Block Ciphers and Cryptanalysis

Cihangir TEZCAN

Department of Cryptography
Institute of Applied Mathematics
Middle East Technical University, Ankara, Turkey

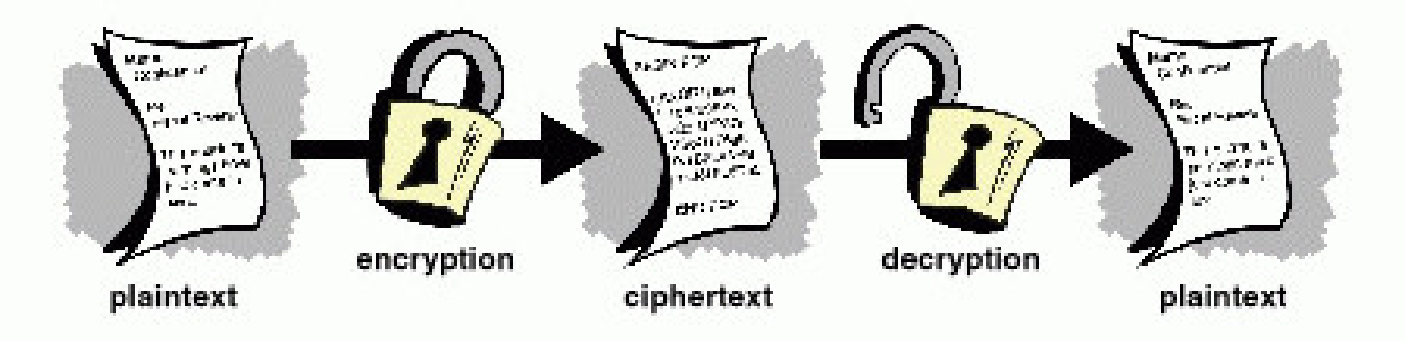
Ankara Cryptology Seminars

November 13, 2012, Ankara, Turkey

What is a Cryptosystem

What is a Cryptosystem?

- **Plaintext** is what you want to protect
- A **cryptosystem** is pair of algorithms that convert plaintext to ciphertext and back.
- **Ciphertext** is the encrypted version of the plaintext
- Ciphertext should appear like a **random** sequence



Kerkckhoffs's Principle

Kerkckhoffs's Principle (1883)

Cipher must not be required to be secret, and it must be able to fall into the hands of the enemy without inconvenience.

In other words, the security of the system must rest entirely on the secrecy of the key.

Claude Shannon

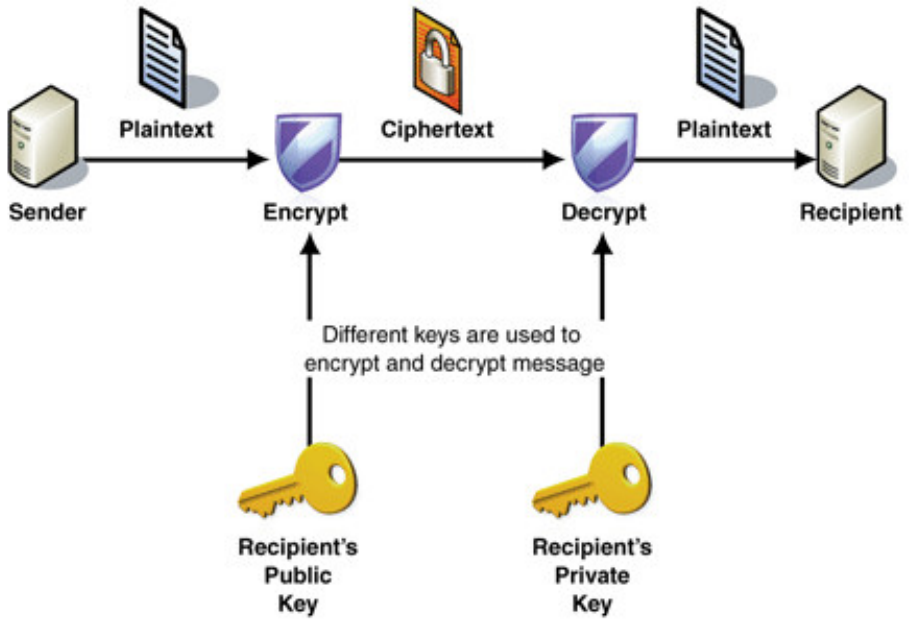
The enemy knows the system.

Symmetric Cryptosystems

- Keys used for encryption and decryption are identical or closely related
- In other words, one can be obtained from the other in polynomial time

Public-key Cryptosystems

- Encryption key is publicly announced
- **Hard** to get the decryption key



Public-key Cryptosystems

Related Courses

- **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

The Unbreakable Cipher

One-time Pad

- Generate a very long sequence of **random** bits (one-time pad)
- XOR the plaintext and the one-time pad to get the ciphertext
- XOR the ciphertext and the one-time pad to get the plaintext

Example

Plaintext	010101111001001...
One-time pad	101111010110101...
Ciphertext	111010101111100...

Warning

- One-time pad must be **truly random**
- Can only be used **once**

Stream Ciphers

Symmetric Ciphers can be classified as

1. Stream Ciphers
2. Block Ciphers

Stream Ciphers

- Instead of a one-time pad, use a shorter key (128 bits)
- Based on this key, generate a **pseudorandom** keystream and use it like a one-time pad
- Security highly depends on the **randomness** of the keystream

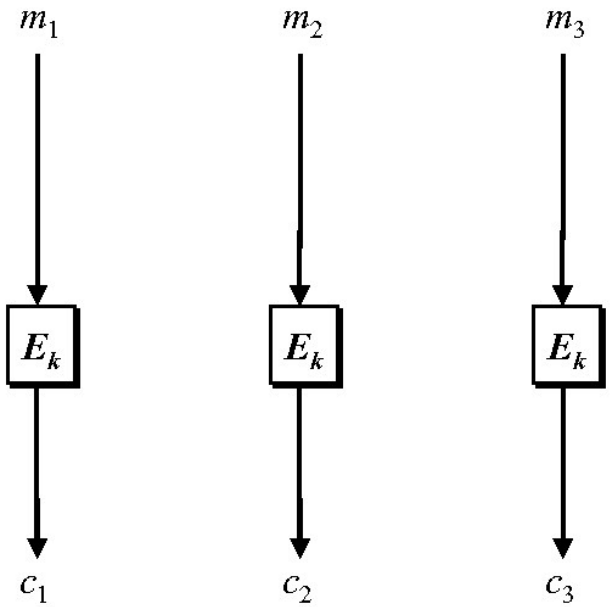
Warning

Keystream is no longer **truly random** but **pseudorandom**

Block Ciphers

Block Ciphers

Divide the plaintext into fixed length blocks (b bits) and then encrypt



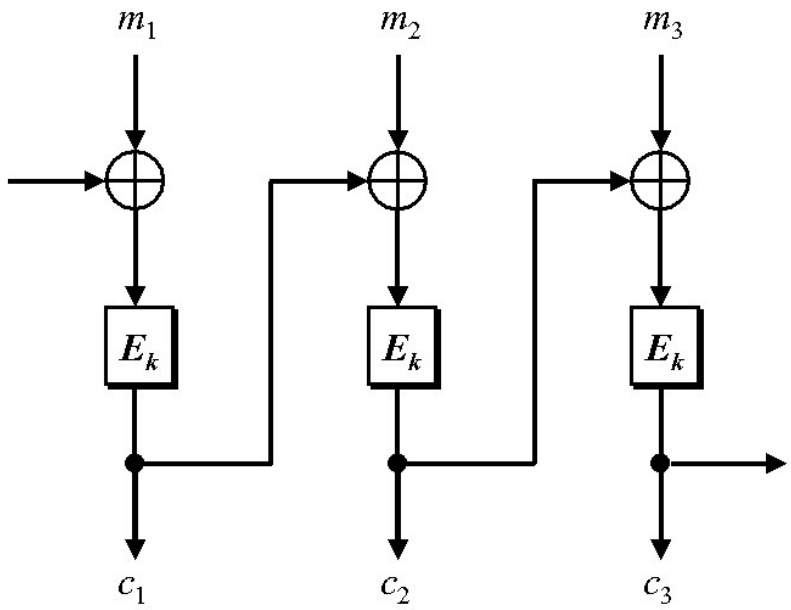
Problem

Direct use is not advised: Same plaintext blocks give same ciphertext blocks

Block Ciphers

Solution

Use a mode of operation. e.g. Block cipher chaining mode



More on modes of operation

Talk will be given by *Dr.Fatih Sulak* on **4.12.2012** at **TOBB**

Block Ciphers

Keys

- Must be strongly protected
- Should be a **random** set of bits of the appropriate length (128, 192 or 256 bits)
- Each key should be used for a limited time only

Related Courses (cont'd)

- **MATH 405** Combinatorics

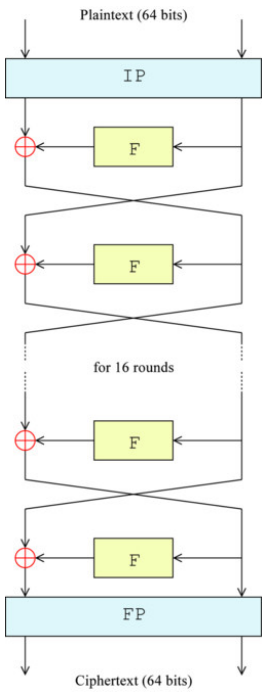
More on Randomness

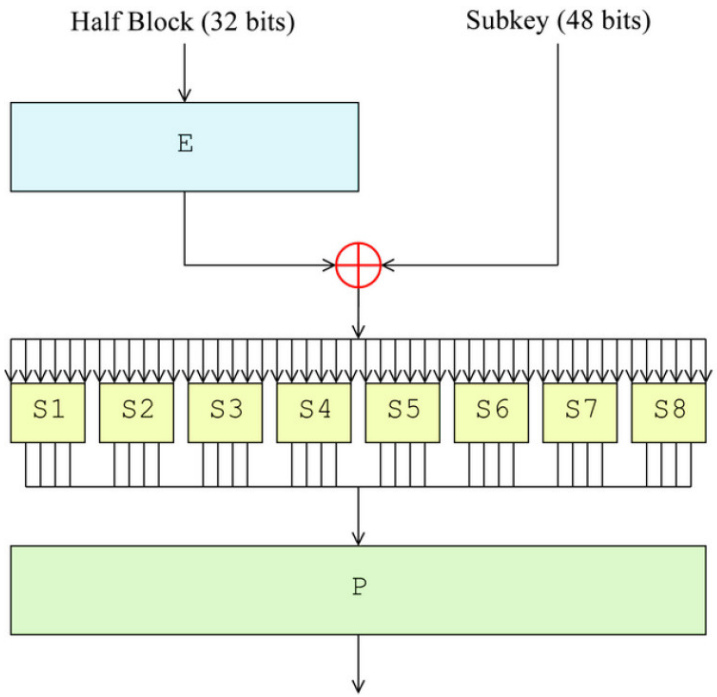
Talk will be given by *Assoc.Prof.Ali Doğanaksoy* on **20.11.2012** at **Atılım University**

Data Encryption Standard

Data Encryption Standard (DES)

- Designed in 1970s by IBM (NSA tweaked the original design)
  - Block Size: 64 bits
  - Key Size: 56 bits
  - Rounds: 16
- Still *unbroken*, but key size made it to weak to use after 1990s





Advanced Encryption Standard

Advanced Encryption Standard (AES)

- Adopted in 2001 by the NIST (winner of an open public design competition)
  - Block Size: 128 bits
  - Key Size: 128, 192, 256 bits
  - Rounds: 10, 12, 14 (depending on the key size)
- All known attacks are *infeasible*

Generic Attacks

Exhaustive Search

- Try every possible key
- For k bit keys, requires 2^k encryptions

How infeasible? (Numbers shamelessly stolen from Arjen K. Lenstra)

- Effort 2^{128}, that's more than 3×10^{38}
- Assume PCs run at 1000GHz: 10^{12} **ops/sec**
- fewer than 3×10^7 sec/year: 3×10^{19} **ops/year**
- 10^{10} people, each 1000 PCs: 3×10^{32} **ops/year**
- Requires **a million years**

Generic Attacks

CPU Speed versus Key Size

- **Moore's Law (1965):** The number of transistors on integrated circuits doubles approximately every two years (actually it is 18 months).
- Moving from 128-bit AES to 256-bit AES
  - takes less than 40% longer
  - but increases the attackers effort by a factor of 2^{128}
- Moore's Law favors the defender

Generic Attacks

Table Attack / Dictionary Attack

- Precompute/capture every plaintext and corresponding ciphertext
- Store them in a table

Complexities

- Exhaustive Search
  - Time complexity: 2^k encryptions
  - Data complexity: 0
  - Memory complexity: 0
- Dictionary attack
  - Time complexity: 0
  - Data complexity: 2^b blocks
  - Memory complexity: 2^b blocks

Attack Models

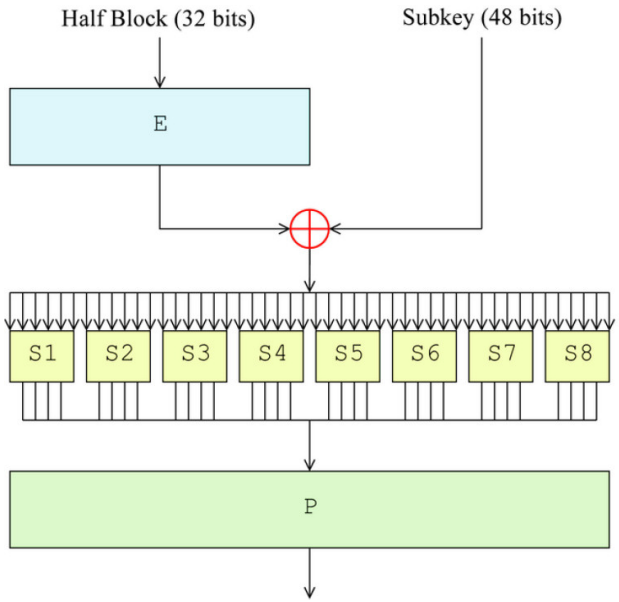
Attack Models

- **Ciphertext-only:** the adversary has access only to the ciphertext.
- **Known plaintext:** the adversary can obtain pairs of plaintexts and their corresponding ciphertexts (e.g. Linear Cryptanalysis).
- **Chosen plaintext:** the adversary can choose the type of plaintexts and gets the corresponding ciphertexts (e.g. Differential Cryptanalysis).
- **Chosen ciphertext:** just like chosen plaintext, but with ciphertexts.
- **Adaptive chosen plaintext:** the adversary may choose what is the next plaintext she wishes for, after seeing an earlier response.
- **Adaptive chosen plaintext and ciphertext:** . . . (e.g. Boomerang Attack)

Differential Cryptanalysis

Differential Cryptanalysis

- First public announcement by E. Biham and A. Shamir, early 1980s
- First discovery *may be* as early as the Second World War
- Find a path (characteristic) so that when the input difference is α, output difference is β with high probability
- DES is *strangely* resistant to Differential Cryptanalysis (to break 16 rounds, 2^{49} chosen plaintexts required)



Differential Cryptanalysis

Example

A game of dice: You are given a dice and asked to find out if it is a fair dice, or a biased dice that has probability $\frac{1}{3}$ for rolling 6. What would you do?

How to compute data/time complexity and success probability?

- This is a statistical attack
- What is the success probability of the attack if we use N chosen plaintexts?
- What is the data complexity if we require the success probability of the attack to be higher than p?
- **Solution:** *Assist. Prof. Ali Aydın Selçuk* provided nice formulas

Related Courses (cont'd)

- **MATH 301** Introduction to Probability Theory

Variants of Differential Cryptanalysis

Variants of Differential Cryptanalysis

- Truncated Differential Cryptanalysis (Knudsen 1994)
- Higher Order Differential Cryptanalysis (Knudsen 1994)
- *Impossible Differential Cryptanalysis (Biham-Biryukov-Shamir 1998)*
- Boomerang Attack (Wagner 1999)
- Improbable Differential Cryptanalysis (Tezcan 2010)
- Multiple Differential Cryptanalysis (Blondeau-Gerard 2011)

Impossible Differential Cryptanalysis

- **Impossible differential:** A differential path where an α difference **never** goes to a β difference (after some rounds of encryption)
- Impossible events were used to cryptanalyse ciphers before

Impossible Attacks

Example

- Cryptanalysis of Enigma during the WWII
- **Impossible event:** A letter is never encrypted to itself
- **Idea:** Plaintext may contain 'Keine besonderen Ereignisse' (means 'nothing to report')

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			

More on Impossible Differential Cryptanalysis

See second part of this seminer.

Conclusion

Thank You for Your Attention