Kriptoloji

Halil Kemal TAŞKIN

Orta Doğu Teknik Üniversitesi
Uygulamalı Matematik Enstitüsü
Kriptografi Bölümü

İçerik

XOR: Exclusive OR ($\oplus$)

- $\{1,0\}^*$ uzayında tanımlıdır.
- Mod 2'de toplama işlemidir.

$$\boxed{\begin{array}{llll} 0 & \oplus & 0 & = 0 \\ 0 & \oplus & 1 & = 1 \\ 1 & \oplus & 0 & = 1 \\ 1 & \oplus & 1 & = 0 \end{array}}$$

$$p \oplus k = c \Leftrightarrow p = k \oplus c$$

$$\begin{array}{cccccccccc} & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ \oplus & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ \hline & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 \end{array}$$

Taban Aritmetiği

- İkilik Taban (Binary): $0, 1$
- Onluk Taban (Decimal): $0, 1, 2, 3, 4, 5, 6, 7, 8, 9$
- Onaltılık Taban (Hexadecimal):
  $0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A(10), B(11), C(12), D(13), E(14), F(15)$

Örnek

$$(AB)_{16} = (171)_{10} = (10101011)_2$$

$$0xAB = ABh = 171 = 10101011b$$

- $(AB)_{16} = 16^1 * 10 + 16^0 * 11 = 160 + 11 = 171$
- $171 = 2^7 + 2^5 + 2^3 + 2^1 + 2^0$

Bilgi Teorisi (Information Theory)

- Kodlama Teorisi (Coding Theory)

  Encoding - Decoding

  $$|\ \text{Girdi}\ | < |\ \text{Çıktı}\ |$$

- Kriptografi (Cryptography)

  Encryption - Decryption

  $$|\ \text{Girdi}\ | = |\ \text{Çıktı}\ |$$

- Sıkıştırma (Compression)

  Compression - Decompression

  $$|\ \text{Girdi}\ | > |\ \text{Çıktı}\ |$$

Kriptoloji Nedir?

- Yunancada:

  kripto: Gizli

  grafi: Yazılmış olan
- Kriptografi bilimin çalışma disiplinine **Kriptoloji** denir.
- Temel Amaç: İki kişi mesajlaşırken üçüncü kişi mesajları okuyamasın.

Temel Kavramlar

Kerckhoffs's 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

Information Theory (Bilgi Teorisi)'nin kurucusu olarak kabul edilir.

Meşhur sözü: "The enemy knows the system"

Temel Kavramlar

Kriptosistem Nedir?

- Şifrelemek istediğimiz metin: Açık metin (plaintext)
- Şifrelenmiş metin: Şifreli metin (ciphertext)
- Şifreleme parametresi: Anahtar (key)
- **Kriptosistem**, Anahtar kullanarak açık metinleri şifreli hale çeviren ve şifreli metinleri de açık metine geri döndüren algoritmalardır.
- Şifreli metin rastgele görünmelidir.

Temel Kavramlar

Şifreleme İşlemi

Şifre Çözme İşlemi

Klasik Şifreleme Sistemleri

- Sezar Şifreleme
- Vigenere Şifreleme
- Afin Şifreleme
- Vernam Şifreleme

Harf - Sayı Dönüşümü

Alfabeyi Sayılarla İfade Etme

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Harfleri toplama ve İşlemler

- Harfleri Toplama İşlemi

  $T + O = ?$

  $19 + 14 = 33 \bmod 26 = 7 =$ H
- Harflerin sayılarla çarpımı ve toplamı

  $3 * T + 4 = ?$

  $3 * 19 + 4 = 61 \bmod 26 = 9 =$J

Sezar Şifreleme

- Jül Sezar tarafından M.Ö. 50 yıllarında kullandıldığı için bu isim verilmiştir.
- Alfabe üzerinde çalışır.
- Frekans analizi ile kırılabilmektedir.
- **Şifrele**$(P) = P + 3 \bmod 26 = C$
- **Çöz**$(C) = C - 3 \bmod 26 = P$

Örnekler

- ABCDEFGHIJKLMNOPQRSTUVWXYZ
  DEFGHIJKLMNOPQRSTUVWXYZABC
- M E R H A B A D U N Y A
  P H U K D E D G X Q B D

Afin Şifreleme

- Sezar Şifrelemenin gelişmiş halidir.
- Anahtar $K = (a, b)$ sayılarından oluşur öyleki $0 \leq a, b < 26, obeb(a, 26) = 1$
- Frekans analizi ile kırılabilmektedir.
- **Şifrele**$(P_i, K) = (a * P_i + b) \bmod 26 = C_i$
- **Çöz**$(C_i, K) = a^{-1}(C_i - b) \bmod 26 = P_i$

Örnek

Harf: H
Anahtar: $K = (3, 4) \implies a = 3, b = 4$
Şifrele: $P_1 = H = 7 \rightarrow C_1 = 3 * 7 + 4 = 25 \bmod 26 = 25 =$Z
Çöz: $C_1 = Z = 25 \rightarrow P_1 = 3^{-1}(25 - 4) = 9 * 21 \bmod = 7 =$ H

Vigenere Şifreleme

- 1553 yılında Giovan Battista Bellaso tarafından bulunmuştur.
- Ancak benzer bir çalışma yapan Blaise de Vigenère'nin ismi ile anılmaktadır.
- Otomatik Anahtarlı Sistemin temelidir.
- Şifreleme için tekrar eden anahtar sözcük kullanılır.
- Kasiski analizi adı verilen istatistiksel yöntem ile kırılabilmektedir.
- **Şifrele**$(P_i, K_i) = P_i + K_i \bmod 26 = C_i$
- **Çöz**$(C_i, K_i) = C_i - K_i \bmod 26 = P_i$

Örnek

Metin	H	A	L	I	L	K	E	M	A	L
Şifre	K	R	I	P	T	O	K	R	I	P
Çıktı	R	R	T	X	E	Y	O	D	I	A

Vernam Şifreleme

- 1919 yılında Gilbert Sandford Vernam bulunmuştur.
- Tek Kullanımlık Şerit (One-time Pad) olarak da adlandırılır.
- Vigenere şifrelemesi ile aynı şekilde çalışır. Ancak tekrar eden şifre sözcüğü yerine tamamen rastgele harfler kullanılmaktadır.
- Dolayısıyla, şifrenin boyutu da mesaj boyutu kadar olduğu için kullanışlı değildir.
- Aynı şifre iki kez kullanılamaz.
- İkili (binary) veriler üzerinde *XOR* işlemi ile uygulanır.
- Koşulsuz olarak güvenli olan tek şifreleme sistemidir.
- Günümüzde en üst seviye gizlilik gerektiren mesajlarda kullanılmaktadır.
- **Şifrele**$(P_i, K_i) = P_i + K_i \bmod 26 = C_i$
- **Çöz**$(C_i, K_i) = C_i - K_i \bmod 26 = P_i$

Modern Kriptoloji

- Bilgisayarların icadı ile ikili sistemler kullanılmaya başlanmıştır.
- Dolayısıyla, veri depolama biçimi ikili hale gelmiştir.
- Varolan klasik kriptosistemler alfabeler üzerinde çalıştığı için bu yeni sistemlere uygulaması zor ve güvenli değiller.
- Şifrelemeden fazlası gereklidir.

Amaçlar

Gizlilik

Veri istenmeyen kişiler tarafından anlaşılamamalıdır.

Bütünlük

Verinin iletilirken hiç değiştirilmemiş olduğu doğrulanmalıdır.

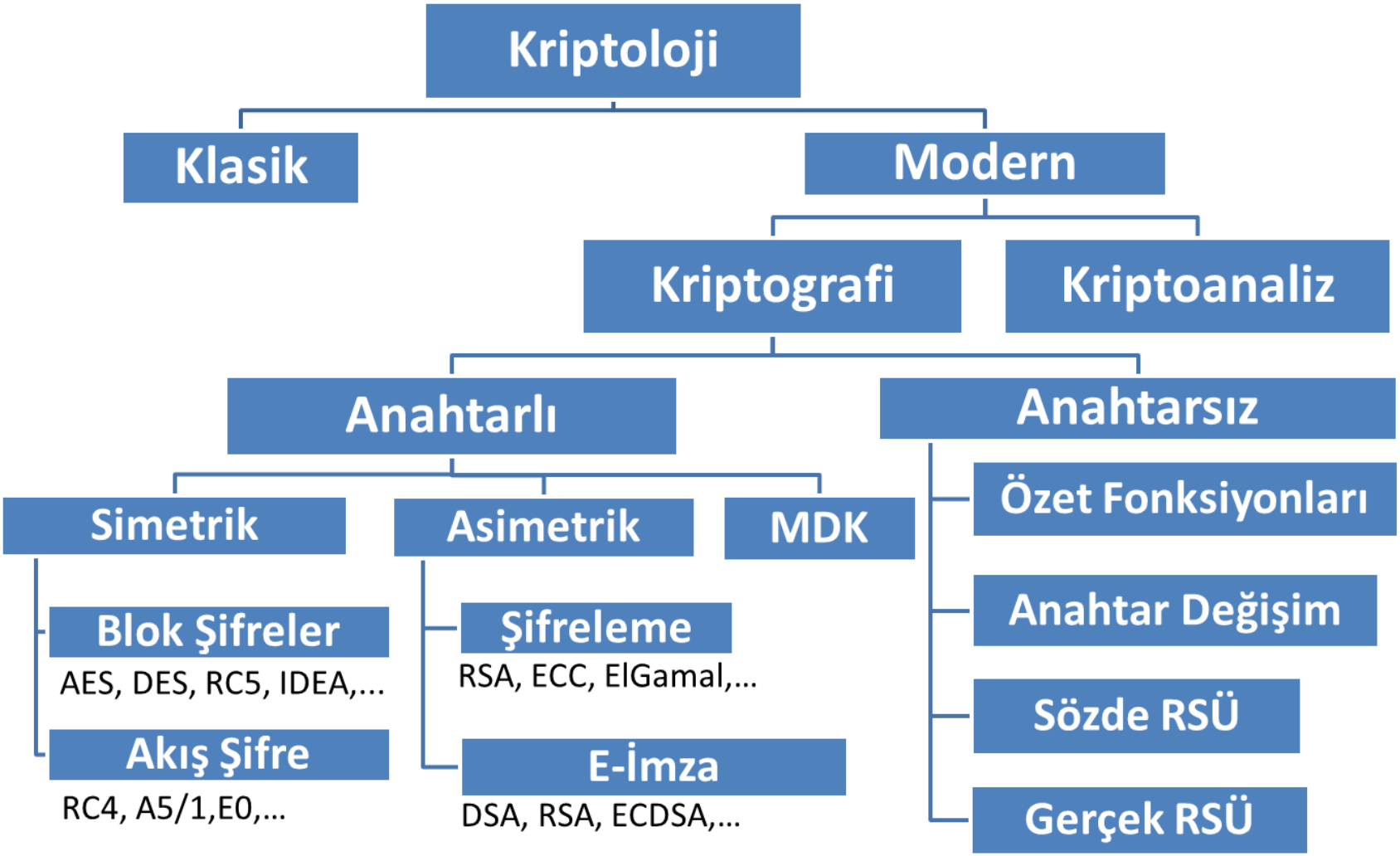
Kimlik Denetimi

Gönderici ve alıcı birbirlerinin kimliklerini doğrulamalıdır.

İnkar edememe

Gönderici veriyi gönderdiğini inkar edememelidir.

Kriptoloji


Kriptoloji
Klasik
Modern
Kriptografi
Kriptoanaliz
Anahtarlı
Anahtarsız
Simetrik
Asimetrik
MDK
Özet Fonksiyonları
Anahtar Değişim
Sözde RSÜ
Gerçek RSÜ
Blok Şifreler
AES, DES, RC5, IDEA,...
Akış Şifre
RC4, A5/1,E0,...
Şifreleme
RSA, ECC, ElGamal,...
E-İmza
DSA, RSA, ECDSA,...

Kriptografi

Simetrik Anahtarlı Kriptografi

Veriyi şifreleme ve çözme için kullanılan anahtarlar aynı ya da ilişkili olmalıdır.
Bir anahtardan diğeri kolaylıkla elde edilebilmelidir.

Asimetrik (Açık) Anahtarlı Kriptografi

Veriyi şifreleme ve çözme için farklı anahtarlar kullanılır.
Şifreleme anahtarı herkesin ulaşabileceği şekilde açıktır.
Ancak, çözme anahtarını elde etmek zordur.

Hash (Özet) Fonskiyonları

Veriyi belirli uzunlukta bir bit dizisine, özet değerine, dönüştürür.
Verideki ufak bir değişiklik özet değerini değiştirmelidir.

Simetrik Anahtarlı Kriptografi

Blok Şifreler (Block Ciphers)

Veriyi belirli uzunluktaki parçalara bölerek şifreleme yapan sistemlerdir.

Akan Şifreler (Stream Ciphers)

Veriyi bit bit şifreleyen sistemlerdir. Vernam Şifrelemesinin uygulanabilir halidir.

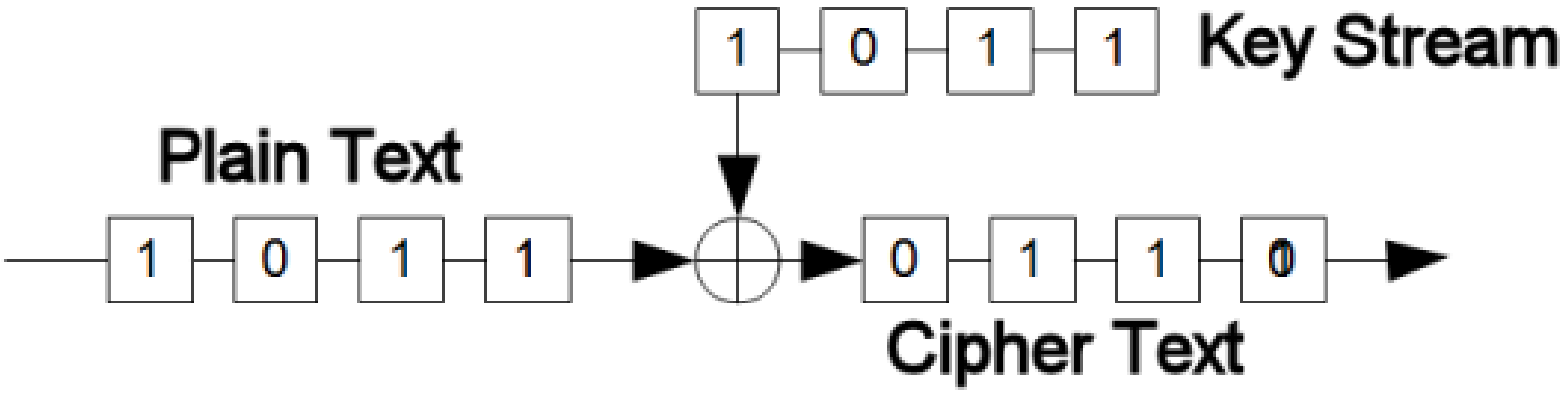
Akan Şifreler

- Vernam şifresindeki gibi mesaj ile aynı boyda bir anahtar kullanmak yerine daha kısa bir anahtar kullanılır. (128-bit vb.)
- Bu kısa anahtar kullanılarak uzun bir yalancı (sözde) rassal anahtar dizisi oluşturulur.
- Bilgi bu anahtar dizisi ile XOR işlemine tabi tutularak şifreleme yapılır.
- XOR işleminin tanımı gereği çözme işlemi de şifreleme işleminin aynısıdır.
- Ayrıca, sözde rassal sayı üreteçleri olarak da bilinir.
- **Sözde Rassallık**: İstatistiksel olarak gerçek sayı üreteçleri ile aynı özelliklerde ancak ilk değerlerden tekrar üretilebilme ve periyodik olma.

Akan Şifreler

Golomb'un Rassallık Postülaları

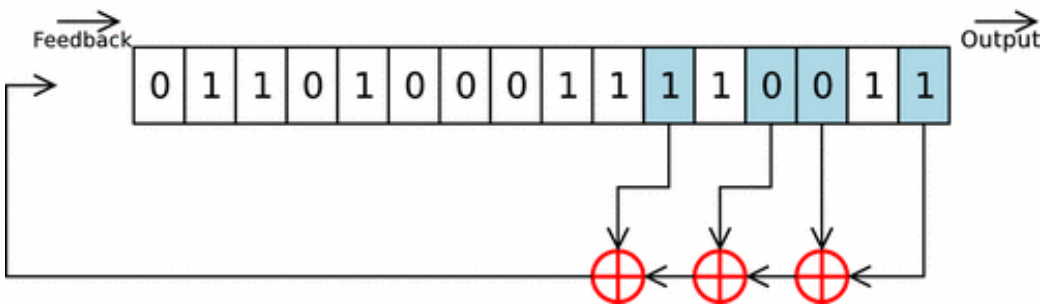
- 1'lerin sayısı ile 0'ların sayısının farkı en çok 1 olmalı.
- Dizi uzunluğu 2^m olmak üzere, uzunluğu m'den küçük 1..1 ve 0..0'ların sayısı dengeli olmalı.
- Dizinin otokorelasyonu 2 değerli olmalı.



Akan Şifreler

Doğrusal Geribeslemeli Kaydırmalı Yazdırgaç (LFSR)

- Akan şifreleme sistemi tasarımının temelinde yer alır.
- n-bit'lik bir LFSR ilkel bir polinom ile $2^n - 1$ uzunluğunda bir dizi üretebilir.
- Matematiksel olarak çok iyi analiz edilmişlerdir ancak tek başlarına kullanımı doğrusal bir yapıda olmaları nedeniyle güvenli değildir.
- Akış şifre tasarımında doğrusal olmayan yapılarla birlikte kullanılırlar.



Akan Şifreler

- **Yaygın olarak kullanılan Akan Şifre Algoritmaları**
  RC4: WEP Kablosuz ağ şifrelemesinde ve SSL/TLS protokolünde kullanılmaktadır. LFSR kullanmaz!
  A5/1: GSM iletişiminin şifrelenmesi için kullanılmaktadır.
  E0: Bluetooth iletişiminin şifrelenmesi için kullanılmaktadır.
- A5/1 ve E0 algoritmaları için bilinen ataklar mevcuttur. RC4 bazı şartlarla güvenlidir.

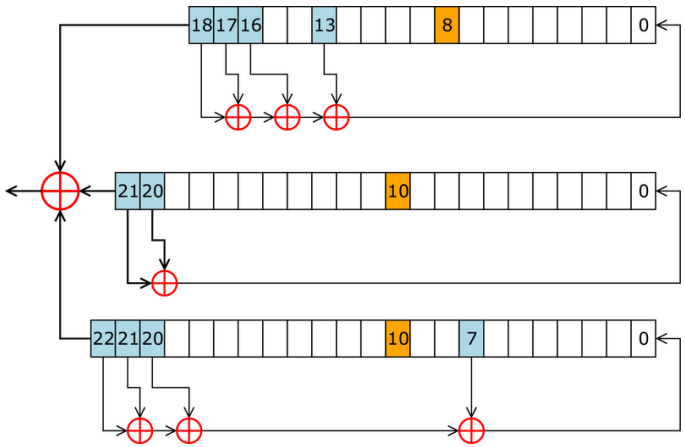


Figure: A5/1 GSM Şifreleme Algoritması

ECRYPT Akan Şifre Projesi

- 2004 yılında, akan şifre kullanımını desteklemek adına eSTREAM projesi başlatıldı.
- Proje 2008 yılında sonuçlandı. İki profil açıklandı.
- Yazılım ve donanım uygulamaları için algoritmalar önerildi.
- 2012 yılında son inceleme raporu yayınlandı. Algoritma analizleri halen devam ediyor.

Profil 1 (Yazılım) $\geq 128-$bit Anahtar	**Profil 2 (Donanım)** $\geq 80-$bit Anahtar
HC-128	Grain v1
Rabbit	MICKEY 2.0
Salsa20/12	Trivium
SOSEMANUK	

Table: eStream Profilindeki Algoritmalar

Blok Şifreler

- Mesajı belirli uzunlukta parçalara böl ve her parçayı ayrı ayrı şifrele.
- Mesaj blok uzunluğu çoğunlukla 64-bit ya da 128-bit seçilir.
- Anahtar uzunlukları genelde 128-bit ya da 256-bit seçilir.
- Anahtar seçimi rastgele olmalıdır.
- Günümüzde daha sık kullanılmaktadır.

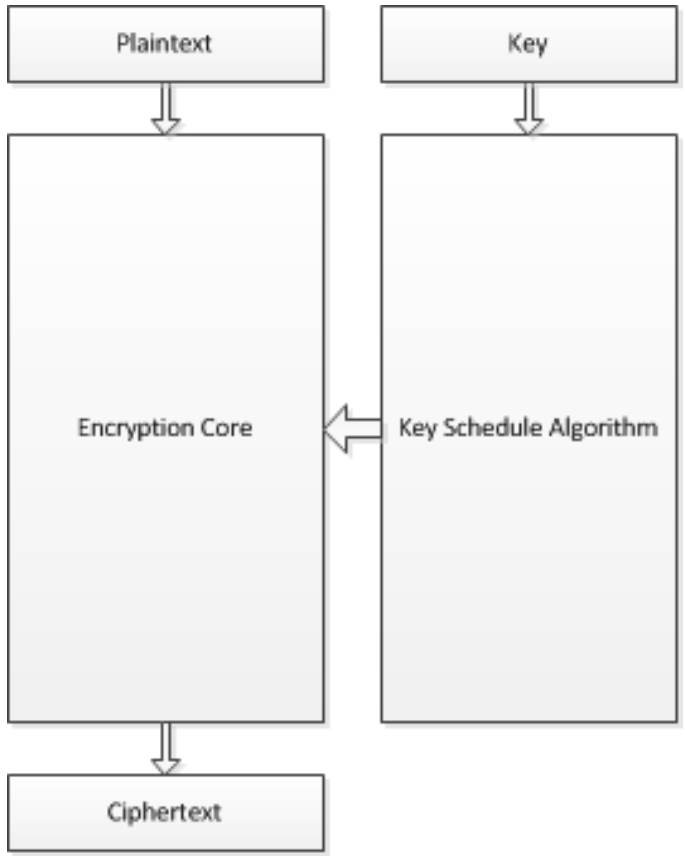


Figure: Blok Şifre Yapısı

Tasarım Kriterleri

Yayılma (Diffusion)

- Giren her mesaj bitinin şifreli metnin her bir biti üzerinde etki etmesine denir.
- Mesaj bloğundaki tüm bitlerin yayılmasını sağlar.
- Doğrusal (Linear) yapılarla sağlanır.

Karıştırma (Confusion)

- Şifreli bir metinden ona karşılık gelen mesaj arasında doğrusal bir bağlatı olmamalıdır.
- Doğrusal olmayan (Non-linear) yapılarla sağlanır.
- Kriptografik güvenliği sağlayan yapılardır.
- Genel olarak Değişim Kutu'ları (S-Box, Substitution Box) denen yapılar ile sağlanır.

Tekrarlı Blok Şifreler

- Günümüz blok şifrelerinin tasarım modelidir.
- Basit bir çevrim (round) fonksiyonu tasarlanır.
- Bu çevrim belirli sayıda tekrar edilir.
- Şifreleme anahtarından farklı alt anahtarlar üretilerek her çevrimde farklı anahatarlar kullanılır.

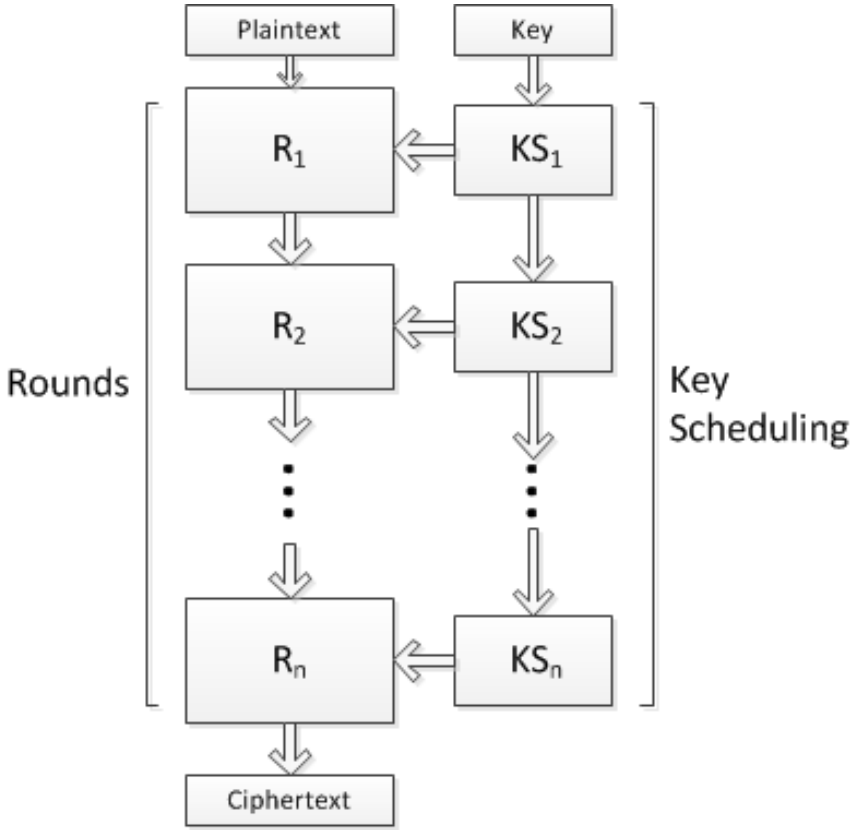


Figure: Tekrarlı Blok Şifre Tasarımı

SP-Network (SPN) Blok Şifreler

- Yayılma (P) ve Karıştırma (S) için birer fonksiyon tasarlanır.
- Yayılma ve karıştırma fonksiyonlarına alt anahtar eklemesi yapılarak çevrim fonksiyonu oluşturulur.
- Bu çevrim belirli sayıda tekrar edilir.
- Şifreleme anahtarından farklı alt anahtarlar üretilerek her çevrimde farklı anahatarlar kullanılır.

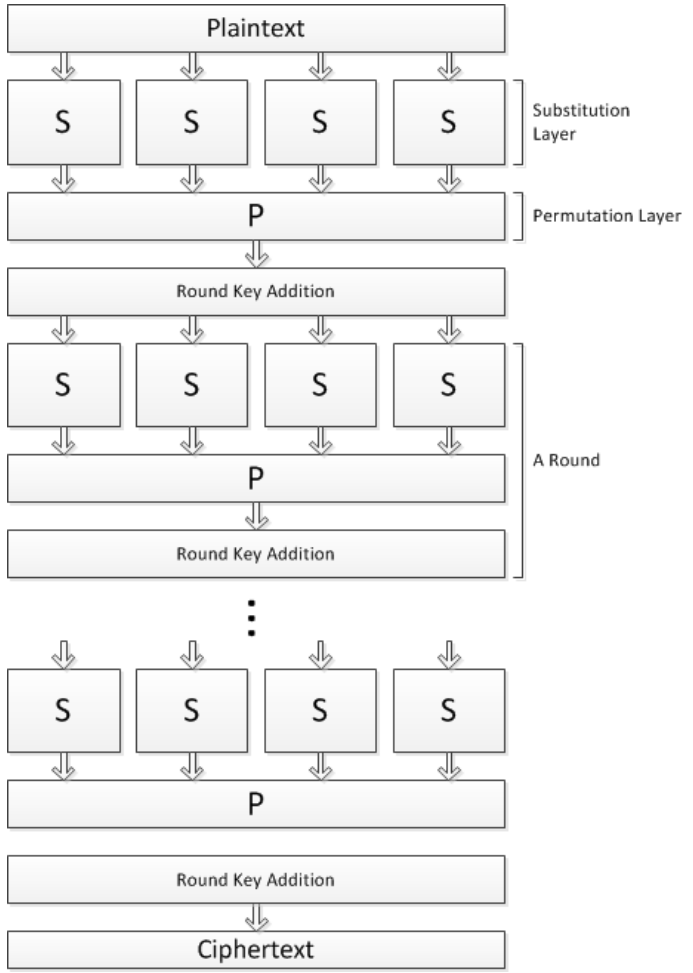


Figure: SPN Blok Şifre Tasarımı

Feistel Blok Şifreler

- Mesaj bloğu iki parçaya bölünür.
- Her çevrimde mesaj bloğunun yarısı işleme sokulur.
- Çevrim fonksiyonun (f) tersinir olması gerekmez.
- Feistel yapısı yayılma özelliğini sağlar.
- Karıştırma özelliği çevrim fonksiyonunun içinde sağlanır.
- Çözme için anahtarlar ters sırada kullanılır.

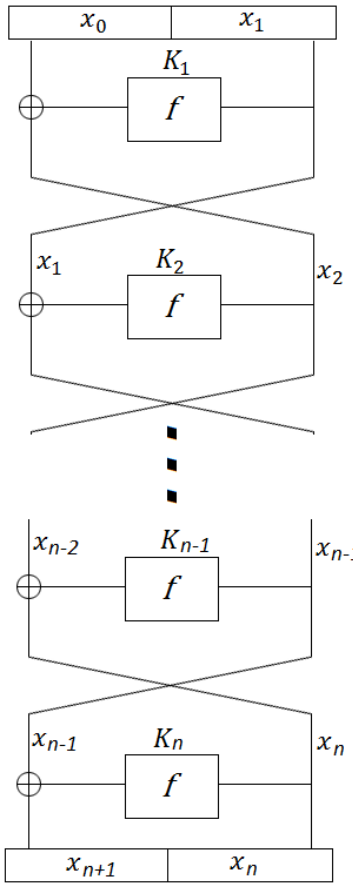


Figure: Feistel Blok Şifre Tasarımı

Blok Şifre Çalışma Kipleri

- Bir blok şifrenin tek bir anahtar altında güvenli bir şekilde tekrarlı kullanımını sağlar.
- Çeşitli kipler tarafından İlklendirme vektörü (IV) denilen ve şifrelemeyi rassallaştırmayı sağlayan değerler kullanılır.
- Mesajın son bloğu blok uzunluğuna uyacak şekilde uygun bir tamamlama şeması (padding) ile uzatılmalıdır.
- Sistemlerin ve protokollerin güvenliği için kullanılan çalışma kipinin doğru seçilmesi önemlidir.

Elektronik Kod Defteri (ECB) Kipi

- **ECB**: Electronic Code Book
- En basit çalışma kipidir.
- Aynı anahartarla kullanıldığında aynı mesaj bloğu aynı şifreli mesajı verir.
- Güvenli kabul edilmemektedir.

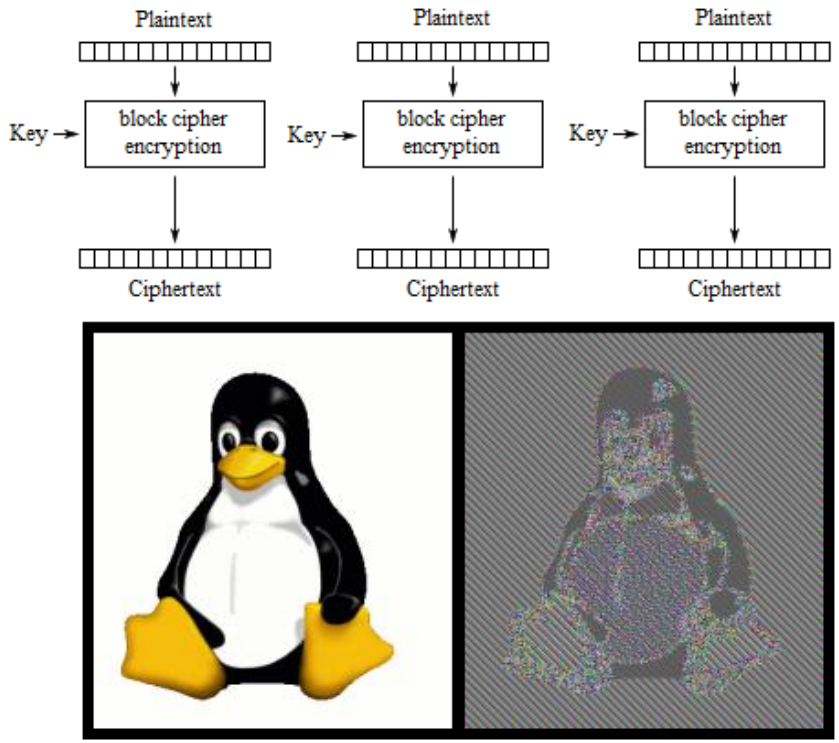


Figure: ECB Çalışma Kipi ve Örnek Şifreleme

Şifre Bloğu Zincirleme (CBC) Kipi

- **CBC**: Cipher Block Chaining
- İlk mesaj bloğuna IV eklenerek rassallık sağlanır.
- Her mesaj bloğuna bir önceki şifreli mesaj bloğu eklenerek (XOR) işlem yapılır.

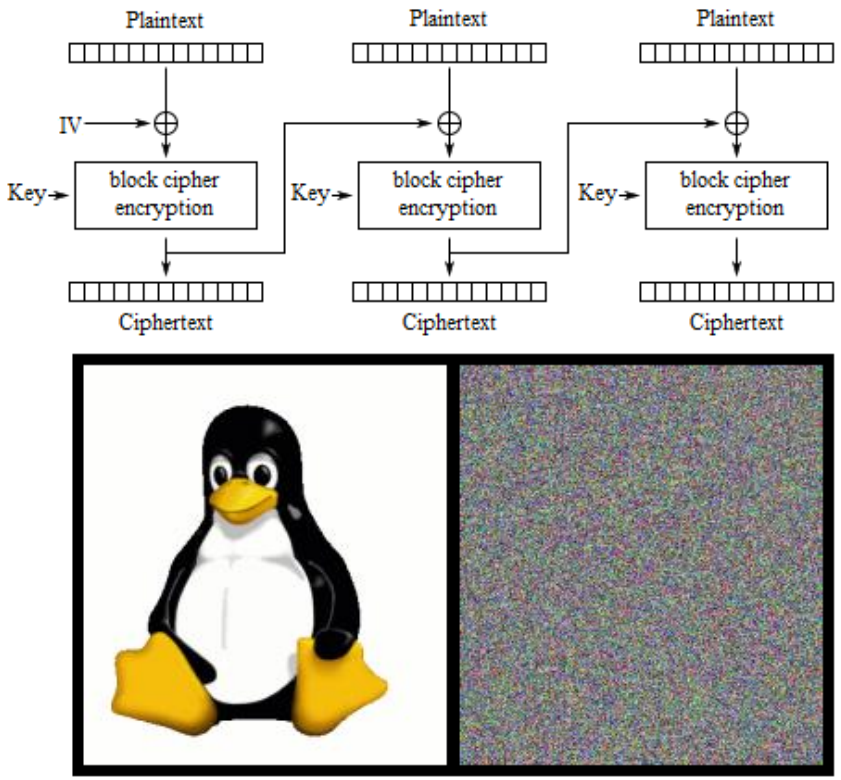


Figure: CBC Çalışma Kipi ve Örnek Şifreleme

Diğer Çalışma Kipleri

- **CTR**: Counter Mode

  Blok şifreleri akan şifre modunda kullanmayı sağlar.
- **OFB**: Output Feedback Mode
- **CFB**: Cipher Feedback Mode
- **PCBC**: Propagating Cipher Block Chaining Mode
- **AES-GCM**: AES Galois Counter Mode
- **XTS**: XEX-based Tweaked-codebook Mode with Ciphertext Stealing Mode

  XTS-AES disk şifrelemesinde standart olmuştur.

Data Encryption Standart (DES)

- 1972 yılında NIST'ın isteği üzerinde IBM tarafından tasarlanmıştır.
- IBM'in tasarladığı Lucifer blok şifrenin geliştirilmiş halidir.
- 1975 yılında açıklanmıştır.
- IBM anahtar boyutunu 64-bit olarak tasarlamıştır, fakat NIST 48-bit'e düşürülmesini istemiştir.
- 56-bit anahtar boyutunda anlaşılmıştır.
- Standart (25 Ekim 1999): FIPS 46-3

Data Encryption Standart (DES)

- **Mesaj Bloğu**: 64-bit
  Anahtar: 56-bit
- Yapı: 16 Çevrim Feistel
- Çevrim Fonksiyonu (F): 8 tane $6x4$ S-Kutusu
- Günümüzde 3DES kullanılmaktadır.
- Uygulanmış bir çok atak mevcuttur.
- Özel donanımlarla (COPACOBANA, RIVYERA) ≤ 1 günde kırılabilmektedir.

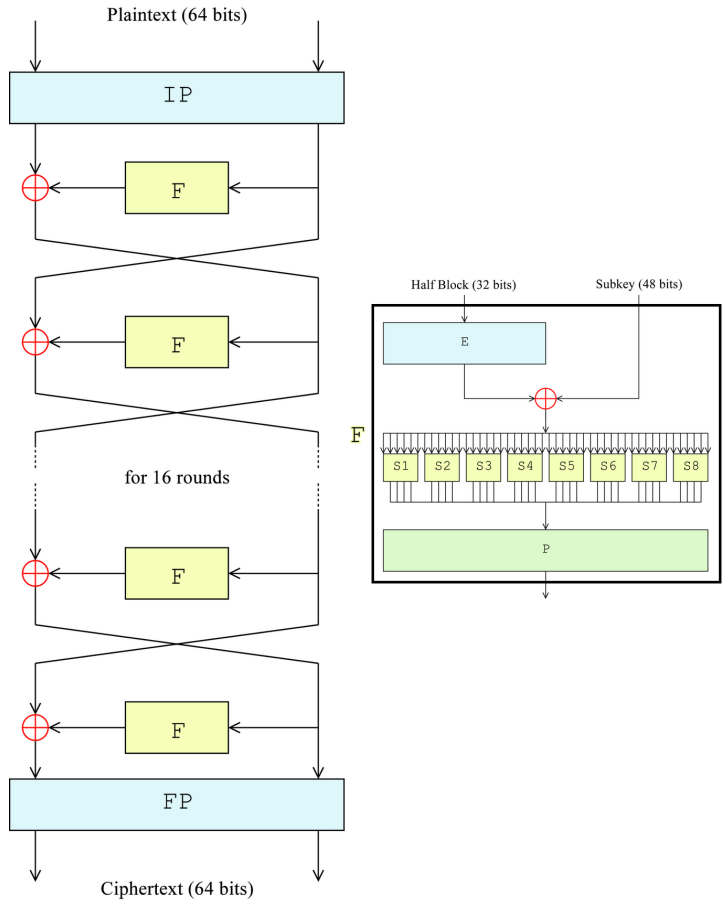


Figure: DES Feistel Yapısı ve F Çevrim Fonksiyonu

Advanced Encryption Standart (AES)

- NIST, 2 Ocak 1997 tarihinde DES'in yerine geçmesi için yeni bir blok şifre tasarlama projesi başlattı.
- Bunun için duyurular yapıldı. Dünyanın çeşitli ülkelerinden 15 farklı blok şifre tasarımı gönderildi.
- 1998 ve 1999'da yapılan AES konferanslarında bu sistemlere yapılan ataklar yayınlandı.
- Bunun sonucunda sadece 5 algoritma finale kaldı.
- 2 Ekim 2000 tarihinde Rijndeal AES olarak seçilmiştir.
- 26 Kasım 2001 tarihinde de FIPS 197 olarak standartlaşmıştır.

Advanced Encryption Standart (AES)

- Tüm adayların mesaj bloğu boyutu: 128-bit
- Tüm adayların anahtar boyutu: 128, 192, 256-bit
- Ayrıca, Rijndael'da 160-bit ve 224-bit mesaj bloğu ve anahtar boyutu desteği mevcut.

Algoritma	**Oy Sayısı**	**Çevrim**	**Yapı**	**Hız**	**Güvenlik**
Rijndael	86+ / 10-	10, 12, 14	SPN	2.	2.
Serpent	59+ / 7-	32	SPN	5.	1.
Twofish	31+ / 21-	16	Feistel	1.	5.
RC6	23+ / 37-	20	Feistel	3.	4.
MARS	13+ / 84-	32	Feistel	4.	3.

Table: AES Adayları Karşılaştırma Tablosu

Advanced Encryption Standart (AES)

- **Mesaj Bloğu**: 128-bit
  Anahtar: 128, 192, 256-bit
- Yapı: 10, 12, 14 Çevrim SPN
- 1 tane 8x8 S-Kutusu
- Günümüzde kullanılan en popüler şifreleme sistemidir.
- Teoride kırılmış pratikte sağlamdır.
- 2020 yılına kadar kullanılması beklenmektedir.

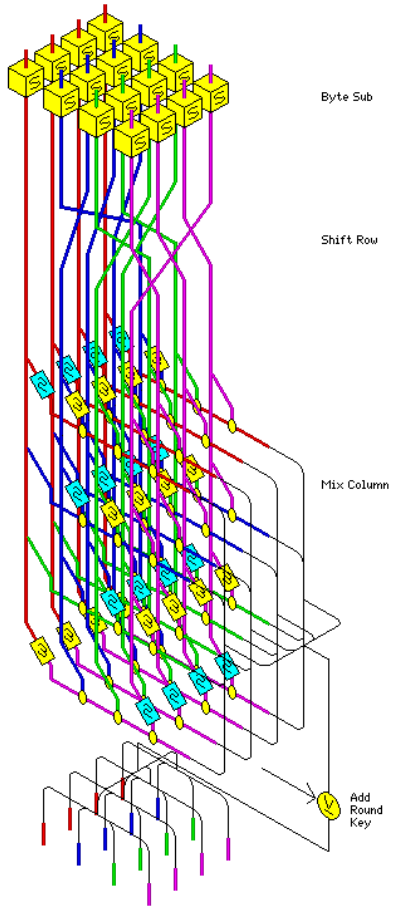


Figure: Bir AES Çevrimi

CAESAR

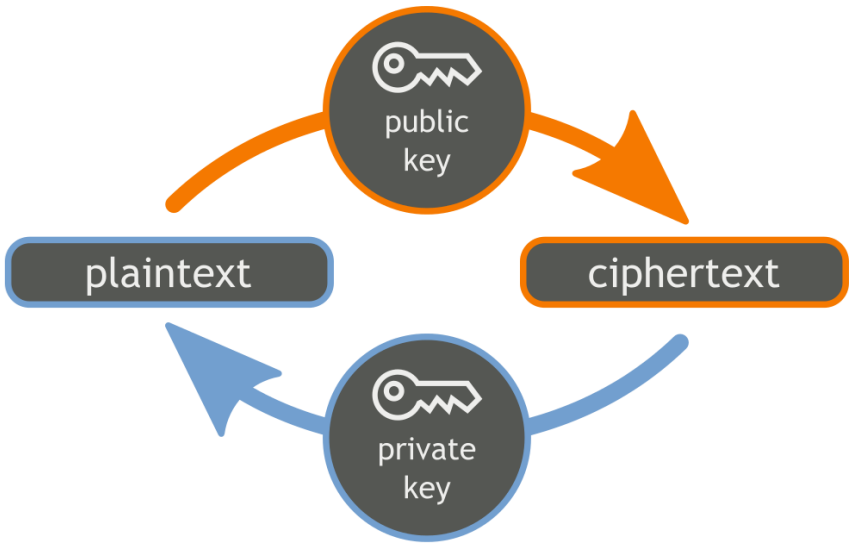
- Competition for Authenticated Encryption: Security, Applicability, and Robustness
- Blok Şifre ve Mesaj Doğrulama Kodu tasarımı
- Ocak 2013'de duyuruldu. Son başvuru: Şubat 2014
- AES, SHA3 ve eSTREAM'in devamı olarak görülüyor.
- NIST düzenlemiyor ama destek veriyor.
- Final: Aralık 2017.
- Site: `http://competitions.cr.yp.to/`

Asimetrik (Açık) Anahtarlı Kriptografi

- Public Key Cryptography, Asymmetric Cryptography
- 1976 yılında ilk kez Diffie ve Hellman tarafından öne sürülmüştür.
- Ancak, 1. Dünya savaşı sırasında ABD tarafından benzer sistemlerin kullanıldığı iddia edilmektedir.
- İngiliz İstihbaratı tarafından 1973 yılında bilindiği bazı belgelerle gösterilmiştir.
- Birbiri ile daha önce görüşmemiş kişilerin güvenli iletişimini hedefler.
- Kimlik doğrulama, anahtar dağırımı ve inkar edememe problemlerine de çözüm sunar.
- Şifreleme ve çözme için farklı anahtarlar kullanılır.

Asimetrik (Açık) Anahtarlı Kriptografi

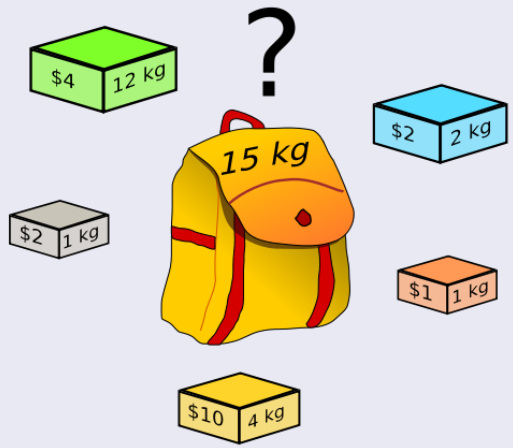
- Şifreleme anahtar (açık anahtar) herkese duyurulabilir.
- Çözme anahtarı (gizli anahtar) sadece sahibinde olmalıdır ve açık anahtardan üretimi pratikte mümkün olmamalıdır.
- Güvenlikleri matematiksel olarak çözümleri olan ancak işlemsel olarak çok uzun zaman alan problemlere dayanır.
- Asimetrik sistemler, simetrik sistemlere göre oldukça yavaştır. Bu yüzden tek başlarına kullanılmaları zordur.



Matematiksel Problemler

Sırt Çantası Problemi (Knapsack Problem)

- Belirli bir sayıdan küçük sayıların toplamlarının o sayıdan büyük ya da eşit olması problemidir.
- Knapsack Kriptosistemi bu problem üzerine kurulmuştur.
- LLL Algoritması ile kırılabilmektedir. Günümüzde kullanılmamaktadır.



Matematiksel Problemler

Ayrık Logaritma Problemi (Discrete Logarithm Problem)

- $Z_p* = \{1, 2, \ldots, p-1\} =< g >$
- Z_p^* üzerinde g ve $y = g^x \bmod p$ değerleri biliniyorsa $x =?$
- Sonlu gruplar üzerinde logaritma hesaplamak zordur: $x = log_g y$
- Problemin zorluğu seçilen gruba göre değişmektedir.
- Eliptik Eğriler üzerinde tanımlı gruplarda, normal gruplarda çalışan ataklar çalışmadığı için, eliptik eğri kriptosistemlerinde daha küçük anahtar boyutları kullanılabilmektedir.
- Kullanıldığı sistemler: Diffie-Hellman anahtar değişimi, ElGamal Açık Anahtarlı Altyapı, DSA, Eliptik Eğri Kriptosistemler.

Matematiksel Problemler

Ayrık Logaritma Problemi Örnek

- $Z_7* = \{1, 2, 3, 4, 5, 6\} =< 3 >$
- $p = 7, g = 3$
- $< 3 >= \{3^1 = 3, 3^2 = 2, 3^3 = 6, 3^4 = 4, 3^5 = 5, 3^6 = 1\}$
- Örnek: Öyle bir x bul ki $3^x = 5 \pmod 7$ olsun.
- Yani $x = log_3 5$

Matematiksel Problemler

Çarpanlara Ayırma Problemi

- Aritmetiğin Temel Teoremi: Birden büyük her tam sayı ya asaldır ya da asal sayıların kuvvetlerinin çarpımı şeklinde yazılabilir.
- Birleşik bir sayıyı asal çarpanlarına ayırma işlemi sayı büyüdükçe zorlaşır.
- Çarpanlara ayrılması en zor sayılar yarıasallardır.
- Bilinen en iyi algoritma "General Number Field Sieve (GNFS)"dir. O bile hızlı değildir.
- Çare Kuantum hesaplama!
- Kullanıldığı sistemler: RSA, Rabin Kriptosistem.

Matematiksel Problemler

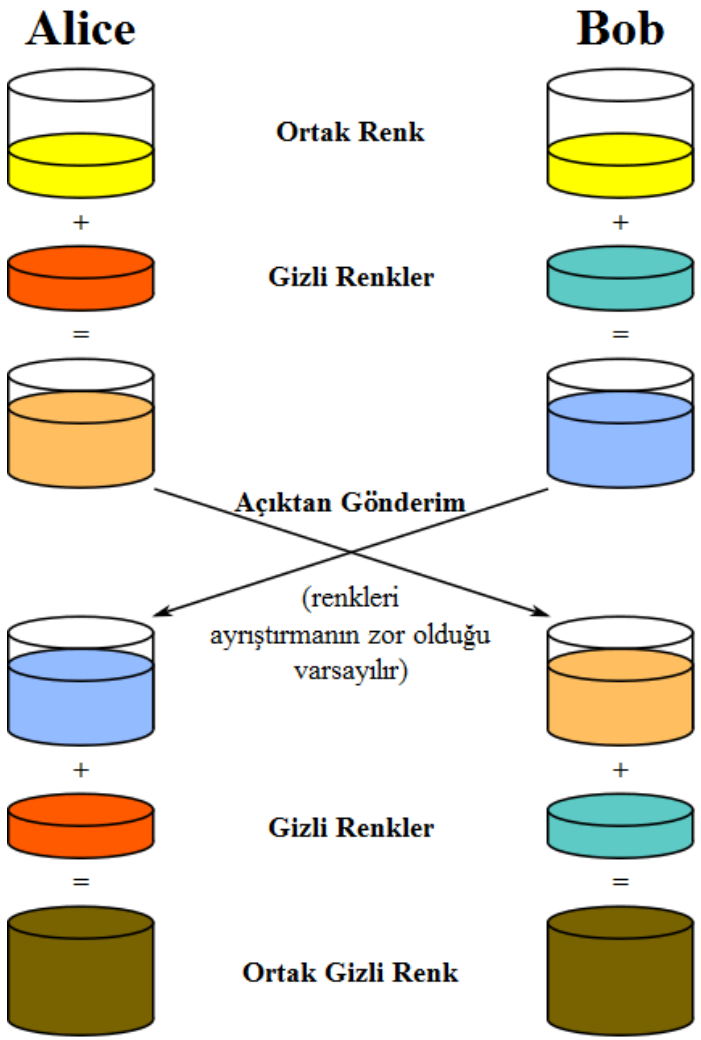
Çarpanlara Ayırma Problemi Örnekleri

- 1977 yılında Ron rivest 125 basamaklı (415-bit) bir yarıasalı çarpanlara ayırmanın 40 katrilyon yıl süreceğini hesapladı ancak günümüzde bu işlem saatler sürüyor.
- 1999 155 basamak (512-bit)
- 2003 174 basamak (576-bit)
- 2012 212 basamak (704-bit)
- 2013 Ekim: NSA tarafından 289 basamak (960-bit) yarıasalın çarpanlara ayrılabildiği iddia ediliyor.

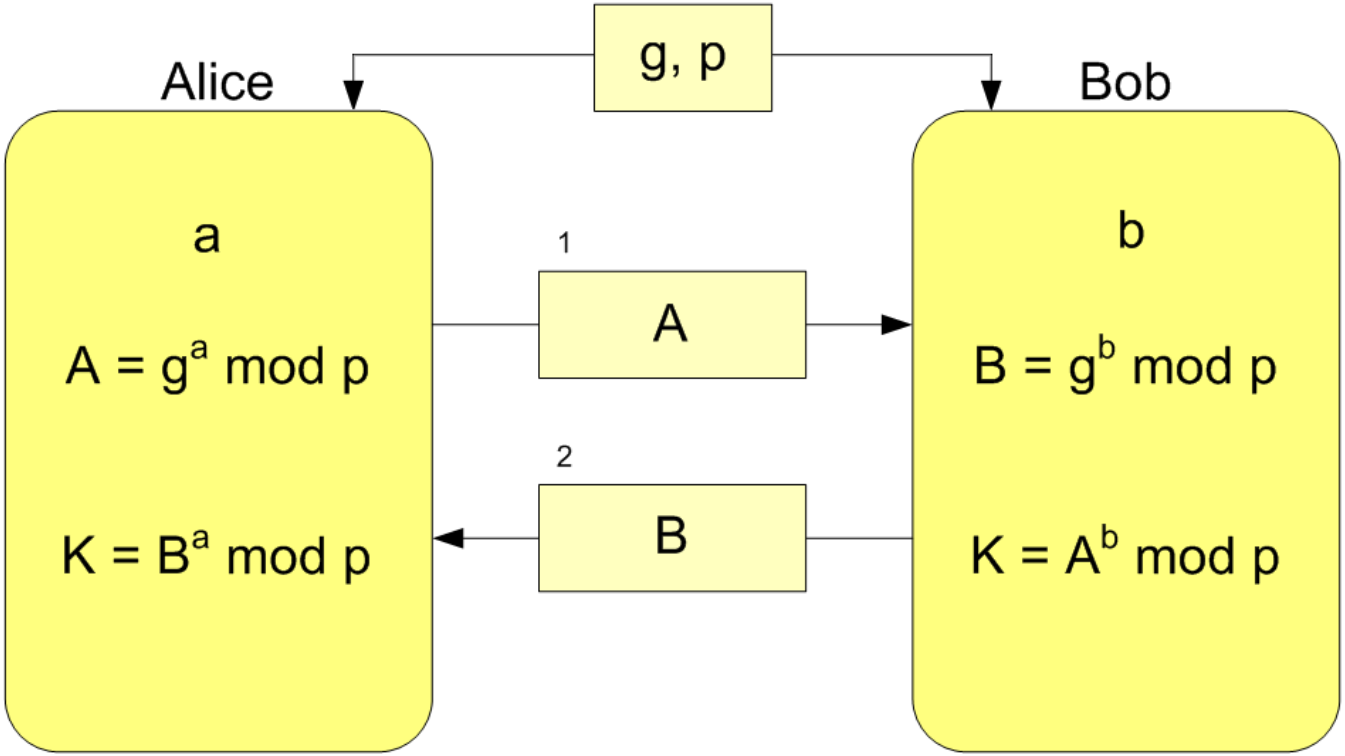
2^{64}	$\approxeq 10^{20}$
2^{80}	$\approxeq 10^{25}$
2^{128}	$\approxeq 10^{39}$
2^{256}	$\approxeq 10^{78}$

Diffie-Hellman Anahtar Değişimi

- Açık Anahtarlı Kriptografinin temeli olarak kabul edilir.
- 1976 yılında Whitfield Diffie ve Martin Hellman tarafından geliştirilmiştir.
- İki tarafın, güvensiz bir ortam üzerinden ortak bir gizli anahtar üzerinde anlaşmasını sağlar.
- Ayrık logaritma problemine dayalıdır.



Diffie-Hellman Anahtar Değişimi



- Alice: $K = B^a \bmod p = (g^b)^a \bmod p$
- Bob: $K = A^b \bmod p = (g^a)^b \bmod p$
- Düşman: $A = g^a \bmod p$, $B = g^b \bmod p \xrightarrow{?} g^{ab} \bmod p$

Rivest-Shamir-Adleman (RSA) Kriptosistem

- 1978'de Ron Rivest, Adi Shamir ve Leonard Adleman tarafından tasarlanmıştır.
- Güvenliği çarpanları ayırma problemine dayanır.
- RSA şifrelemeyi kırmanın çarpanlara ayırma problemini kırmak kadar zor olup olmadığı hala kesinleşmemiş bir problemdir.
  - Çok büyük sayılarla işlem yapıldığından dolayı çok yavaştır. Şifreleme, çözme işlemine göre daha hızlıdır.
  - 1980'lerde 512-bit RSA şifreleme işlemi 10 dakika sürerken, günümüz bilgisayalarında saniyede ≈ 80.000 işlem yapılabilmektedir.

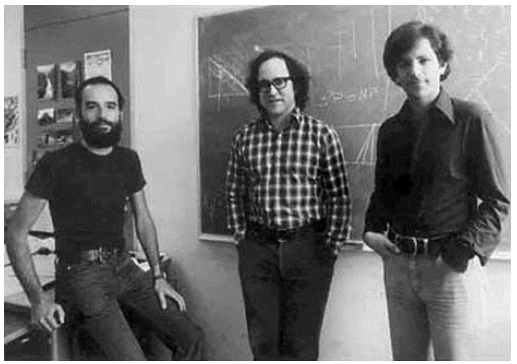


Figure: Adleman, Rivest, Shamir

RSA Kriptosistemi Parametreleri

- Örneğin, RSA 2048 için her birisi 1024-bit (≈ 300 basamak) olan iki tane asal sayı seç: p, q
- Modül değeri: $N = p * q$, N sayısı 2048-bit (≈ 600 basamaklı)
- Euler Phi Fonksiyonunu hesapla: $\varphi(N) = (p-1)(q-1)$
- $obeb\,(e, \varphi(N)) = 1$ olacak şekilde e sayısı seç.
- e sayısı çoğunluka $2^{16} + 1 = 65537$ olarak seçilir.
- $e \cdot d \equiv 1 \bmod \varphi(N)$ olacak şekilde d sayısını hesapla.

- **Açık Anahtar**: (e, N)
- **Gizli Anahtar**: (d, N)

RSA Şifreleme ve Çözme

Şifreleme İşlemi

Şifrelenecek mesaj m, açık anahtar (e, N) çifti olsun. Şifreli mesaj c aşağıdaki gibi hesaplanır.

$$c = m^e \bmod N$$

Şifre Çözme İşlemi

Gizli anahtar (d, N) çifti olsun. Şifreli mesaj c'den açık mesaj p'yi elde etmek için aşağıdaki hesaplama yapılır.

$$p = c^d \bmod N$$

RSA Neden Çalışır?

- Euler'in Teoremi:

$$(a, N) = 1, 0 < a < N \implies a^{\varphi(N)} \equiv 1 \bmod N$$

- Şifre Çözme İşlemi:

$c^d \bmod N$

$\equiv (m^e)^d \bmod N$

$\equiv m^{(1+k\cdot\varphi(N))} \bmod N$ (Çünkü: $ed \equiv 1 \bmod \varphi(N)$)

$\equiv m \cdot m^{(k\cdot\varphi(N))} \bmod N$

$\equiv m \bmod N$

Asal Sayı Üretme

- Büyük asal sayılar üretmek RSA için en önemli noktadır.
- Bilinen en meşhur asallık testi: Miller-Rabin.
- İstatistikseldir. Kesin sonuç vermez!
- **Asal sayı üretme yöntemi:**

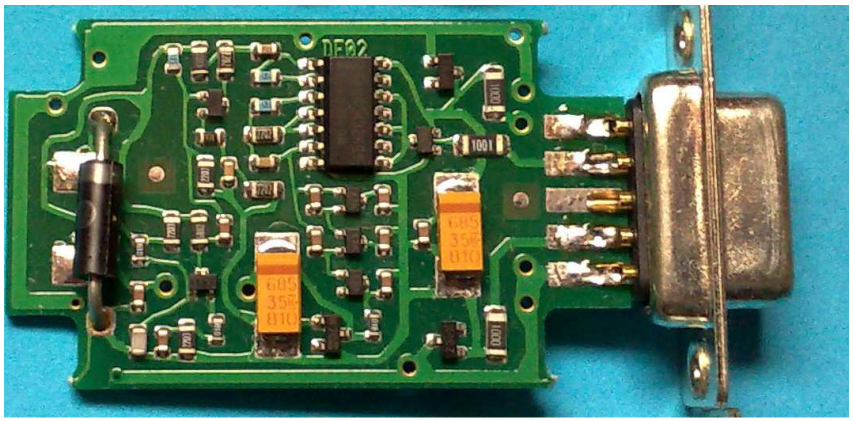
  Rastgele bir sayı seç.

  Asal mı kontrol et. Değilse yeniden dene.

Rastgele Sayı Üreteçleri (RSÜ) (RNG)

Gerçek RSÜ (True RNG)

- Fiziksel kaynakları kullanarak elde edilir. Örnek: Zener diyotlar, radyoaktif gürültü, termal gürültü vb.
- Üretilen dizi tekrar üretilemez. (Non-deterministic)
- Üretim kapasiteleri (throughput) düşüktür.
- Örnek Site: `http://www.random.org/`



TRNG9803

Rastgele Sayı Üreteçleri (RSÜ) (RNG)

Sözde RSÜ (Pseudo RNG)

- Belirli bir ilk değer kullanılarak üretilirler.
- Aynı ilk değer ile hep aynı rastgele dizi üretilir. (Deterministic)
- Periyodiktir. Belirli bir yerden sonra tekrar etmeye başlar.
- Üretim kapasiteleri yüksektir.
- Örnek: LCG, Mersenne twister, Blum Blum Shub,... Genel Liste
- Test! NIST Test Paketi ve Diehard Testleri

Elektronik İmza

- Bir verinin, gizli anahtar ile çözme işlemine tabi tutulması sonucu elde edilen bilgiye elektronik imza denir.
- Elektronik İmza bilgisi sadece gizli anahtar sahibi tarafından üretilebileceği için belirli bir veri ve kişi için benzersizdir.
- Elektronik İmza bilgisi açık anahtar ile şifrelenirse orjinal metni vereceğinden doğrulama işlemi herkes tarafından yapılabilir.
- Elektronik İmza ve Açık Anahtarlı Şifreleme için aynı anahtar çifti kullanılmamalıdır. Kullanıldığı durumda, oluşturulan her şifreli metnin imzası ona karşılık gelen açık metin olacaktır.

Elektronik İmza

- Elektronik İmza mesajın gizliliğini sağlamaz. Sadece kaynak doğrulamasını yapar.
- Aynı zamanda imzayı atan kişinin de bunu inkar edememesini sağlar. Çünkü gizli anahtar sahibi kişi, anahtarını korumakla mesuldür.
- Elektronik İmza direkt olarak mesaja uygulanırsa imza boyutu da mesaj boyutu ile aynı olacaktır.
- Bu yüzden Hash (Özet) Fonksiyonları denen yapılar kullanılarak bu durum önlenir.

DSA: Sayısal İmza Algoritması

- Güvenliği, ayrık logaritma problemine dayalıdır.
- ElGamal elektronik imza algoritmasının düzenlenmiş halidir.
- NSA mühendisi David W. Kravitz tarafından tasarlanmıştır ve patentlidir.
- Sadece Elektronik İmza için kullanılır.
- İlk kez 1991'de NIST tarafından yayınlanmıştır. Son versiyonu 2013 yılında FIPS 186-4 standardı ile yayınlanmıştır.

Eliptik Eğri Kriptografi (ECC)

- 1985 yılında Miller ve Koblitz tarafından önerilmiştir.
- RSA'nın alternatifi: hızlı ve daha az bellek kullanımı
- Güvenliği, eliptik eğriler üzerinde ayrık logaritma problemine dayanır.
- Ayrık logaritma problemi için önerilen çözümler eliptik eğriler üzerinde tam olarak çalışmadığı için daha güvenli olarak kabul edilmektedir.
- NIST 2005 yılında yayınladığı "Suite B" kriptografi setinde "çok gizli" olarak tasniflendirilecek dokümanlarda 384-bit ECC kullanımını zorunlu hale getirmiştir.

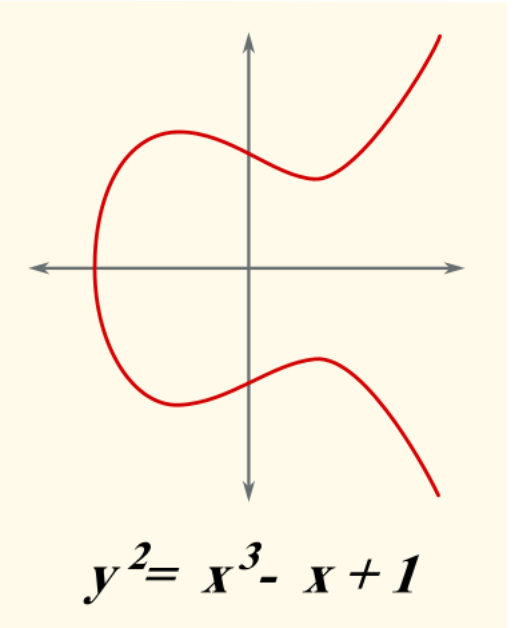


Figure: Eliptik Eğri

ECC Algoritmaları

- **ECDH**: Elliptic Curve Diffie–Hellman Key Exchange
- **ECDSA**: Elliptic Curve Digital Signature Algorithm
- **ECIES**: Elliptic Curve Integrated Encryption Scheme
- **Dual_EC_DRBG**: Dual Elliptic Curve Deterministic Random Bit Generator

  2006 yılında yayınlanan Dual_EC_DRBG'de NSA tarafından konulduğu iddia edilen bir arka kapı (backdoor) bulunmuştur!

AAA Karşılaştırma

Algoritma	Şifreleme	İmzalama	Anahtar Değişimi
Diffie-Hellman	Hayır	Hayır	Evet
RSA	Evet	Evet	Evet
ElGamal	Evet	Evet	Evet
DSA	Hayır	Evet	Hayır
ECDH	Hayır	Hayır	Evet
ECDSA	Hayır	Evet	Hayır

Hash (Özet) Fonskiyonları

- $H: \{0,1\}^* \rightarrow \{0,1\}^n, n = 160, 256, 512$ vb.
- Her boyuttan bilgiyi sabit uzunluklu bit dizisine dönüştüren fonksiyonlara denir.
- Özet değerini hesaplamak kolay olmalıdır.
- Teorik olarak tek yönlü olması mümkün değildir. Ancak pratikte öyle olduğu varsayılır.
- Yani, aynı özet değerini veren ikinci bir mesaj bulmak zor olmalıdır.
- Bir özete karşılık gelecek mesajı oluşturmak zor olmalıdır.
- Aynı özete sahip iki farklı mesaj bulmak zor olmalıdır.

Hash (Özet) Fonskiyonları

- Özet fonksiyon tasarımı tekrarlı blok şifre tasarımına benzer şekilde yapılabilir.
- En meşhur özet fonksiyon tasarımı Merkle-Damgard tasarım şemasıdır.
- Şifre depolama, doğrulama, bütünlük kontrolü ve e-imza kullanım alanlarından bir kaçıdır.
- En sık kullanılan özet fonksiyonlar MD5 ve SHA ailesidir.

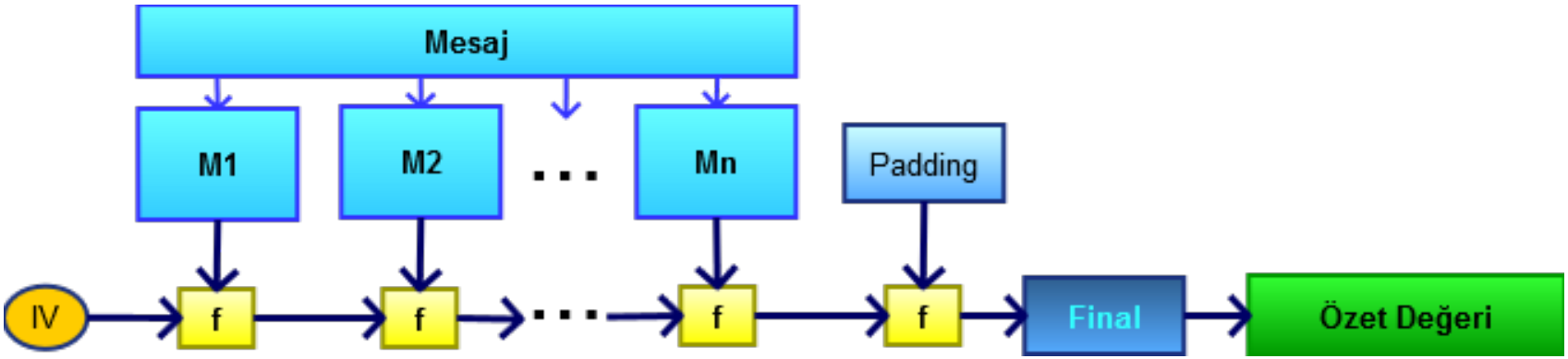


Figure: Merkle-Damgard Yapısı

Hash (Özet) Fonskiyonları

- Doğum Günü Paradoksu: 32-bit uzunluğunda rastgele sayılar üretiyorsunuz, aynı sayıyı ikinci kez üretme ihtimaliniz kaçıncı üretimden sonra %50'den fazla olur?

Hash (Özet) Fonskiyonları

- Doğum Günü Paradoksu: 32-bit uzunluğunda rastgele sayılar üretiyorsunuz, aynı sayıyı ikinci kez üretme ihtimaliniz kaçıncı üretimden sonra %50'den fazla olur?
- Cevap: $\gtrapprox \sqrt{2^{32}} = 2^{16}$
- Benzer şekilde çıktı boyutu n-bit olan bir özet fonksiyonunun güvenliği $2^{\frac{n}{2}}$'dir.
- Hellman tabloları veya Rainbow tablolarını kullanarak bazı özet değerlerine karşılık gelen mesajları bulmak olasıdır.
- Teorik olarak en optimize edilmiş tabloların bile kapsama oranı %56'dan fazla olamaz.

Message Digest 5 (MD5)

- Ronald Rivest tarafından 1992 yılında MD4'ün devamı olarak tasarlanmıştır.
- Standart: RFC 1321
- Özet değeri boyutu: 128-bit
- Merkle-Damgard Yapısı kullanmaktadır.
- Günümüz bilgisayarlarında 20 saniyeden az sürede kırılabilmektedir. (2009)
- Dolayısıyla, kriptografik uygulamalar için güvenli değildir.

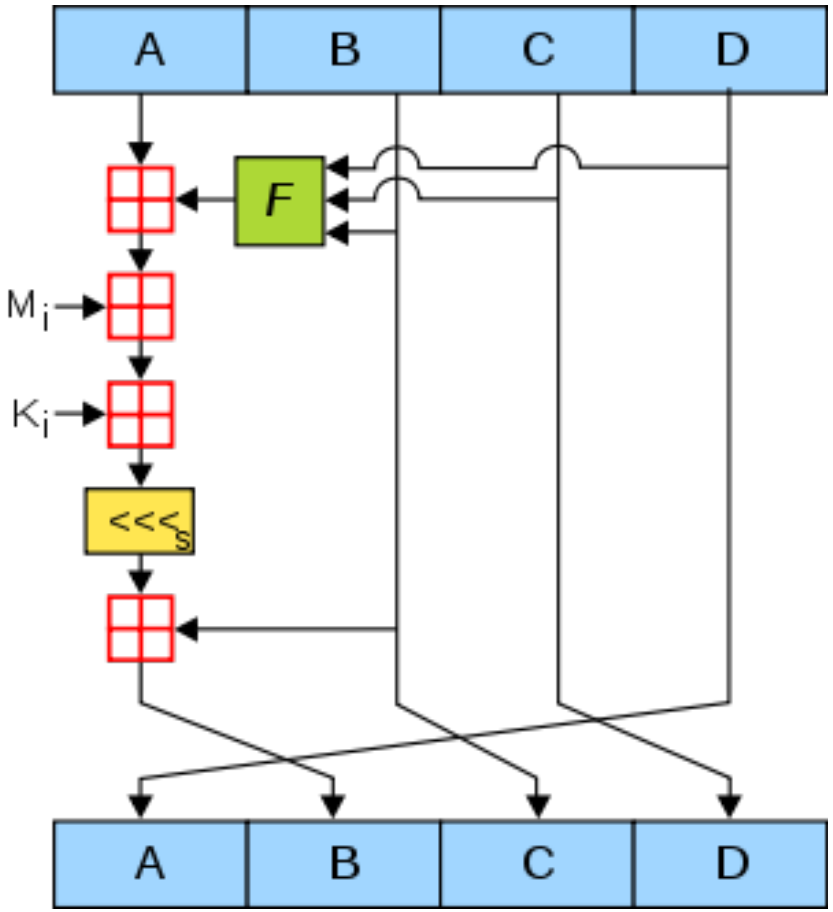


Figure: MD5 Çevrim Fonksiyonu

Secure Hash Algorithm (SHA) Ailesi

- MD5'in zayıflıklarının ortaya çıkması ile 1993 yılında NIST tarafından yayınlanan ve NSA tarafından tasarlanan ilk hash fonksiyonu SHA0 olmuştur.
- Ancak, açıklanmayan bir zayıflığından ötürü daha yayınlanmadan kullanımı iptal edilmiştir.
- Ardından, MD5'in yerini alması için 1995 yılında SHA-1 algoritması yayınlanmıştır.
- 2001 yılında SHA-1 yerine SHA-2 ailesi getirilmiştir. SHA-2 ailesinde SHA-224, SHA-256, SHA-384 ve SHA-512 bulunmaktadır.

Secure Hash Algorithm (SHA) Ailesi

- SHA-1 ve SHA-2 ailesi de MD5 gibi Merkle-Damgard yapısını kullanmaktadır.
- SHA-0: FIPS PUB 180
- SHA-1: FIPS PUB 180-1
- SHA-2: FIPS PUB 180-2
- **SHA-3**: FIPS PUB 180-5

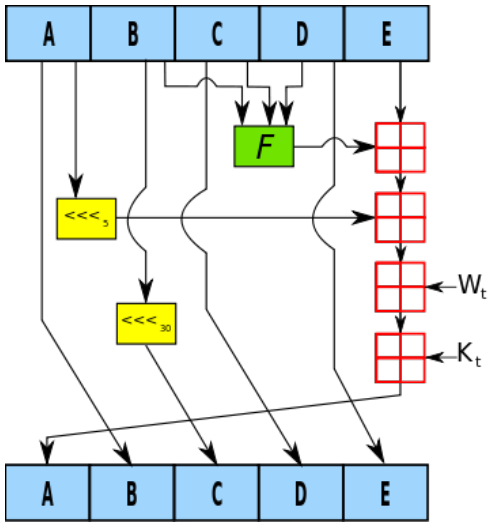


Figure: SHA1 Çevrim Fonksiyonu

Algorithm and variant		Output size (bits)	Internal state size (bits)	Block size (bits)	Max message size (bits)	Word size (bits)	Rounds	Operations	Collisions found?
SHA-0		160	160	512	$2^{64} - 1$	32	80	add, and, or, xor, rotate, mod	Yes
SHA-1									Theoretical attack (2^{60})
SHA-2	*SHA-256/224*	256/224	256	512	$2^{64} - 1$	32	64	add, and, or, xor, rotate, mod, shift	No
	SHA-512/384	512/384	512	1024	$2^{128} - 1$	64	80		

SHA-3

- NSA'ya olan güvenin azalması, AES sürecinin emsal teşkil etmesi ve akademik olarak böyle bir çalışmaya ihtiyaç duyulması gerekçeleriyle 2 Kasım 2007'de NIST tarafından SHA-3 yarışması duyuruldu.
- Tasarım kriteri olarak SHA-2 ailesinde desteklenen bit uzunlukları belirtildi.
- 31 Ekim 2008'e kadar başvurular kabul edildi. Toplam 64 başvuru oldu. 51'i ilk aşamaya seçildi.
- İkinci aşamaya sadece 14 algoritma seçildi.
- 51 adaydan 4 tanesi Türk'tü. Sadece biri ilk 14'e kaldı.
- Üçüncü ve son aşamaya 5 algoritma seçildi.

Türk SHA-3 Adayları

Başvuru	İsim	Elenme Sebebi
Özgül Küçük	Hamsi	İlk 14'te fakat çok yavaş
Kerem Varıcı	Sarmal	Teorik zayıflık
Çetin Kaya Koç	Spectral Hash	Teorik zayıflık
TÜBİTAK UEKAE	SHAMATA	Pratikte kırıldı

SHA-3 Final Adayları

- Eleme Kriterleri: Güvenlik, Maliyet, Performans, Tasarım Karakteristiği

BLAKE	İsviçre Kudelski Siber Güvenlik Merkezi
Grostl	Knudsen ve Ekibi
JH	Singapur Nanyang Teknik Üniversitesi
Keccak	AES'i tasarlayan ekip (ST, NXP)
Skein	Bruce Schneier ve Ekibi

- 2 Ekim 2012 tarihinde KECCAK algoritması yeni SHA-3 standardı olarak belirlendi.

Anahtar Üretme Fonksiyonu

- Key Derivation Function (KDF)
- En popüler olanı PBKDF2 (Password-Based Key Derivation Function 2)

  $DK = PBKDF2(PRF, Password, Salt, c, dkLen)$
- Hash fonksiyonları kullanarak, kullanıcı tarafından yazılan bir parolayı kriptografik olarak uygun hale getirmek amaçlı kullanılır.
- Tablo ataklarını önlemede etkilidir.

  WPA2:
  $DK = PBKDF2(HMAC - SHA1, passphrase, ssid, 4096, 256)$

  Zayıf parolayı kırmak karmaşıklığı 4096(12-bit) kat güçlendirilmiştir.
- Diğer bir örnek: WinZip vs. WinRAR

Password Hashing Competition

- Tek standart olan PBKDF2'ye alternatif üretme amaçlı düzenlenmektedir.
- CPU ve GPU ataklarına dayanıklı bir sistem.
- 2013 başlarında duyuruldu. Son başvuru Ocak 2014.
- Final: Haziran 2015.
- Site: `https://password-hashing.net/`

Kriptoanaliz

- Herhangi bir şifreleme sisteminin zayıflığını bulma sanatıdır.
- Temel amaç anahtar olmadan bilgiye ulaşmaktır.
- Matematiksel kriptoanaliz, protokol analizi ve yan kanal saldırıları olmak üzere üç ana bölümde toplanabilirler.
- Matematiksel analizler, sistem tasarımındaki zayıflıkları bulmak ve bunları kullanarak bilgiyi ele geçirme yöntemleridir. Çoğunlukla teoriktir.
- Protokol Analizi, kriptosistemlerin protokollerde kullanım yöntemlerini inceleyerek bilgiye ulaşma analizidir. Örneğin: WEP ve RC4.
- Protokol ya da kriptosistemin implement edildiği cihaza yapılan saldırılara yan kanal saldırısı denir. Örneğin bazı akıllı kartlarda çalışan bir RSA 1024-bit anahtarı bu yöntemle 18 saatte çıkarılabilmektedir.

Enigma - Bombe

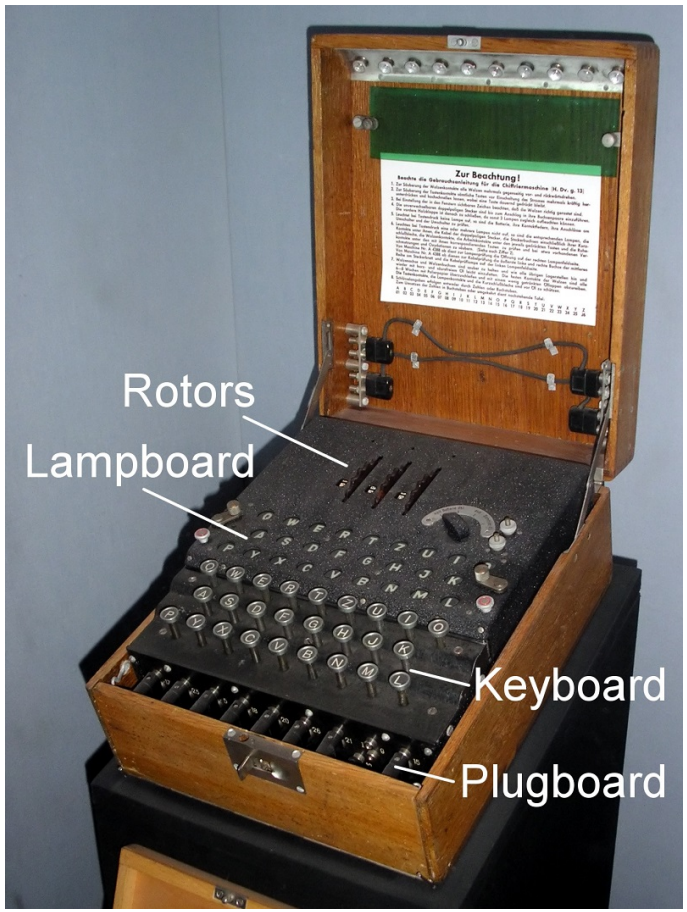


Figure: Enigma

Figure: Bombe

Tam Arama Yöntemi (Brute Force, Exhaustive Search)

- Bir kriptoanaliz yöntemi değildir.
- Kaba kuvvet kullanarak olası tüm ihtimalleri deneyerek doğrusunu bulmaktır.
- $n-$bit boyutundaki bir anahtar için tüm ihtimal sayısı 2^n'dir.

Tam Arama Örnek

- 128-bit anahtar için tüm uzayı aramak isteyelim.
- Her çekirdek saniyede 2^{48} deneme yapsın. ($\approxeq 300\,THz$ işlem gücü)
- Dünyadaki insan sayısı: 7 Milyar $\approxeq 2^{33}$
- Her insan $1024 (= 2^{10})$ çekirdekli bilgisayara sahip olsun.

$$\frac{2^{128}}{\approxeq 2^{33} \cdot 2^{10} \cdot 2^{48}}$$

- Toplam Süre $\approxeq 2^{37}$ saniye.
- $\approxeq$ 1.6 Milyon gün.

Atak Modelleri

- **Sadece Şifreli Metin (Ciphertext Only)**

  Sadece şifreli metin üzerinden yapılan ataklardır. En zor senaryodur.
- **Bilinen Düz Metin (Known plaintext)**

  Düz metin ve ona karşılık gelen şifreli metinler ile yapılan saldırılar.
- **Seçili Düz Metin (Chosen Plaintext)**

  İstenilen düz metinlere karşılık gelen şifreli metinler elde edilerek yapılan ataklardır.

Atak Modelleri

- **Seçili Şifreli Metin (Chosen Ciphertext)**

  İstenilen şifreli metinlere karşılık gelen açık metinler elde edilerek yapılan ataklardır.
- **Uyarlanabilir Seçili Düz Metin (Adaptive Chosen Plaintext)**

  İstenilen açık metin ve ona karşılık gelen şifreli metni elde ettikten sonra tekrar istekte bulunarak yapılan ataklardır.
- **Uyarlanabilir Seçili Şifreli Metin (Adaptive Chosen Ciphertext)**

  İstenilen şifreli metin ve ona karşılık gelen açık metni elde ettikten sonra tekrar istekte bulunarak yapılan ataklardır.

Sözlük Atağı

Sözlük Atağı

- Tüm ihtimalleri denemek yerine olasılığı yüksek ihtimalleri deneme yöntemidir.
- Örneğin, gizli anahtar, kullanıcının belirlediği bir parola ise, en çok kullanılan parolaları denemek sonuç verebilir.

Tablo Atağı

Rainbow ve Hellman Tablolar

- Açık metinler ve onlara karşılık gelen şifreli metinler belirli bir formatla tablolarda tutulur.
- Çözülmek istenen bir şifreli metin bu tablodan bakılarak geri çevrilebilir.
- Tuz (salt) kullanımı ile tablolara karşı dayanıklılık sağlanabilir.
- Hellman tabloları ve ardından da Rainbow tabloları tasarlanmıştır. Aralarındaki en büyük fark tablolardaki ara verileri hesaplama yöntemleridir.
- En iyi hazırlanmış bir Rainbow tablosu tüm uzayın %51'ini kapsarken, Hellman tablosu %56'sını kapsamaktadır.
- Örnek: GSM A5/1 algoritması 2.2 Terabayt'lık bir Rainbow tablosu ile kırılabilmektedir.

Doğrusal ve Diferansiyel Kriptoanaliz

- Günümüzde, simetrik sistemler için en yaygın olarak kullanılan saldırılardır.
- Bulunmaları ile birlikte simetrik sistem tasarımında önemli bir kriter olmuşlardır.
- Şifreleme sistemlerinin tamamına uygulamak her zaman mümkün olmayabilir.
- Bu yüzden zayıflatılmış (daha az çevirmi olan) hallerine uygulanır.
- Bu ataklar ile genellikle alt anahtarlar kurtarılarak esas gizli anahtara ulaşılmaya çalışılır.

Doğrusal Kriptoanaliz (Linear Cryptanalysis)

- 1992 yılında Matsui tarafından bulunmuştur. Simetrik şifreleme sistemlerine uygulanabilir.
- Açık metnin belirli bitleri ile şifreli metnin belirli bitleri arasında doğrusal bir ilişki olmasının 1/2'den farklı bir olasılıkla olduğu durumları inceleyerek atak gerçekleştirilir.
- Bu bilgi ile belirli sayıda açık ve şifreli metin analiz edilerek alt anahtarları kurtarmak mümkün olabilir.

Diferansiyel Kriptoanaliz (Differential Cryptanalysis)

- 1980'lerin sonunda Biham ve Shamir tarafından bulunmuştur.
- Açık metindeki belirli bitlerdeki değişikliklerin şifreli metinde belirli bitlerde yüksek olasılıkla değişikliğe sebep olduğu durumları inceleyerek atak gerçekleştirilir.
- Açık metinden şifreli metine giden bu yüksek olasılıklı bitler takip edilerek, açık metin ve şifreli metinler üzerinde analizler yaparak alt anahtarları kurtarmak mümkün olabilir.

Teşekkürler.
Sorular?