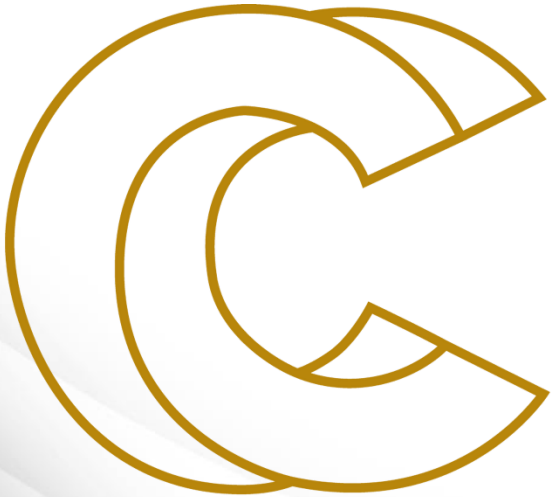


EURO 4SEE

GPU Assisted Brute Force Cryptanalysis of GPRS, GSM, RFID, and TETRA

Cihangir Tezcan, PhD
Graduate School of Informatics, METU, Ankara

ncc@ulakbim.gov.tr

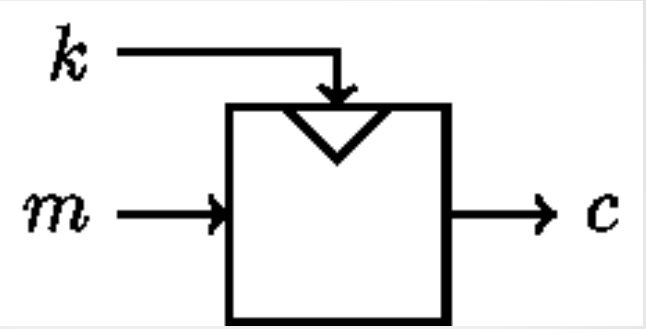
Lesson 1: Introduction to Block Ciphers

Introduction to Block Ciphers

- Cryptography solves many problems and confidentiality is just one of them.
- Encryption algorithms provide confidentiality.
- Data we want to encrypt can be:
  - Data at rest
  - Data in transit
  - Data in process

Lesson 1: Introduction to Block Ciphers

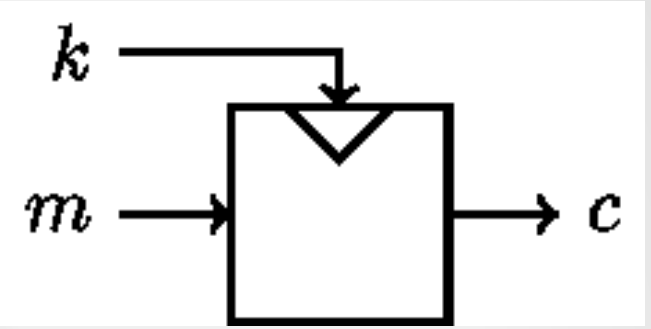
Some Definitions



- Plaintext **m** is what we want to protect.
- Ciphertext **c** is the encrypted version of the plaintext.
- A cryptosystem/cipher is a pair of algorithms that convert plaintext to ciphertext and back.
- Ciphertext should appear like a random sequence of bits.
- Details of a cipher should not be kept secret. The only secret is the secret key **k** that is chosen by the user.

Lesson 1: Introduction to Block Ciphers

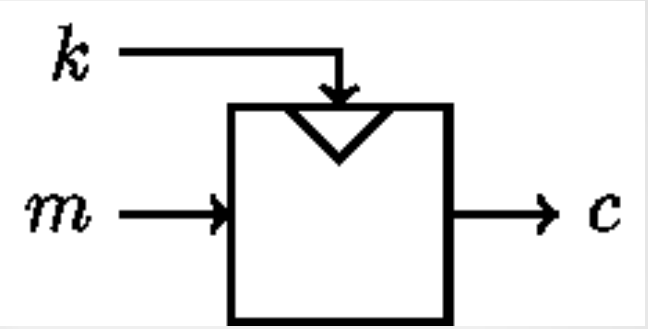
Encryption Algorithms



- We can use public key encryption algorithms like *RSA* or *El-Gamal* but they are not as fast as symmetric key encryption algorithms.
- Symmetric key encryption algorithms can be categorized into two:
  - **Block Ciphers**
  - **Stream Ciphers**
- Block ciphers divide the plaintext into **b**-bit blocks and perform a fixed transformation.
- Stream ciphers can also work on blocks or sometimes on bits but they perform a time varying transformation because they have some sort of a memory that changes during encryption.

Lesson 1: Introduction to Block Ciphers

Block Ciphers



- Block ciphers operate on **b**-bit blocks of data.
- Plaintext is divided into **b**-bit blocks.
- Each block is encrypted by a secret key **k** to produce b-bit output.
- Output blocks form the ciphertext (depends on **mode of operation**).
- Thus, a block cipher and the chosen key is actually a permutation from $\mathbf{2^b}$ elements to $\mathbf{2^b}$ elements.
- Generally **b** is 64 or 128-bit and **k** is 128, 192 or 256-bit.

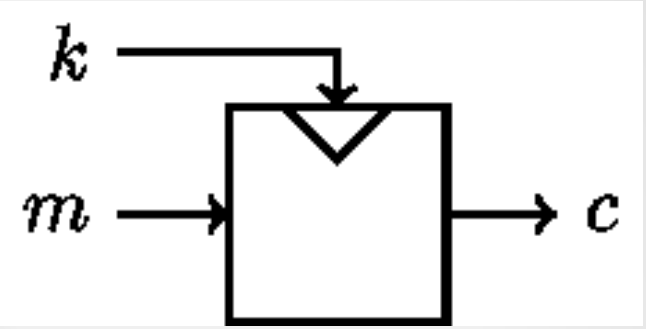
Lesson 1: Introduction to Block Ciphers

Block Cipher Design Principles

- Claude Shannon is considered as ”the father of information theory”.
- Contributed to the field of cryptanalysis for USA defense during World War II.
- His landmark paper Communication Theory of Secrecy Systems (1949) introduced the twin ideas of confusion and diffusion for practical cipher design
  - **Confusion**: ”to make the relation between the simple statistics of the ciphertext and the simple description of the key a very complex and involved one”.
  - **Diffusion**: ”the statistical structure of the plaintext which leads to its redundancy is dissipated into long range statistics in the cryptogram”.
- Note that these concepts are not measurable, absolute concepts.
- Thus, security of block ciphers are always measured as security against known cryptanalysis techniques.

Lesson 1: Introduction to Block Ciphers

Block Cipher Design

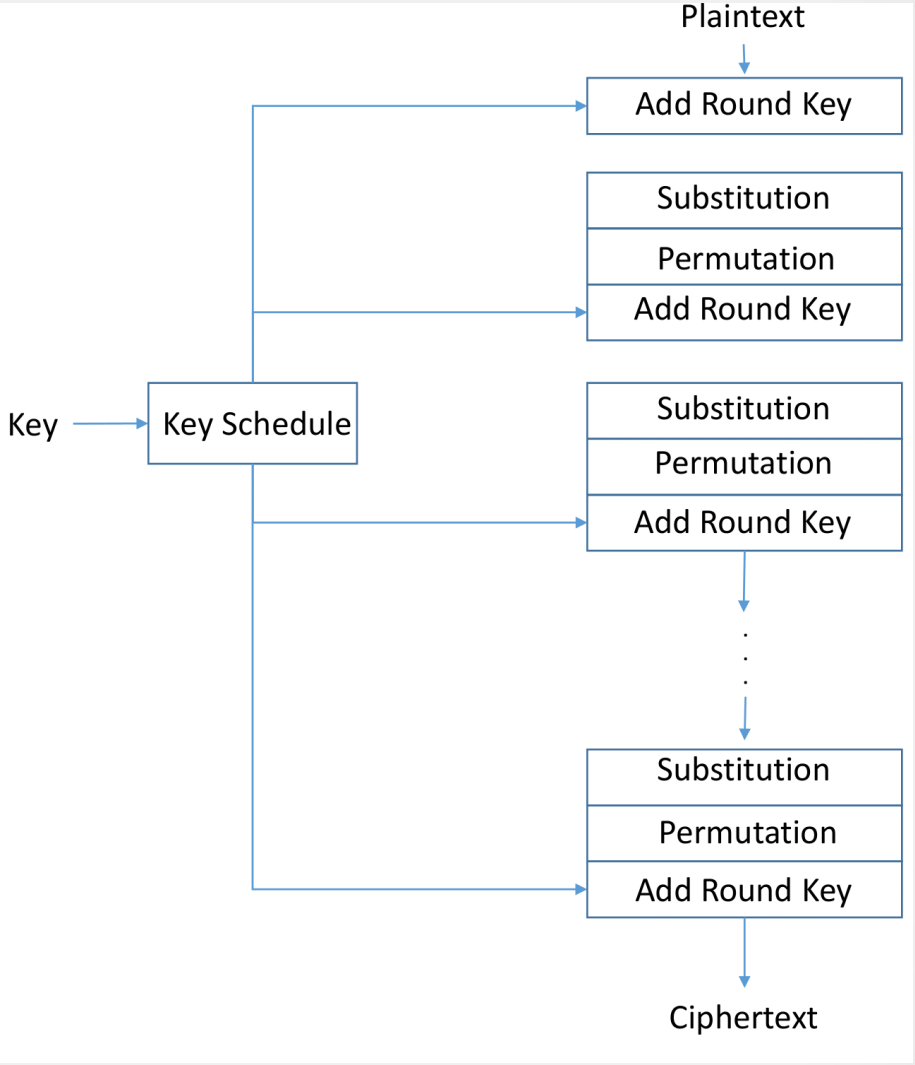


- Instead of designing a very complex cipher, generally a **round** that provides diffusion and confusion is designed and it is repeated **r** times
- Instead of using the key directly in every round, a **key schedule** algorithm is used that generate **round keys** from the secret key
- Common block cipher designs can be categorized as
  - **Substitution Permutation Network (SPN)**
  - **Feistel Network**
  - **Sponge Function / Permutation-based**

Lesson 1: Introduction to Block Ciphers

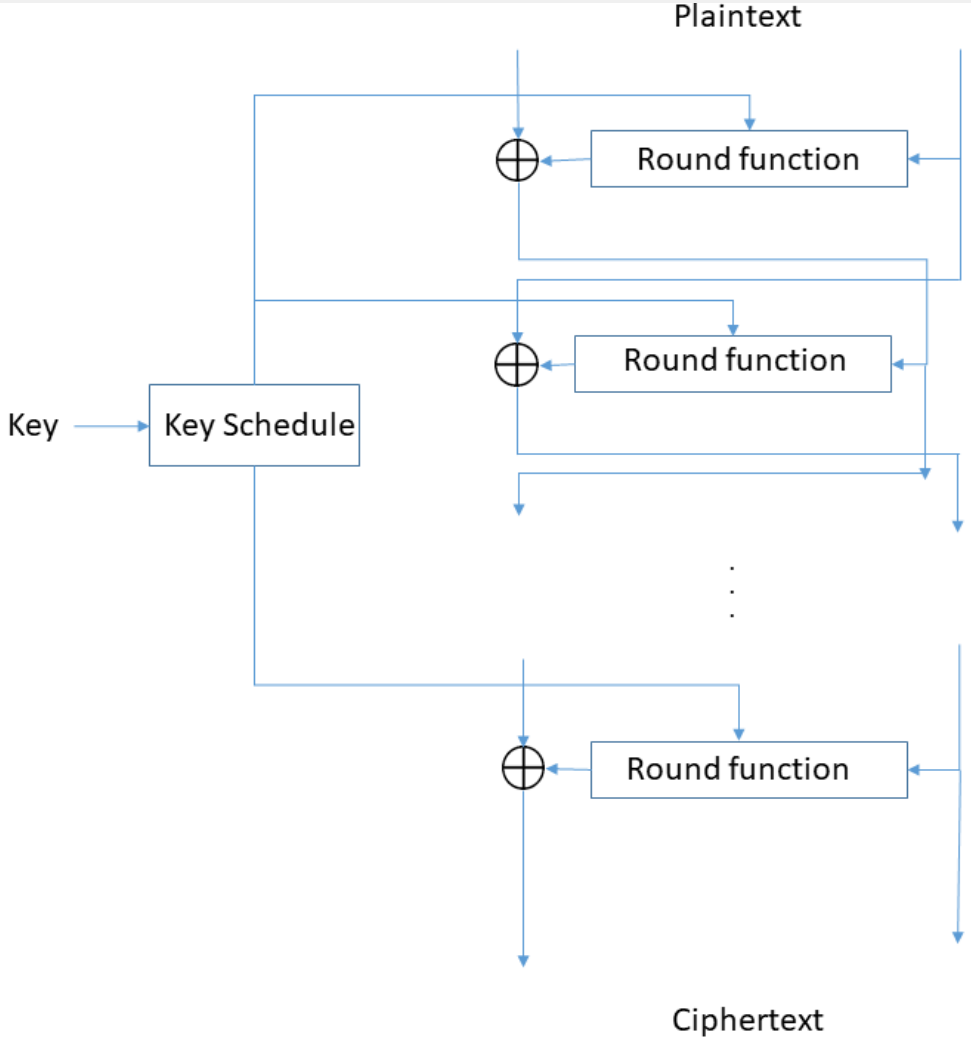
Substitution Permutation Network

- A round of an SPN consists of 3 layers
  - **Key Addition:** Combines the round key with the plaintext
  - **Substitution:** Provides confusion
  - **Permutation:** Provides diffusion
- **AES** and **PRESENT** are examples for SPN



Lesson 1: Introduction to Block Ciphers

Feistel Network



Next lecture

Introduction to Stream Ciphers

- How stream ciphers work
- Block cipher and stream cipher differences

EURO 4SEE

Thanks!

Co-funded by
the European Union

EuroHPC
Joint Undertaking

This project has received funding from the European High-Performance Computing Joint Undertaking (JU) under grant agreement No 101191697. The JU receives support from the Digital Europe Programme and Germany, Türkiye, Republic of North Macedonia, Montenegro, Serbia, Bosnia and Herzegovina.