Block Ciphers

Gaspare FERRARO
CINI Cybersecurity National Laboratory

Matteo ROSSI
Politecnico di Torino

CYBER CHALLENGE.IT

CYBERSECURITY NATIONAL LABORATORY

https://cybersecnatlab.it

License & Disclaimer

License Information

Disclaimer

- We disclaim any warranties or representations as to the accuracy or completeness of this material.
- Materials are provided “as is” without warranty of any kind, either express or implied, including without limitation, warranties of merchantability, fitness for a particular purpose, and non-infringement.
- Under no circumstances shall we be liable for any loss, damage, liability or expense incurred or suffered which is claimed to have resulted from use of this material.

Goal

- Introduce the definitions and concepts of block ciphers
- Present the functioning and vulnerabilities of the two standard block ciphers DES and AES

Prerequisites

- Lecture:
  - *CR_1.2 – XOR Cipher*

Outline

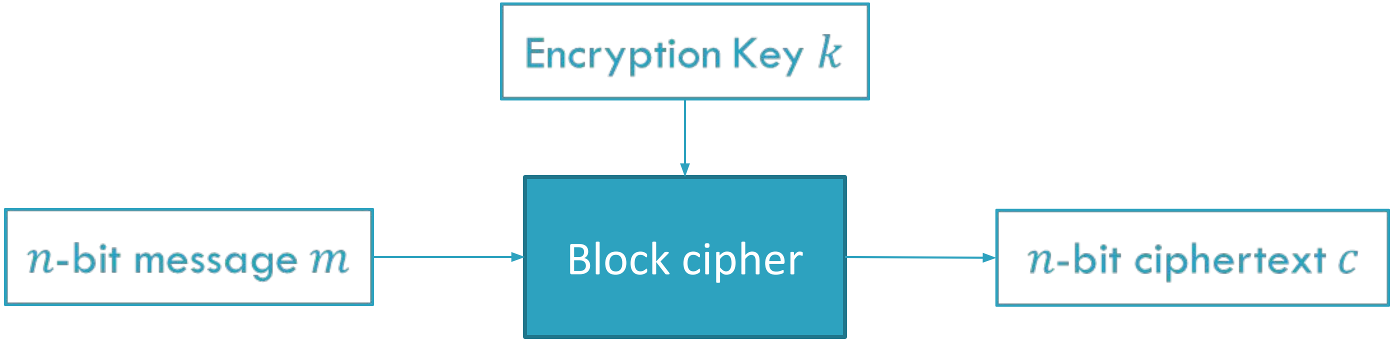
- Block Ciphers General Structure
- The Data Encryption Standard
- Weaknesses of DES and the introduction of 3DES
- The Advanced Encryption Standard

Outline

- Block Ciphers General Structure
- The Data Encryption Standard
- Weaknesses of DES and the introduction of 3DES
- The Advanced Encryption Standard

Introduction

- A *block cipher* is an algorithm that allows the encryption of blocks of *fixed length*



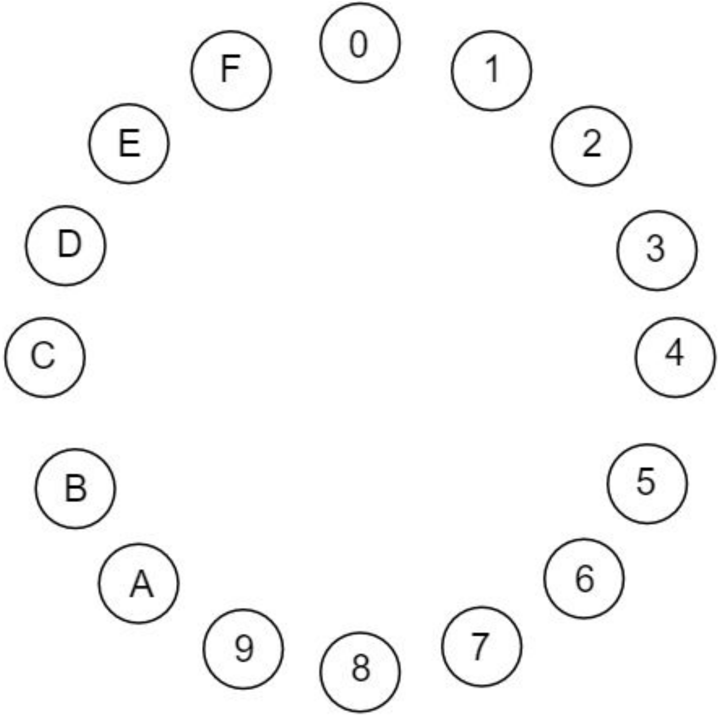
Introduction

- The length of a message is called the *blocksize* of the cipher
- *Note*: there is no strict rule on the length of the key, that in general depends on the block cipher

Keyed Permutations

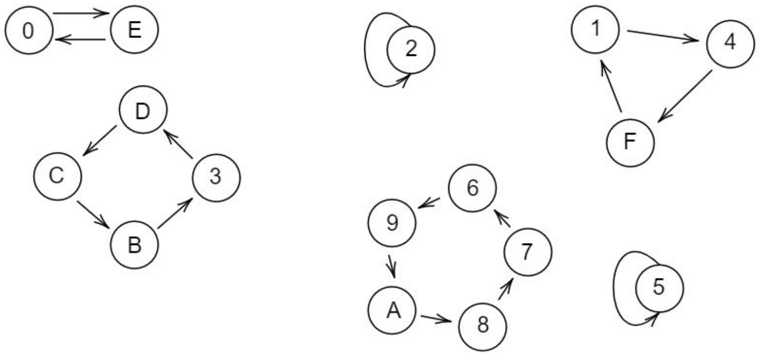
- A block cipher can be referenced in general as a *keyed permutation*, more particularly:
  - It is a *permutation* over all the n-bit strings, because it maps each possible block to some other block
  - It is *keyed* because the key determines exactly which block is mapped to which

Keyed Permutations - Example



Keyed Permutations - Example

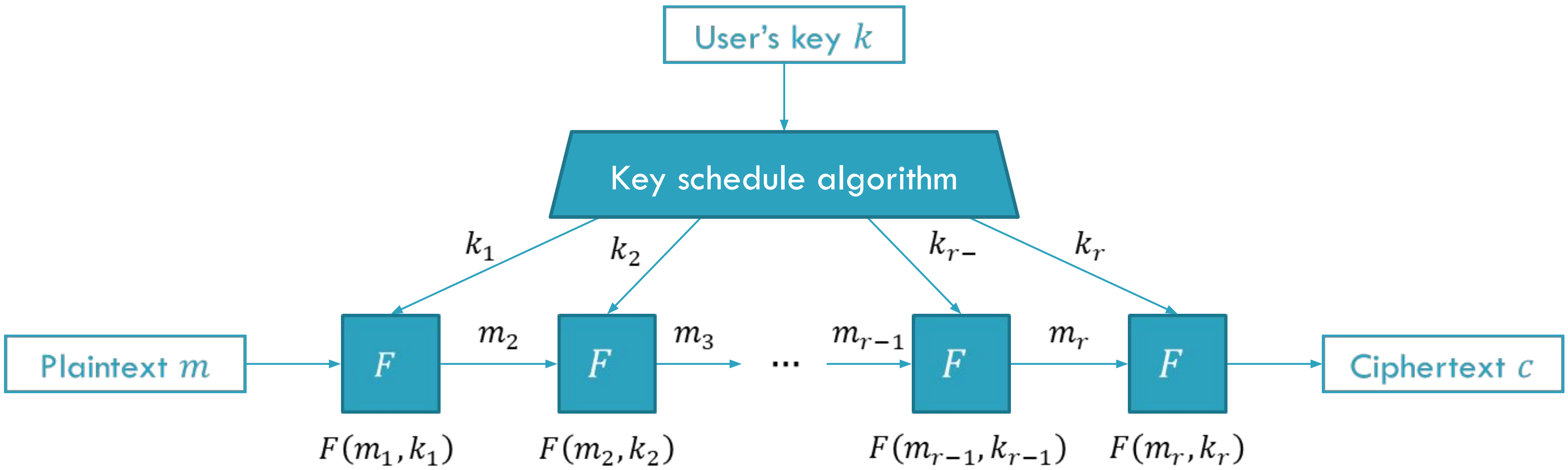
- Consider the permutation in the following image
- Here the blocksize is 4 bit (the length of a digit in hex)
- Each character of the string (block) is mapped to the new character in the direction of its arrow
- Example: the string $B75E210D$ is mapped to $365024EC$



Block Ciphers in practice

- In practice, all modern block ciphers are designed as *iterated ciphers*
- Iterated ciphers have two common components:
  - A *key schedule algorithm*, that produces r subkeys from a master key
  - A *round function* $F(message, key)$, that is iterated r times over the input message

Block Ciphers in practice



Remarks on iterated ciphers

- Does iteration enable the implementation of a secure block cipher? Nobody knows
  - There are heuristic evidences that iterating simple functions makes a cipher secure
  - Not every function is good for iteration (e.g., linear functions)
  - In general, analyzing the security of block cipher is considered a hard problem

Standard Encryption Algorithms

- In the next sections we will present:
  - the two standard block cipher algorithms *DES* and *AES*
  - their internal descriptions
  - their weaknesses

Outline

- Block Ciphers General Structure
- The Data Encryption Standard (DES)
- Weaknesses of DES and the introduction of 3DES
- The Advanced Encryption Standard

The Data Encryption Standard (DES)

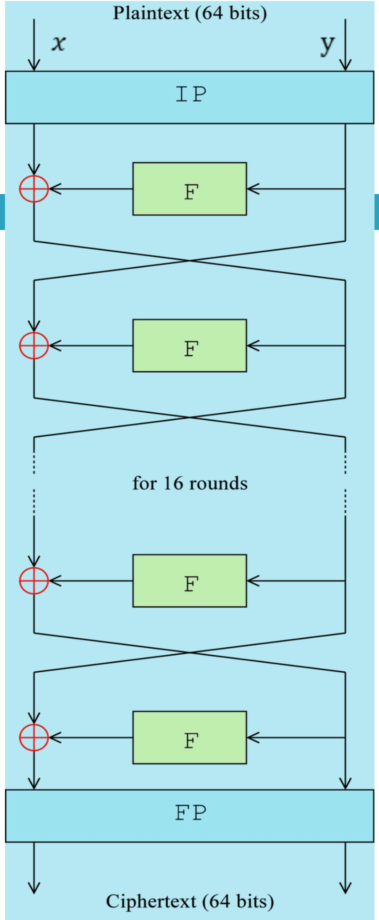
- Developed between 1973 and 1975 by IBM
- FIPS standard from 1977
- 64-bit blocks and 56-bit keys
- Broken for the first time in public in 1997
- Officially retired in 2005

DES – Overview

- The DES algorithm can be summarized as follows:
  - The key schedule algorithm produces 16 round keys of 48 bits each
  - A permutation IP (Initial Permutation) is applied to the 64-bit input
  - 16 rounds of an iterated round function are performed
  - The inverse permutation of IP, called FP (Final Permutation), is applied

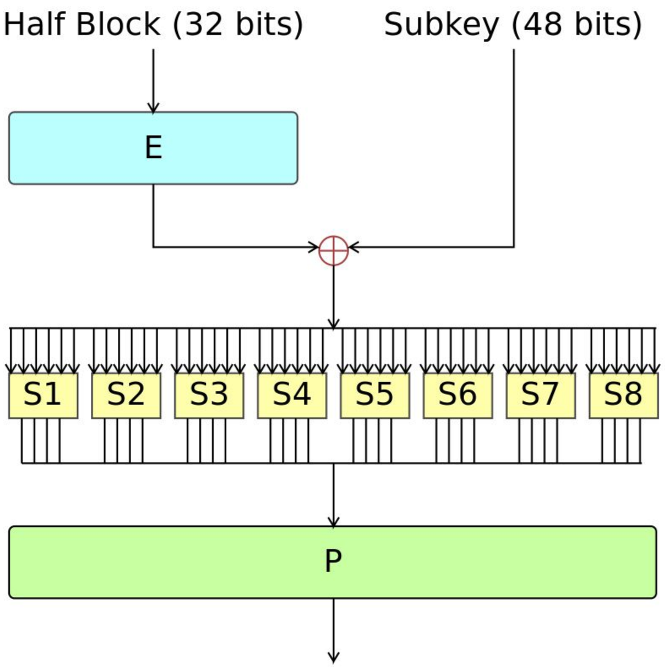
DES – Round Function

- The input is split into two blocks x and y of a same length
- A round function R is applied 16 times and has the form of:
  - $R(x, y, k) = (y, x \oplus F(y, k))$
- Where:
  - k is the round key, generated by the key schedule algorithm
  - F is a function involving substitutions, permutations and XOR, that returns a 32-bit value
  - $\oplus$ is the bitwise XOR operation
- At the end of a round we will have:
  - $(x, y) = R(x, y, k)$
- This structure is called a Feistel Network



DES – Round Function

- *The F function is composed of:*
  - *An Expansion function that maps 32 bits to 48 bits.*
  - *A XOR between the expanded block and the subkey.*
  - *8 substitution boxes (S1-S8) with 6-bit input and 4-bit output*
  - *A final Permutation*



Outline

- Block Ciphers General Structure
- The Data Encryption Standard
- Weaknesses of DES and the introduction of 3DES
- The Advanced Encryption Standard

DES – Weaknesses

- Nowadays 56-bit keys are not strong enough: with relatively-low budget, they can be bruteforced in a matter of hours.
- There are some (known) keys k, called *weak keys*, such that $E(k, E(k, m)) = m$
  - Example: alternating ones + zeros ($0x0101010101010101$)
- There are some (known) pair of keys (k_1, k_2), called *semi-weak keys* such that $E(k_2, E(k_1, m)) = m$
  - Example: $0x011F011F010E010E$ and $0x1F011F010E010E01$

DES – The introduction of 3DES

- In order to avoid bruteforce attacks, in 1995 the Triple-DES (3DES) was introduced, 3DES:
  - Takes three 56-bit keys (a 168-bit key in total) and a 64-bit messages
  - Its encryption routine is:

$$E_{3DES}(m, k_1, k_2, k_3) = E\left(k_1, D\left(k_2, E(k_3, m)\right)\right)$$

  - E and D are the encryption and decryption functions of DES
- Note: this is compatible with the standard DES by using $k_1 = k_2 = k_3$

3DES – Why not 2DES?

- Despite having 112-bit keys, 2DES is vulnerable to a Meet-in-the-Middle (MITM) attack
- Consider $E_{2DES}(k_1, k_2, m) = E\big(k_2, E(k_1, m)\big)$, it holds:
  - $E\big(k_2, E(k_1, m)\big) = C \rightarrow$
  - $D\Big(k_2, E\big(k_2, E(k_1, m)\big)\Big) = D(k_2, C) \rightarrow$
  - $E(k_1, m) = D(k_2, C)$
- We can simply precompute a table of all the 56-bit keys encryptions and use the DES decryption function to find a match
  - In this way, 2DES can be broken just in the double of time of DES by using the previous equivalence

Meet-in-the-Middle attack

- Despite having 112-bit keys, 2DES is vulnerable to a Meet-in-the-Middle (MitM) attack
- This vulnerability shows that two independent 56-bit keys does not really improve the security of the cipher, as they are equivalent of a single 57-bit key, instead of a 112-bit one, in terms of time needed the attack a ciphertext ($2 * 2^{56} = 2^{57}$)
- Note that also 3DES is vulnerable to MITM: in a similar way its security can be reduced to a single 112-bit key instead of 168!

Outline

- Block Ciphers General Structure
- The Data Encryption Standard
- Weaknesses of DES and the introduction of 3DES
- The Advanced Encryption Standard (AES)

The Advanced Encryption Standard

- In 1999 the Advanced Encryption Standard (AES) was proposed
- In 2001 AES was approved as a standard
- AES takes 128-bit messages, and has 3 versions with 128, 192, and 256-bit keys, respectively
- No (significant) vulnerability is known on the AES encryption function

AES – Structure

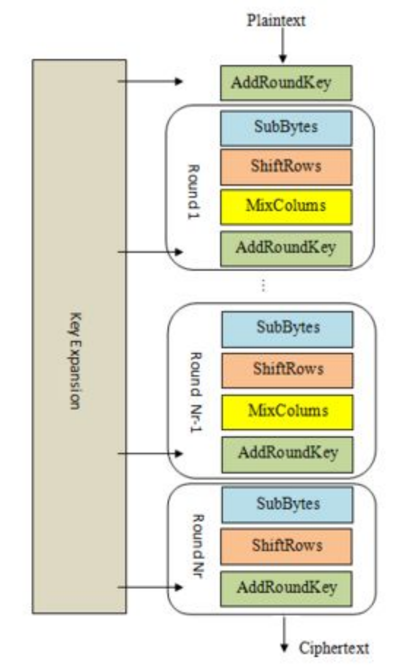
- AES is an iterated cipher but has not a Feistel structure (as DES): it is a *Substitution-Permutation Network* (SPN)
- The 3 versions of AES have 10, 12 and 14 rounds, respectively, for 128, 192, 256 bits in the key
- In principle, the different versions of AES trade-off efficiency and security

AES – Sub.-Perm. Networks

- Substitution-Permutation Networks are based on Shannon's Confusion-Diffusion principle:
  - Diffusion: changing a bit in the plaintext should result in a random change *in the whole ciphertext*. This is in general performed via permutation
  - Confusion: like diffusion, but for the key-ciphertext relation; in general, obtained using substitutions

AES – General Structure

- In AES, the 16-bytes plaintext is arranged in a 4×4 matrix called the *state matrix*
- The Key Expansion algorithm generates $N_r + 1$ *keys* (where N_r is the number of rounds), each as a 4×4 matrix

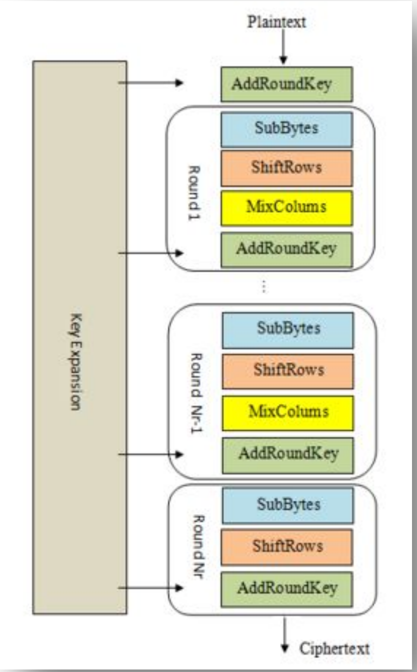


AES – Round Structure

- AES has 4 major components in the round function:
  - *AddRoundKey*: an element-wise XOR between the state matrix and the round key matrix
  - *SubBytes*: an element-wise substitution using a (fixed) table on the state matrix
  - *ShiftRows*: a cyclical shift of the rows of the state matrix
  - *MixColumns*: a (sort of) matrix multiplication of the state matrix with a fixed matrix

AES – Remarks

- By design, MixColumns is always omitted in the last round
- Confusion is obtained via the SubBytes operation
- Diffusion is obtained with the combination of ShiftRows and MixColumns



What next

- In the next lecture:
  - Using block ciphers to encrypt more than one block (modes of operation)
  - Common mistakes and vulnerabilities in implementing block ciphers
  - Stream ciphers and their relationship with block ciphers
  - Basic vulnerabilities of stream ciphers

Block Ciphers

Gaspare FERRARO
CINI Cybersecurity National Laboratory

Matteo ROSSI
Politecnico di Torino

CYBER CHALLENGE.IT

CYBERSECURITY NATIONAL LABORATORY

https://cybersecnatlab.it