48 bitlik anahtar ile birlikte çalışır. Anahtar ile XOR yapılarak 32 bitlik çıktılar üretilir.

>> R den çıkan 32 bitlik sonuç L kısmı ile XOR işlemi yapılarak yeni Rbit ve Lbit oluşturulur.

>> Buna Feistel şeması denir. Bu 16 tur boyunca devam eder.

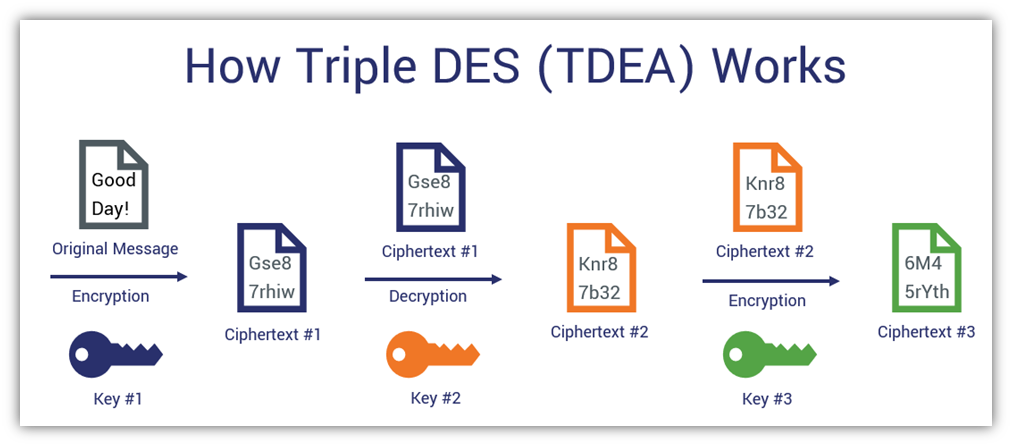
>> Her tur için anahtar farklı dönüşümler gerçekleştirir bu sayede 16 farklı anahtar oluşur.

>> Son turda Lbit ve Rbit kısımları yer değiştirmeler ile birleştirilir ve birleşim ters başlangıç permütasyonuna tabi tutulur. Bu sayede 64 bitlik şifrelenmiş veri oluşur.

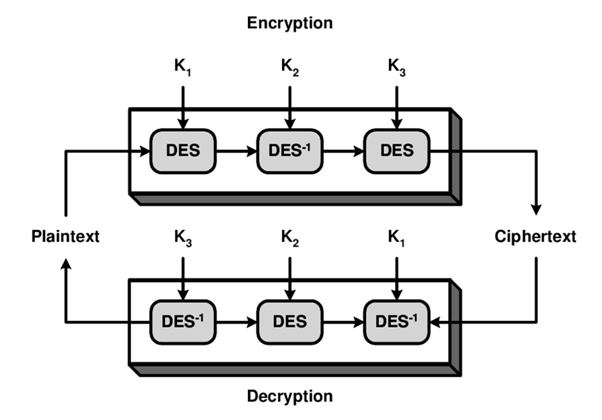
**Triple DES**

Triple DES, klasik DES algoritmasının güvenliği tam olarak koruyamadığı düşünülerek, DES algoritmasının daha güçlendirilmiş versiyonudur. DES algoritması uzun zamandır kullanılan ve sistemlere yerleşik bulunduğu için yeni bir algoritma koymak yerine DES algoritmasını 3 kez uygulayarak Triple DES algoritmasını oluşturmuştur.

* DES şifrelemesi 56 bitlik bir anahtar içerdiği için şifrenin kırılması Brute Force saldırılarıyla kolayca yapılabiliyordu fakat birçok sistem bu algoritmayı kullandığı için DES algoritmasını 3 kez uygulamak hem yerleşik algoritmayı etkilemeyecek hem de şifrenin kırılma olasılığı azaltacaktı çünkü 3 farklı anahtar toplamda 168 bitlik bir anahtar meydana getirmiş olacak.



* 3 kez DES algoritmasına sokulurken Encrypt- Decrypt- Encrypt işlemlerinden geçer. Burdaki işlemler aslında yine DES algoritmasına geri dönüyor gibi gözükse de aslında burada hem DES algoritmasını değiştirmemiş hem de 168 bitlik bir anahtar elde etmiş oluruz. Yani hem DES algoritmasına bağlı kalınır hem de anahtar uzunluğu arttığı için şifrenin kırılma olasılığı azalır.
* S​ifreli Veri=EK1​(DK2​(EK3​(Veri))) şeklinde oluşur buna “EDE” yöntemi denir. Decrypt işlemi içinde bu işlemler ters sırayla yapılır



**Advanced Encryption Standard (AES)**

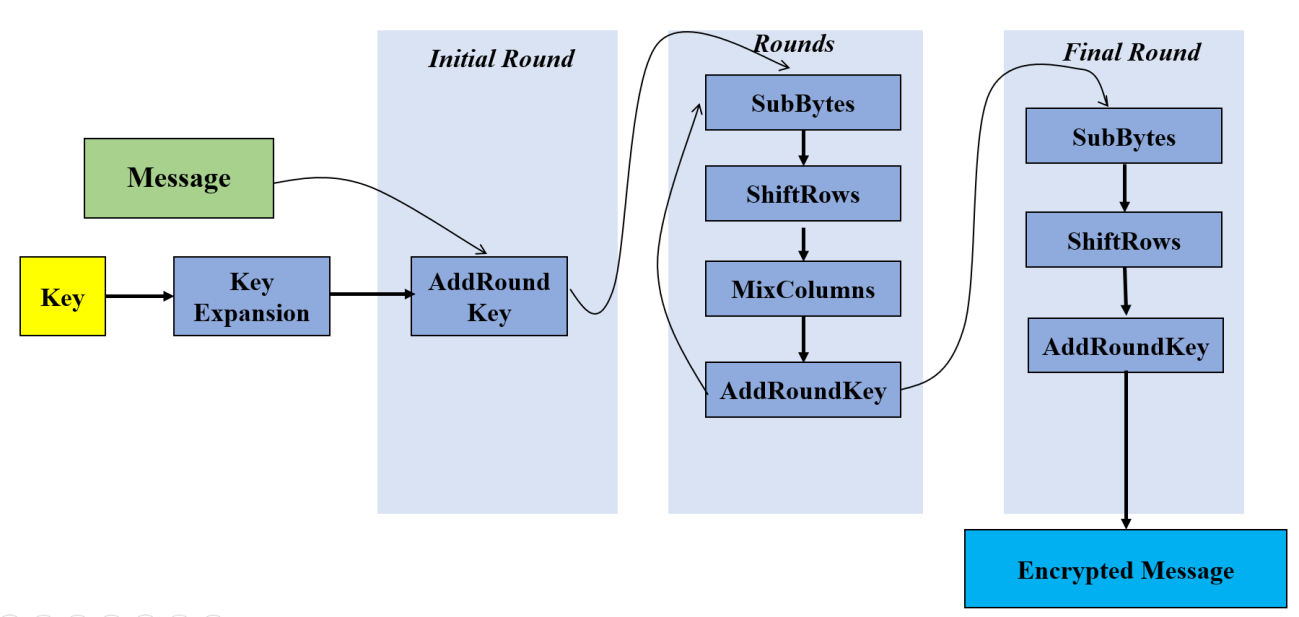
Günümüzde en yaygın kullanılan AES şifreleme algoritması en popüler simetrik blok şifreleme algoritmasıdır. Çünkü AES, Triple DES ve DES algoritmalarından çok daha hızlı, güvenli ve esnektir.

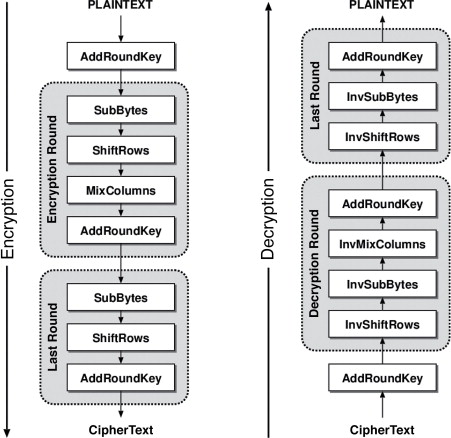
AES algoritması, DES algoritmasının yetersizlikleri üzerine ABD tarafından 2001 yılında yayınlanmış ve kullanılmaya başlanmıştır.

* 128 bit blok boyutu uzunluğu
* 128, 192 veya 256 bit anahtar uzunluğu
* 10, 12 veya 14 tur yaparak bu anahtar uzunluklarını oluştururlar.

<Çalışma Mantığı>

* AES, 128 bitlik bloklar halinde çalışır. Bu bloklar ile işleme giren anahtarlar her tur farklı yeni anahtarlar üretir. Örneğin 12 tur için işleme giren 128 bitlik anahtar, giriş anahtarıyla birlikte 13 anahtar üretir.
* Gizlenecek metin ilk anahtar ile XOR işlemine girer ve her bir turda 4 işlem uygulanır.
* Subbyte adımında her byte bir S-box tablosuna göre değiştirme işlemine girer
* ShiftRows adımında satırlar sola kaydırılarak bir yer değiştirme gerçekleşir
* MixColumns adımında sütunlar matris çarpımı yapılarak karıştırılır
* AddRoundKey adımında alt anahtar XOR işlemi yapılır

🡪Son round yine aynı işlemler tekrar ederken MixColumns adımı uygulanmaz çünkü şifre çözme adımında geri alma işlemini çok zorlaştırırdı o yüzden son tur bu adım yapılmamaktadır.

 >> AES çözme işleminde aynı adımlar ters sırada ve ters işlemlerle yapılır. Yandaki resimdeki gibi.

>> Bu sayede AES algoritması Brute Force saldırılarına karşı dayanıklı anahtarlar üretebilmektedir. Karmaşık lineer dönüşümler ve matrisler kullanılmıştır.

>> Hızlı ve verimli çalışır

🡪Wifi güvenliğinde (WPA2,WPA3)

🡪 VPN, TLS/SSL , HTTPS protokolü

🡪Dosya şifreleme (BitLocker,VeraCrypt)

🡪Mobil uygulamarda örneğin Whatsapp gibi

şifrelemenin önemli olduğu uygulamalarda kullanılır.

**RC4, RC5, RC6 Şifrelemeleri**

RC4, RC5 ve RC6 şifrelemeleri Ron Rivest tarafından geliştirilmiş simetrik anahtar algoritmalarıdır. Yapılarına ve kullanım amaçlarına göre farklılık gösterir.

*>>> RC4 Şifreleme:* Akış şifreleme algoritmalarına dahildir. Hızlı ve basit bir yapıya sahip olduğundan dolayı eskiden SSL/TLS ve WEP sistemlerinde kullanılmaktaydı. Genellikle 128 bitlik anahtar uzunluğunda olmakla birlikte 40-2048 bit arasında değişebilir. Bir bit dizisi olarak akışta bulunan veriler ile;

* Anahtardan 256 baytlık S dizi oluşturulur buna KSA (Key Scheduling Algorithm) denir.
* Oluşturulan S dizisiyle akış anahtarı oluşturulur. Bu anahtar şifrelenecek metinle XOR işlemi yapılarak şifreli metin oluşturulur.
* Başlangıç baytlarının öngörülebilir olması şifrenin kırılma ihtimalini arttırdığından kullanımı çok azalmıştır.

*>>>RC5 Şifreleme:* Simetrik blok şifreleme algoritması olan RC5, RC4’ten daha güvenli olmasıyla birlikte daha modüler ve genişletebilir bir tasarıma sahiptir. Blok boyutları 32,64, 128 bit olabildiği gibi anahtar uzunluğu 0 ile 2040 bit arasında belirlenebilir. Tur sayısı da 0 ile 255 arasında değişkenlik gösterebilir. Şifrelenecek veriler her tur bazı manipülasyonlara, rotasyonlara, toplama ve XOR işlemlerine tabi tutularak şifrelenir.

Günümüzde hala eksikler bulunmasıyla birlikte düşük güç tüketimli olan mikrodenetleyiciler de kullanılabilmesiyle birlikte pek tercih edilmediğini ver yerini AES şifrelemenin aldığını söyleyebiliriz.

*>>> RC6 Şifreleme:*  RC5’in gelişmiş versiyonu olarak kullanılan RC6, AES yarışması için geliştirilmiş bir algoritma olarak ortaya çıkan simetrik bir blok şifreleme algoritmasıdır. RC5’e benzer bir çalışma stili olsa da daha karmaşık bir yapıya sahiptir.

* 128 bitlik blok boyutu
* 128, 192, 256 bitlik seçilebilen anahtar boyutu
* Varsayılan olarak 20 tur olacak şekilde tasarlanmıştır.

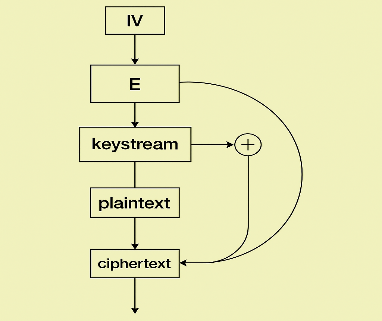
AES finalistlerinden olsa da AES olarak seçilememiştir fakat işleyişi itibariyle yüksek güvenlik ve hız sunar.

!!!KARŞILAŞTIRMA:

* Güvenlik açısından en güçlü RC6 en zayıf RC4
* RC4 akış şifreleme kullanırken, RC5 ve RC6 blok şifreleme kullanır.
* Anahtar uzunluğu RC4 ve RC5 de ortalama 2040 bitlere çıkabilirken, RC6’ da 256 bite kadar çıkar.

**Şifreleme Modları**

Şifreleme modları, AES ve DES şifreleriyle herhangi bir bağı bulunmaz ve onlar gibi bir algoritmik yapıları da yoktur. Şifreleme modlarında amaç, şifrelemeye girecek olan plain text’in seçimi ve text için gerçekleştirilecek işlemlerdir. Blok şifreleme algoritmasının farklı şekillerde kullanabilmesini sağlar. Modlar sabit uzunlukta veri şifreleyebilen blok şifreleme algoritmalarını gerçek dünya verilerine uygulanabilecek hale getirirler.

1. ECB (Electronic Codebook): En basit ve zayıf olan blok şifreleme modudur. Yeni blokların çıktıları bir önceki bloğun çıktısına bağımlı olmaması durumu söz konusu olduğu için her veri bloğu birbirinden bağımsız olarak şifrelenir. Bu da aynı bloğun hep aynı şifreli bloğu oluşturmasına sebep olur. Tekrarlanan veri blokları desenin çözülebilmesini kolaylaştırır. Bu durum güvenlik açısından büyük tehlikedir bu yüzden bu modun zayıf bir şifreleme modu olduğunu söyleyebiliriz.
2. CBC (Cipher Block Chaining): Veri bloklarından ilki IV (Initialization Vector) adı verilen vektör ile XOR işlemine sokulur. Sonraki diğer veri blokları kendinden önce şifrelenen veri bloğuyla XOR işlemine girerek arada birbirine zincir şeklinde bağlı bir şifrelenmiş metin oluşur. Bu da her bloğun birbirini etkileyecek çıktılar vermesi sebebiyle şifrelenmiş metnin sürekli değişmesine ve şifre kırmanın zorlaşmasına sebep olur. Bu açıdan güvenli olsa da yavaş bir işleme süresine ve verilerin kolay manipüle edilmesine sebep olur. Çünkü yapılacak ufak bir değişiklik bile zincirdeki diğer blokları etkileyecektir. Bu yüzden fazla tercih edilmeyen bir moddur.
3. CFB (Cipher Feedback Mode): Blok şifrenin akış şifresi mantığında çalışmasını sağlar. Yani rastgele bitler üretir, bu bitleri de zincirdeki her blok kendinden önceki bloktan şifreli metin ve anahtar kullanarak oluşturur. Veri yerine şifreli blok şifrelenir ve sonuçta oluşan veriye XOR işlemi uygulanır. Buradaki mantık şifreleme işlemi yapılan bloğun her turda bir önceki şifreli bloğun üzerinden devam etmesi şeklindedir. Yani geri beslemeli bir mod gibi düşünülmelidir. Tekrar eden desenler bu sayede gizlenir ama hata oluşabilecek herhangi bit bir sonraki bitleri de etkileyeceğinden hata katsayısı büyüyecektir.
4. OFB (Output Feedback Mode): CFB’ye çok benzer şekilde çalışır ama önemli bir farklılığı bulunur. CFB gibi bir blok şifreyi akış şifresi gibi kullanır ama, veri CFB’deki gibi tekrar şifrelenmek için geri beslemeye dahil olmaz. Yani her blok bir sonraki bloğun çıktılarıyla şifrelenmez bunun yerine sadece algoritmadan alınan sonuç çıktısı geri besleme yapar. Burada anlatılmak istenen blokların tek tek şifrelenmeyip şifreleme çıktısının(keystream bloğu) daha sonra açık verilen metinle XOR işlemine girmesiyle açık metinden şifreli metin elde etme yaklaşımdır. Bu sayede bloklar birbirine bağlı olmadığı için zincirleme bir hata yayılımının önüne geçilebilir. Bir bitteki hatadan sadece bir blok etkilenir.

1. Counter Mode (CTR): Yine blok şifreleme algoritmalarını akış şifresi gibi çalıştırmayı amaçlayan bir şifreleme modudur. Bu modda amaç:

* Her blokta var olan sayaç değerinin önce sabit IV (Initialization Vector) ile birleştirilmesi 🡪 IV || Counter.
* Bu birleşimden sonra blok şifreleme algoritmalarından biriyle şifrelenir bu sayede keystream bloğu oluşur.
* Elde edilen KS bloğu ile açık metin XOR işlemine girerek şifreli metin bloğu oluşturulur.
* Blokları geçtikçe sayaç bir arttırılarak diğer bloklar içinde aynı işlemler tekrar eder.
* Şifreyi çözmek içinde şifreli metinle keystream bloğu XOR’lama yapılır. Bu da açık metini verecektir.

**Saldırı Yöntemleri**

Simetrik blok şifrelemelerinde en önemli ve en çok kullanılan saldırı yöntemleri Linear Cryptanalysis (Doğrusal analiz ) ve Differential Cryptanalysis (Fark analizi) saldırılarıdır.

*Linear Cryptanalysis:* Şifreleme işlemlerinde kullanılan S-box çıkışlarındaki ara bitler ile şifreli metin bitleri ve düz metin arasında karşılaştırma yaparak lineer bir ilişki kurmaya çalışır. Eğer doğrusal ilişkilerde belirli tutarlılıklar keşfedilirse bulunan anahtar bitlerinin doğruluğu da artacaktır. Bu şekilde anahtara ulaşacak kadar tutarlı analiz yapıldığı sürece anahtar keşfedilebilmektedir. Özellikle DES şifreleme bu saldırıya karşı dayanıksızdır çünkü 56 bit uzunluğunda anahtar, çok fazla sayıda düz metin ile şifreli metin karşılaştırması deşifre edebilir. AES ise daha dirençli kalmaktadır.

*Differential Cryptanalysis:* İki farklı düz metin arasındaki farkların, şifreleme sonrasında bu farkların nasıl dönüşüm geçirdiğinin gözlemlenmesiyle kullanılan anahtarı ile ilgili bilgi toplamaya çalışarak yapılan bir analizdir. Yani kısaca şifrenin rastgele davranış göstermediği yerleri fark analizleriyle bulmaya çalışmaktır. Çünkü bazı bitler şifreyi oluştururken kritik rol oynarlar bu bitlerin tespit edilmesi de haliyle şifrenin çözülmesinde en çok yardımcı olacak bitlerdir. DES şifreleme yine 56 bit uzunluğunda olması ve yapısı gereği bu analizlerin yapılabileceği bir şifreleme algoritmasıdır. Fakat AES yine bu saldırıya karşı daha dayanıklıdır çünkü S-boxları (verilen girdi bit dizisini belirlenen kurala göre başka bit dizisine dönüştüren yapı) bu saldırılara karşı daha dikkatli tasarlanmıştır.

>>> Bununla birlikte simetrik şifreleme algoritmaları Brute Force, bilinen düz metin saldırısı, seçilmiş düz metin saldırısı, seçilmiş şifreli metin saldırısı, Meet in the Middle, Replay attack, Padding Oracle, Side Channel gibi saldırı türleriyle decrypt edilebilmektedir. Özellikle DES algoritması bunlardan bir çoğu ile deşifre edilebildiği için günümüzde kullanımı çok azalmıştır.