Simetrik Kriptografi

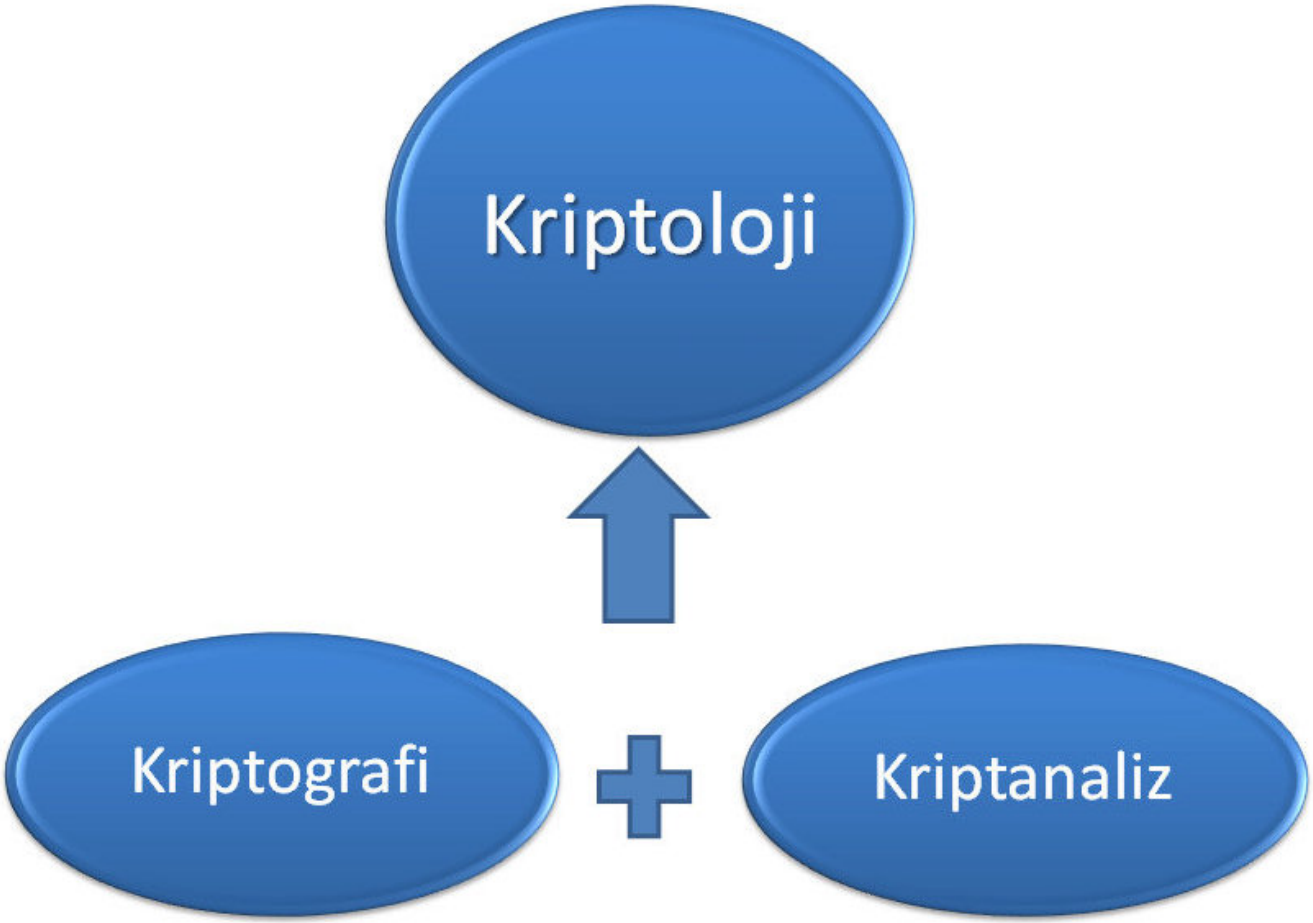
Cihangir TEZCAN

Uygulamalı Matematik Enstitüsü
Kriptografi Bölümü
Orta Doğu Teknik Üniversitesi

Ankara Kriptoloji Seminerleri

12 Mart 2013

Temel Kavramlar



Temel Amaçlar

Gizlilik

Bilgi istenmeyen kişiler tarafından anlaşılamamalıdır.

Bütünlük

Bilginin iletilirken hiç değiştirilmemiş olduğu doğrulanmalıdır.

Kimlik Denetimi

Gönderici ve alıcı birbirlerinin kimlikleri doğrulamalıdır.

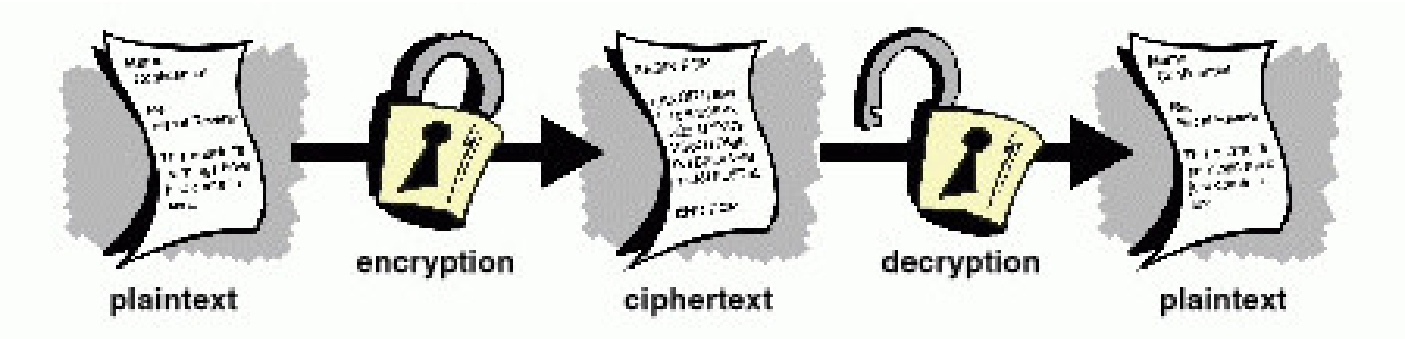
İnkar Edememe

Gönderici bilgiyi gönderdiğini inkar edememelidir.

Kriptosistem/Şifre ne demektir?

Kriptosistem/Şifre ne demektir?

- Korumak istediğiniz şey **düz metin**
- **Şifreli metin** düz metinin şifrelenmiş halidir
- Düz metinden şifreli metin oluşturan ve şifreli metni düz metne geri dönüştüren algoritmalara **kriptosistem/şifre** denir
- Şifreli metin *rastgele* (random) karakterler dizisi gibi gözükmelidir



Kerkckhoffs Prensibi

Kerkckhoffs Prensibi (1883)

Şifre gizli tutulmak zorunda olmamalıdır ve şifrenin düşman eline geçmesi hiçbir sıkıntı oluşturmamalıdır.

Yani, sistemin güvenliği tamamiyle *anahtarın* gizli tutulmasına bağlı olmalıdır.

Claude Shannon

The enemy knows the system.

3 B's of Cryptography

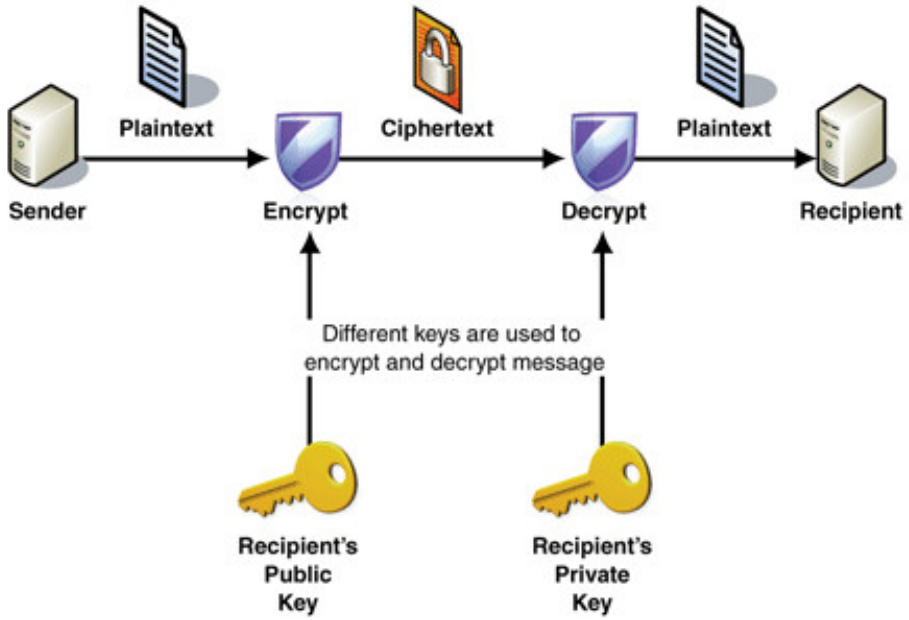
Bribe, Burglary, Blackmail

Simetrik Kriptosistemler

- Şifreleme ve deşifreleme için kullanılan anahtarlar aynı ya da birbiriyle yakın ilişkilidir
- Yani, anahtarın biri, diğer anahtardan kolaylıkla elde edilebilmelidir (in polynomial time)

Asimetrik/Açık Anahtarlı Kriptosistemler

- Şifreleme anahtarı herkesin ulaşabileceği şekilde açıktadır
- Deşifreleme anahtarını elde etmek **zordur**



Asimetrik/Açık Anahtarlı Kriptosistemler

İlgili Dersler

- **MATH 365** Elementary Number Theory I
- **MATH 368** Field Extensions and Galois Theory
- **MATH 473** Ideals, Varieties and Algorithms
- **MATH 476** Algebraic Curves
- **MATH 523** Algebraic Number Theory
- **MATH 551** Algebraic Geometry

Kırılamayan Şifre

Kırılamayan Şifre (One-time pad)

- **Rastgele** bitlerden oluşan çok uzun bir dizi oluşturun (one-time pad)
- Şifreli metin elde etmek için, düz metni one-time pad ile XOR'layın
- Düz metni elde etmek için, şifreli metni one-time pad ile XOR'layın

Kırılamayan Şifre

Kırılamayan Şifre (One-time pad)

- **Rastgele** bitlerden oluşan çok uzun bir dizi oluşturun (one-time pad)
- Şifreli metin elde etmek için, düz metni one-time pad ile XOR'layın
- Düz metni elde etmek için, şifreli metni one-time pad ile XOR'layın

Example

Düz metin	010101111001001...
One-time pad	101111010110101...
Şifreli metin	111010101111100...

Kırılamayan Şifre

Kırılamayan Şifre (One-time pad)

- **Rastgele** bitlerden oluşan çok uzun bir dizi oluşturun (one-time pad)
- Şifreli metin elde etmek için, düz metni one-time pad ile XOR'layın
- Düz metni elde etmek için, şifreli metni one-time pad ile XOR'layın

Example

Düz metin	010101111001001...
One-time pad	101111010110101...
Şifreli metin	111010101111100...

Dikkat

- One-time pad **gerçekten rastgele** olmalıdır
- Her one-time pad **sadece bir kez** kullanılabilir

Akan Şifreler

Simetrik Şifreler iki sınıfa ayrılır

1. Akan Şifreler
2. Blok Şifreler

Akan Şifreler

- One-time pad kullanmak yerine, daha kısa bir anahtar kullanılır (örneğin 128 bit)
- Bu anahtar kullanılarak, uzun bir *sözde* rastgele *anahtar dizisi* oluşturulur ve bu dizi one-time pad gibi kullanılır
- Şifrenin güvenliği çoğunlukla anahtar dizisinin rastgeleliğine bağlıdır

Akan Şifreler

Simetrik Şifreler iki sınıfa ayrılır

1. Akan Şifreler
2. Blok Şifreler

Akan Şifreler

- One-time pad kullanmak yerine, daha kısa bir anahtar kullanılır (örneğin 128 bit)
- Bu anahtar kullanılarak, uzun bir *sözde* rastgele *anahtar dizisi* oluşturulur ve bu dizi one-time pad gibi kullanılır
- Şifrenin güvenliği çoğunlukla anahtar dizisinin rastgeleliğine bağlıdır

Dikkat

Anahtar dizisi artık *gerçekten rastgele* değil, *sözde rastgele*dir

Akan Şifreler

Bazı akan şifreler

- A5/1 (GSM)
- RC4 (WEP)
- E0 (Bluetooth)

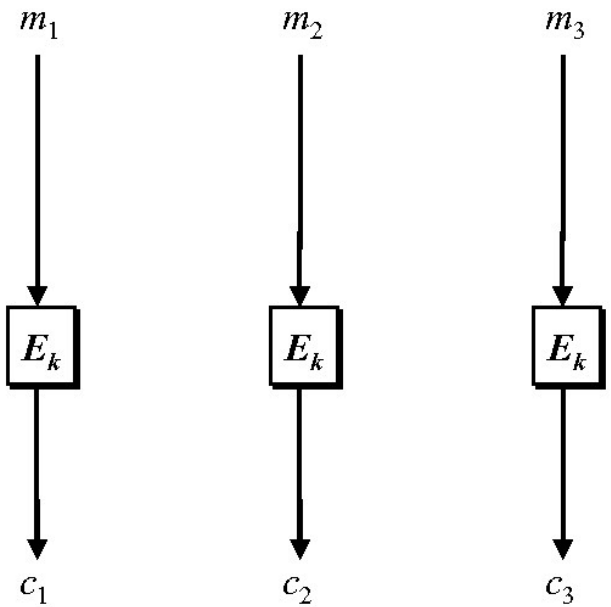
Akan Şifreler

- Genellikle blok şifrelerden çok daha hızlıdırlar
- 2004 yılında yapılan eStream yarışmasına katılan 34 aday algoritmadan 7 tanesi Eylül 2008'de kullanılabilir olarak seçildi ama standartlaştırmak için henüz erken olduğu belirtildi
- Donanım: Grain v1, MICKEY 2.0, Trivium
- Yazılım: HC-128, Rabbit, Salsa20/12, SOSEMANUK

Blok Şifreler

Blok Şifreler

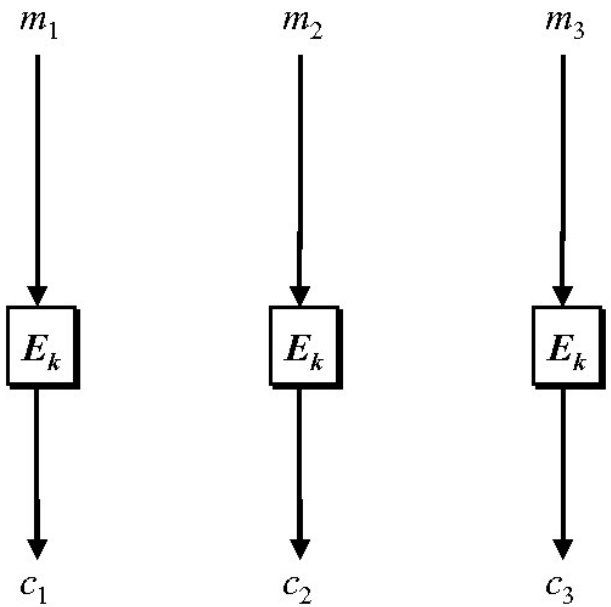
Düz metin eşit uzunluklardaki (b bit) bloklara ayrılıp şifreleme işlemi bloklar üzerinden yapılır



Blok Şifreler

Blok Şifreler

Düz metin eşit uzunluklardaki (b bit) bloklara ayrılıp şifreleme işlemi bloklar üzerinden yapılır



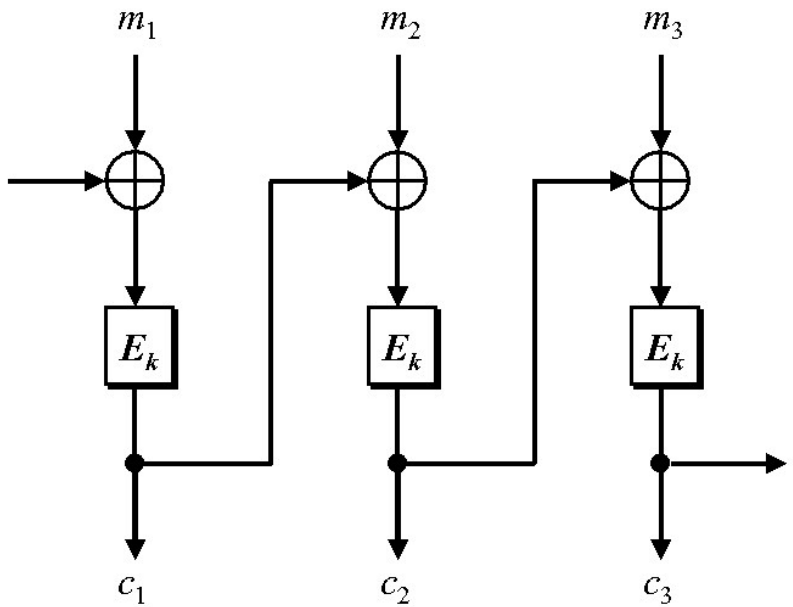
Problem

Direk kullanım tavsiye edilmez: Aynı düz metin blokları aynı şifreli metin bloklarına dönüşür.

Blok Şifreler

Çözüm

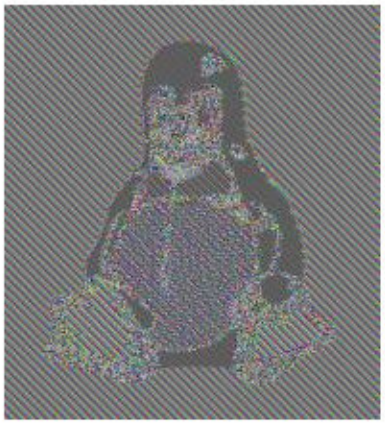
Bir çalışma modu kullanın. örn: Blok şifre zincirleme modu



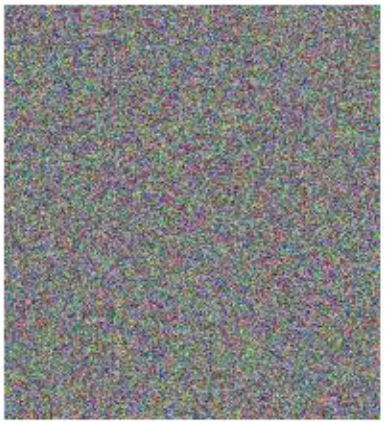
Blok Şifreler

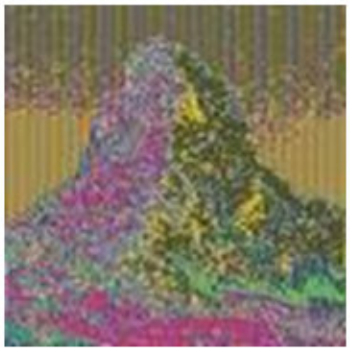
Orjinal resim

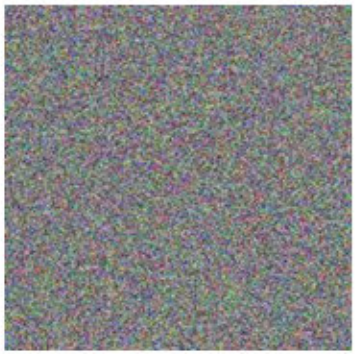
ECB modu



CTR modu







Blok Şifreler

Anahtarlar

- **Çok iyi** şekilde korunmalıdır
- Uygun uzunlukta (128, 192 ya da 256 bit) **rastgele** bitlerden oluşmalıdır
- Her anahtar sınırlı bir süreliğine kullanılmalıdır

İlgili Dersler

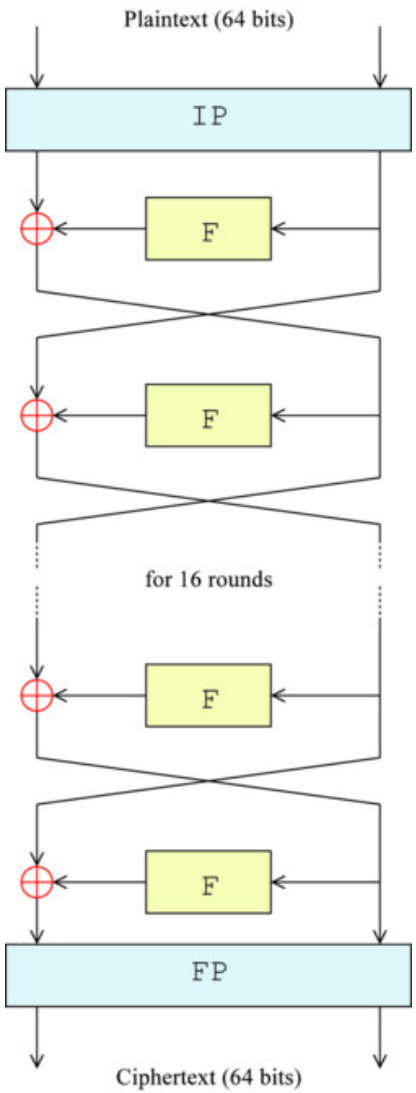
- **MATH 405** Combinatorics

Veri Şifreleme Standardı

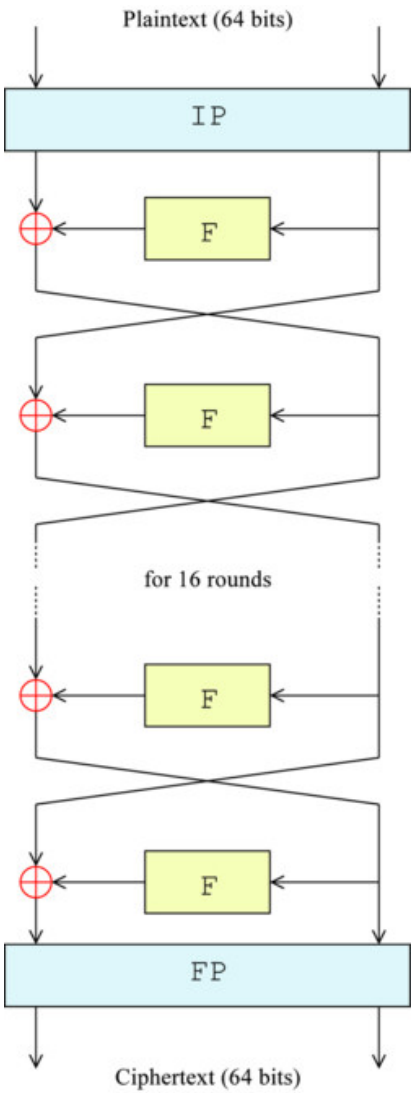
Veri Şifreleme Standardı (DES)

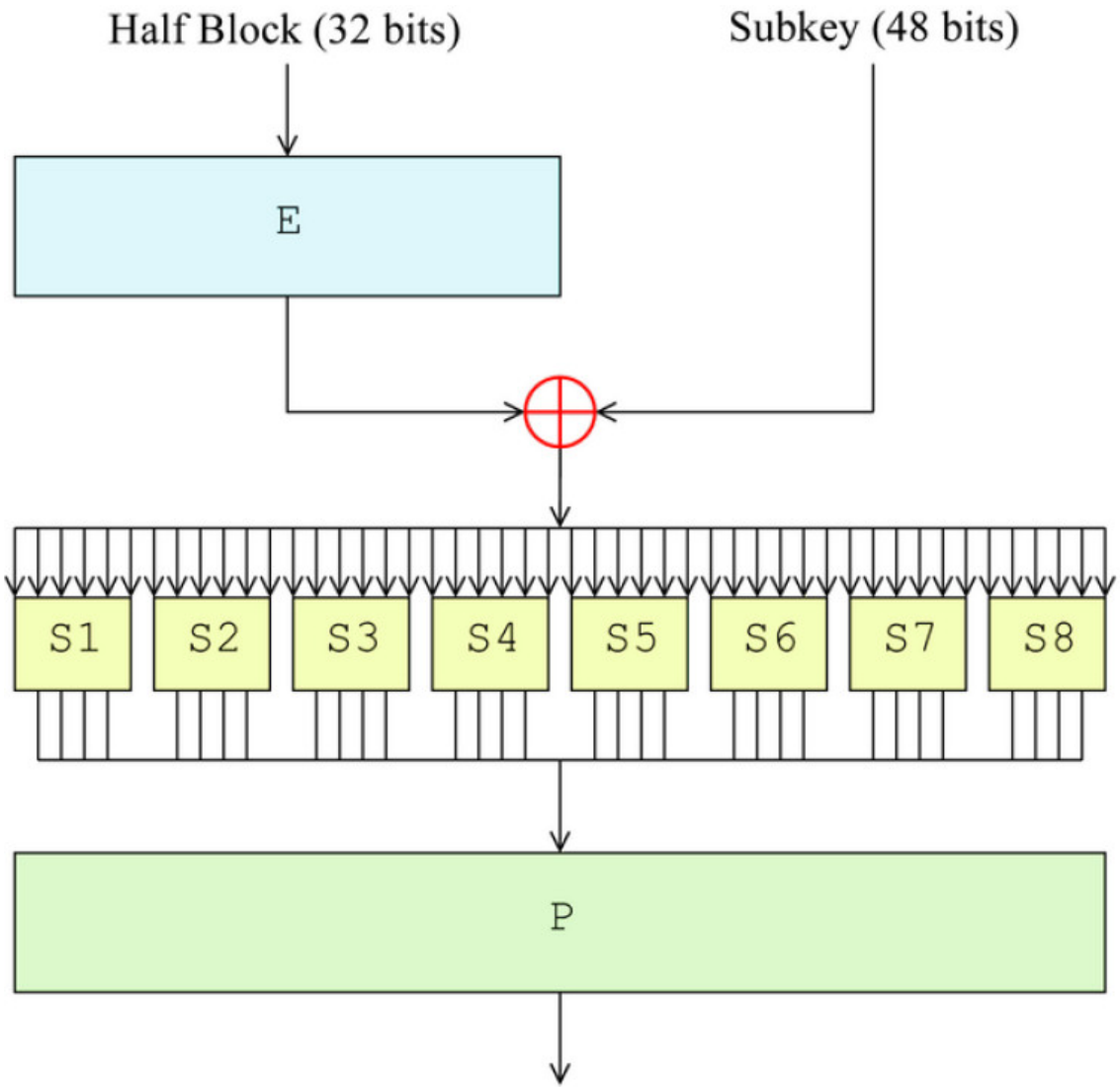
- 1970lerde IBM tarafından tasarlandı (NSA orjinal dizaynda değişiklikler yaptı)
  - Blok Uzunluğu: 64 bit
  - Anahtar Uzunluğu: 56 bit
  - Döngü Sayısı: 16
- Hala *kırılmadı*, ama anahtar uzunluğu 1990lardan sonra kısa kaldı

Data Encryption Standard



Data Encryption Standard





Gelişmiş Şifreleme Standardı

Gelişmiş Şifreleme Standardı (AES)

- NIST 2001'de standart olarak kabul etti (herkese açık dizayn yarışmasının kazananı)
  - Blok Boyutu: 128 bit
  - Anahtar Boyutu: 128, 192, 256 bit
  - Döngü sayısı: 10, 12, 14 (anahtar uzunluğuna göre)
- Bilinen hiçbir atak *uygulanabilir değil*

Genel Ataklar

Tam Arama / Kaba Kuvvet

- Her anahtarın doğru olup olmadığı tek tek denenir
- k bitlik anahtar için, 2^k tane şifreleme işlemi gerektirir

Genel Ataklar

Tam Arama / Kaba Kuvvet

- Her anahtarın doğru olup olmadığı tek tek denenir
- k bitlik anahtar için, 2^k tane şifreleme işlemi gerektirir

Ne kadar mümkün? (Numbers shamelessly stolen from Arjen K. Lenstra)

- 2^{128} sayısı, 3×10^{38}'dan daha büyüktür

Genel Ataklar

Tam Arama / Kaba Kuvvet

- Her anahtarın doğru olup olmadığı tek tek denenir
- k bitlik anahtar için, 2^k tane şifreleme işlemi gerektirir

Ne kadar mümkün? (Numbers shamelessly stolen from Arjen K. Lenstra)

- 2^{128} sayısı, 3×10^{38}'dan daha büyüktür
- Bilgisayarınızın 1000GHz'te çalıştığını varsayalım (normalde 4 GHz): 10^{12} **ops/sec**

Genel Ataklar

Tam Arama / Kaba Kuvvet

- Her anahtarın doğru olup olmadığı tek tek denenir
- k bitlik anahtar için, 2^k tane şifreleme işlemi gerektirir

Ne kadar mümkün? (Numbers shamelessly stolen from Arjen K. Lenstra)

- 2^{128} sayısı, 3×10^{38}'dan daha büyüktür
- Bilgisayarınızın 1000GHz'te çalıştığını varsayalım (normalde 4 GHz): 10^{12} **ops/sec**
- Bir yılda 3×10^7'dan daha az saniye vardır: 3×10^{19} **ops/year**

Genel Ataklar

Tam Arama / Kaba Kuvvet

- Her anahtarın doğru olup olmadığı tek tek denenir
- k bitlik anahtar için, 2^k tane şifreleme işlemi gerektirir

Ne kadar mümkün? (Numbers shamelessly stolen from Arjen K. Lenstra)

- 2^{128} sayısı, 3×10^{38}'dan daha büyüktür
- Bilgisayarınızın 1000GHz'te çalıştığını varsayalım (normalde 4 GHz): 10^{12} **ops/sec**
- Bir yılda 3×10^7'dan daha az saniye vardır: 3×10^{19} **ops/year**
- 10^{10} insan, hepsinin 1000 tane bilgisayarı olsun: 3×10^{32} **ops/year**

Genel Ataklar

Tam Arama / Kaba Kuvvet

- Her anahtarın doğru olup olmadığı tek tek denenir
- k bitlik anahtar için, 2^k tane şifreleme işlemi gerektirir

Ne kadar mümkün? (Numbers shamelessly stolen from Arjen K. Lenstra)

- 2^{128} sayısı, 3×10^{38}'dan daha büyüktür
- Bilgisayarınızın 1000GHz'te çalıştığını varsayalım (normalde 4 GHz): 10^{12} **ops/sec**
- Bir yılda 3×10^7'dan daha az saniye vardır: 3×10^{19} **ops/year**
- 10^{10} insan, hepsinin 1000 tane bilgisayarı olsun: 3×10^{32} **ops/year**
- Hala **bir milyon yıl** gerekli (eğer elektrik faturasını ödeyebilirseniz)

Genel Ataklar

İşlemci hızı, Anahtar uzunluğu kıyaslaması

- **Moore Kanunu (1965):** Entegre devrelerdeki transistör sayısı yaklaşık olarak her 2 yılda ikiye katlanır (aslında her 18 ayda).

Genel Ataklar

İşlemci hızı, Anahtar uzunluğu kıyaslaması

- **Moore Kanunu (1965):** Entegre devrelerdeki transistör sayısı yaklaşık olarak her 2 yılda ikiye katlanır (aslında her 18 ayda).
- 128-bit AES'ten 256-bit AES'e geçince
  - şifreleme işlemi yaklaşık 40% daha uzun sürer

Genel Ataklar

İşlemci hızı, Anahtar uzunluğu kıyaslaması

- **Moore Kanunu (1965):** Entegre devrelerdeki transistör sayısı yaklaşık olarak her 2 yılda ikiye katlanır (aslında her 18 ayda).
- 128-bit AES'ten 256-bit AES'e geçince
  - şifreleme işlemi yaklaşık 40% daha uzun sürer
  - ama atak yapanın çabası 2^{128} kat artacaktır
- Moore Kanunu atak yapanın değil, savunanın tarafındadır

Genel Ataklar

Tablo Atağı / Sözlük Atağı

- Tüm düz metinleri ve karşılık gelen şifreli metinleri ele geçirilir/önceden hesaplanır
- Tüm metinler bir tabloda tutulur

Genel Ataklar

Tablo Atağı / Sözlük Atağı

- Tüm düz metinleri ve karşılık gelen şifreli metinleri ele geçirilir/önceden hesaplanır
- Tüm metinler bir tabloda tutulur

Karmaşıklık

- Tam arama/Kaba kuvvet
  - Zaman karmaşıklığı: 2^k şifreleme işlemi
  - Veri karmaşıklığı: 0
  - Bellek karmaşıklığı: 0
- Tablo Atağı / Sözlük Atağı
  - Zaman karmaşıklığı: 0
  - Veri karmaşıklığı: 2^b blok
  - Bellek karmaşıklığı: 2^b blok

Atak Modelleri

Atak Modelleri

- **Sadece şifreli metin:** düşman sadece şifreli metinlere erişebilir.

Atak Modelleri

Atak Modelleri

- **Sadece şifreli metin:** düşman sadece şifreli metinlere erişebilir.
- **Bilinen düz metin:** düşman düz metin ve karşılık gelen şifreli metin çiftlerine erişebilir (örn: Lineer Kriptanaliz).

Atak Modelleri

Atak Modelleri

- **Sadece şifreli metin:** düşman sadece şifreli metinlere erişebilir.
- **Bilinen düz metin:** düşman düz metin ve karşılık gelen şifreli metin çiftlerine erişebilir (örn: Lineer Kriptanaliz).
- **Seçili düz metin:** düşman istediği tür düz metinleri seçip karşılık gelen şifreli metinlere erişebilir (örn: Diferansiyel Kriptanaliz).

Atak Modelleri

Atak Modelleri

- **Sadece şifreli metin:** düşman sadece şifreli metinlere erişebilir.
- **Bilinen düz metin:** düşman düz metin ve karşılık gelen şifreli metin çiftlerine erişebilir (örn: Lineer Kriptanaliz).
- **Seçili düz metin:** düşman istediği tür düz metinleri seçip karşılık gelen şifreli metinlere erişebilir (örn: Diferansiyel Kriptanaliz).
- **Seçili şifreli metin:** seçili düz metin saldırıları gibi ama bu sefer şifreli metinlerle.

Atak Modelleri

Atak Modelleri

- **Sadece şifreli metin:** düşman sadece şifreli metinlere erişebilir.
- **Bilinen düz metin:** düşman düz metin ve karşılık gelen şifreli metin çiftlerine erişebilir (örn: Lineer Kriptanaliz).
- **Seçili düz metin:** düşman istediği tür düz metinleri seçip karşılık gelen şifreli metinlere erişebilir (örn: Diferansiyel Kriptanaliz).
- **Seçili şifreli metin:** seçili düz metin saldırıları gibi ama bu sefer şifreli metinlerle.
- **Uyarlanabilir seçili düz metin:** düşman seçtiği düz metin ve karşılık gelen şifreli metinlere göre yeni düz metinler seçip karşılık gelen şifreli metinleri elde edebilir.

Atak Modelleri

Atak Modelleri

- **Sadece şifreli metin:** düşman sadece şifreli metinlere erişebilir.
- **Bilinen düz metin:** düşman düz metin ve karşılık gelen şifreli metin çiftlerine erişebilir (örn: Lineer Kriptanaliz).
- **Seçili düz metin:** düşman istediği tür düz metinleri seçip karşılık gelen şifreli metinlere erişebilir (örn: Diferansiyel Kriptanaliz).
- **Seçili şifreli metin:** seçili düz metin saldırıları gibi ama bu sefer şifreli metinlerle.
- **Uyarlanabilir seçili düz metin:** düşman seçtiği düz metin ve karşılık gelen şifreli metinlere göre yeni düz metinler seçip karşılık gelen şifreli metinleri elde edebilir.
- **Uyarlanabilir seçili düz metin ve şifreli metin:** . . . (örn: Bumerang Atak)

Diferansiyel Kriptanaliz

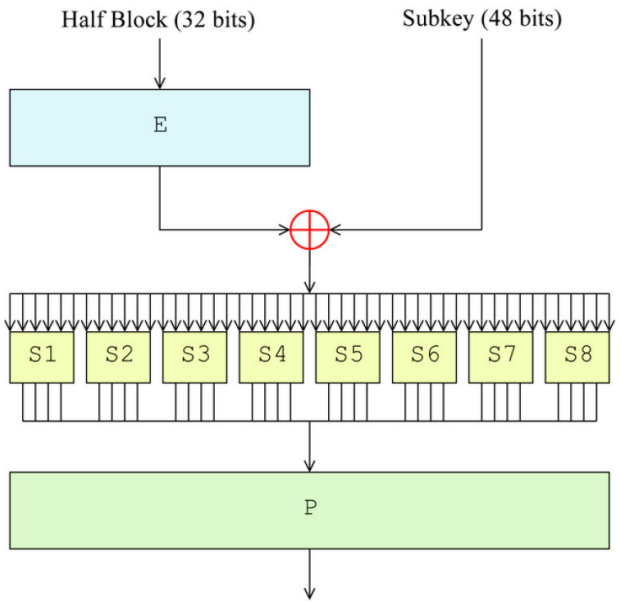
Diferansiyel Kriptanaliz

- E. Biham ve A. Shamir tarafından 1980lerin sonunda duyurulmuştur
- İlk bulunuşu İkinci Dünya Savaşı dönemi kadar eskidir *olabilir*
- Şifrede, düz metinlerdeki çok küçük değişikliklerin, yüksek olasılıkla belli şifreli metin farklarına gittiğini gösteren bir yol bulunur
- DES **garip** bir şekilde Diferansiyel Kriptanalize dayanıklıdır (16 döngüyü kırmak için 2^{49} adet seçili düz metine ihtiyaç vardır)

Diferansiyel Kriptanaliz

Diferansiyel Kriptanaliz

- E. Biham ve A. Shamir tarafından 1980lerin sonunda duyurulmuştur
- İlk bulunuşu İkinci Dünya Savaşı dönemi kadar eskidir *olabilir*
- Şifrede, düz metinlerdeki çok küçük değişikliklerin, yüksek olasılıkla belli şifreli metin farklarına gittiğini gösteren bir yol bulunur
- DES **garip** bir şekilde Diferansiyel Kriptanalize dayanıklıdır (16 döngüyü kırmak için 2^{49} adet seçili düz metine ihtiyaç vardır)



Diferansiyel Kriptanaliz

Example

Bir zar oyunu: Verilen bir zarın adil bir zar mı yoksa 6 gelme ihtimali $\frac{1}{3}$ olan hileli bir zar mı olduğunu bulmanız isteniyor. Ne yapardınız?

Diferansiyel Kriptanaliz

Example

Bir zar oyunu: Verilen bir zarın adil bir zar mı yoksa 6 gelme ihtimali $\frac{1}{3}$ olan hileli bir zar mı olduğunu bulmanız isteniyor. Ne yapardınız?

Veri/zaman karmaşılıklığı ve başarı olasılığı nasıl hesaplanır?

- Diferansiyel Kriptanaliz istatistiksel bir ataktır
- Eğer N tane seçili düz metinle atağı yaparsak atağın başarılı olasılığı ne olur?
- Atağın başarı olasılığının p'den fazla olması için ne kadar seçili düz metine ihtiyaç vardır?
- **Çözüm:** *Ali Aydın Selçuk* bu soruların çözümü için güzel formüller sunmuştur (2008), ayrıca Celine Blondeau (2009)

İlgili Dersler

- **MATH 301** Introduction to Probability Theory

Diferansiyel Kriptanaliz Türleri

Diferansiyel Kriptanaliz Türleri

- Kesikli Diferansiyel Kriptanaliz (Knudsen 1994)
- Yüksek Dereceden Diferansiyel Kriptanaliz (Knudsen 1994)
- *İmkansız Diferansiyel Kriptanaliz (Biham-Biryukov-Shamir 1998)*
- Bumerang Attack (Wagner 1999)
- Olası Olmayan Diferansiyel Kriptanaliz (Tezcan 2010)
- Çoklu Diferansiyel Kriptanaliz (Blondeau-Gerard 2011)

Diferansiyel Kriptanaliz Türleri

Diferansiyel Kriptanaliz Türleri

- Kesikli Diferansiyel Kriptanaliz (Knudsen 1994)
- Yüksek Dereceden Diferansiyel Kriptanaliz (Knudsen 1994)
- *İmkansız Diferansiyel Kriptanaliz (Biham-Biryukov-Shamir 1998)*
- Bumerang Attack (Wagner 1999)
- Olası Olmayan Diferansiyel Kriptanaliz (Tezcan 2010)
- Çoklu Diferansiyel Kriptanaliz (Blondeau-Gerard 2011)

İmkansız Diferansiyel Kriptanaliz

- **İmkansız Diferansiyel:** Düz metinlerdeki belli bir değişikliğin, bir kaç döngü sonrasında asla belli bir şifreli metin farkına gitmediği diferansiyel yollardır
- İmkansız olaylar daha önceden de şifrelerin kırılmasında kullanılmıştır

İmkansız Ataklar

Example

- Enigma'nın 2. Dünya Savaşı sırasında kriptanalizi
- **İmkansız olay:** Bir harf asla kendisine şifrelenmez

İmkansız Ataklar

Example

- Enigma'nın 2. Dünya Savaşı sırasında kriptanalizi
- **İmkansız olay:** Bir harf asla kendisine şifrelenmez
- **Varsayım:** Düz metinin 'Keine besonderen Ereignisse' kelimesini içermesi (anlamı 'rapor edecek bir şey olmadı')

İmkansız Ataklar

Example

- Enigma'nın 2. Dünya Savaşı sırasında kriptanalizi
- **İmkansız olay:** Bir harf asla kendisine şifrelenmez
- **Varsayım:** Düz metinin 'Keine besonderen Ereignisse' kelimesini içermesi (anlamı 'rapor edecek bir şey olmadı')

Ciphertext	O	H	J	Y	P	D	O	M	Q	N	J	C	O	S	G	A	W	H	L	E	I	H	Y	S	O	P	J	S	M	N	U
Position 1			K	E	I	N	E	B	E	S	O	N	D	E	R	E	N	E	R	E	I	G	N	I	S	S	E				
Position 2				K	E	I	N	E	B	E	S	O	N	D	E	R	E	N	E	R	E	I	G	N	I	S	S	E				
Position 3					K	E	I	N	E	B	E	S	O	N	D	E	R	E	N	E	R	E	I	G	N	I	S	S	E			

Teşekkürler

Sorular?