CYBER CHALLENGE
CyberChallenge.IT

cini
Cybersecurity National Lab

SPONSOR PLATINUM

accenturesecurity

aizoon AUSTRALIA EUROPE USA
TECHNOLOGY CONSULTING

B5

EY Building a better working world

eni

exprivia | ITALTEL

IBM

KPMG

LEONARDO

NTT DATA
Trusted Global Innovator

NUMERA
SISTEMI E INFORMATICA S.p.A.

Telsy

SPONSOR GOLD

bip.

cisco

MONTE DEI PASCHI DI SIENA
BANCA DAL 1472

negg

NOVANEXT
connecting the future

pwc

SPONSOR SILVER

DiGi ONE
the leading digital company

ICT CYBER CONSULTING

Symmetric encryption and block ciphers

Rocco DE NICOLA
IMT Lucca

CYBER CHALLENGE
CyberChallenge.IT

cini
Cybersecurity
National Lab

https://cybersecnatlab.it

License & Disclaimer

License Information

Disclaimer

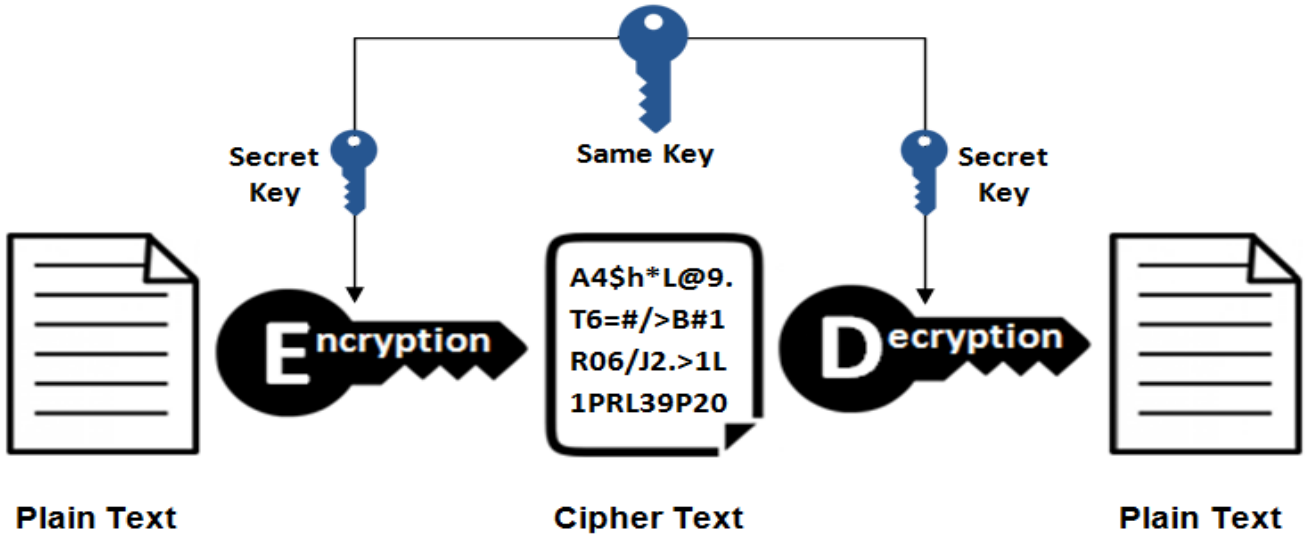
- We disclaim any warranties or representations as to the accuracy or completeness of this material.
- Materials are provided “as is” without warranty of any kind, either express or implied, including without limitation, warranties of merchantability, fitness for a particular purpose, and non-infringement.
- 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.

Outline

- The shared key models
- Stream Encryption
- Block Encryption
- Feistel Cipher
- Data Encryption Standard (DES)
- Variants of DES

Symmetric key cryptography

- Requires that both sender and recipient know the same key.
- An issue is how they do share it without meeting.



Block vs Stream Ciphers

- Block ciphers process messages into blocks, each of which is then encrypted or decrypted
  - Essentially a polyalphabetic substitution technique with a very big characters set (64-bits or more) paired with permutation techniques
- Stream ciphers process messages a bit or byte at a time when encrypting or decrypting
  - An approximation of one-time pad (OTP);
  - The keystream is combined with the plaintext using exclusive or (XOR)
- Many current ciphers are based on block cipher techniques
  - Better analysed and with broader range of applications

Stream Ciphers

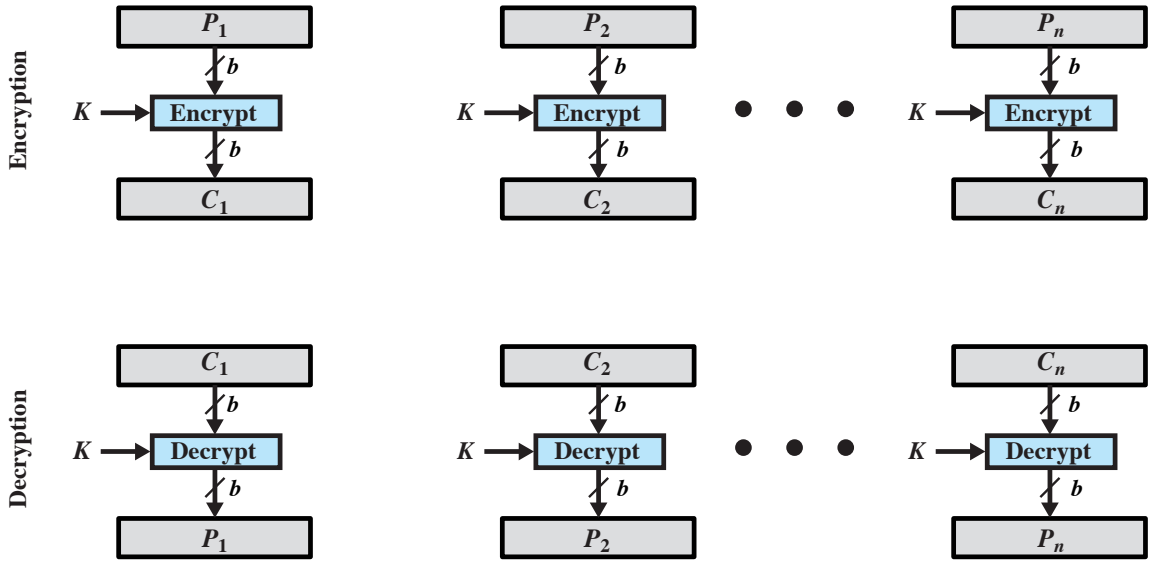
- Stream Ciphers encrypt a digital data stream one bit or one byte at a time
- Plaintext digits are combined (XOR-ed) with a pseudorandom cipher digit stream (keystream) to get a digit of the cipher text stream
- The bit stream generator is an algorithmic procedure employed by both communication peers to produce the cryptographic bit stream used to encrypt or decrypt.
- To guarantee robustness it must be computationally impractical to predict future portions of the bit stream knowing its previous portions
- The two peers, to produce the key stream, need only share the generating key

Block Ciphers

- A block cipher operates on a plaintext block of n bits to produce a ciphertext block of n bits.
- A block of plaintext is treated as a whole and used to produce a ciphertext block of equal length
- Typical block sizes of 64 or 128 bits are used (n = 64 or 128)
- Users share a symmetric encryption key
- There are 2^n possible different plaintext blocks and, for the encryption to be reversible, each must produce a unique ciphertext block.

Block Ciphers

A given plaintext of n*b length is divided into b blocks of n bits



Each block is encrypted using the same algorithm and the same key, to produce a sequence of b blocks of n-bits of ciphertext.

Block Ciphers - transformation

- Block ciphers are based on the idea of encrypting by mapping a sequence of n-bits in a different sequence of the same length.
- To decipher and obtain the original plaintext, the map must be reversible.
- Below there are a reversible and an irreversible mapping for n = 2

Reversible Mapping

Plaintext	Ciphertext
00	11
01	10
10	00
11	01

Irreversible Mapping

Plaintext	Ciphertext
00	11
01	10
10	01
11	01

From: W. Stalling: Cryptography and Network Security, Int'l Edition, Pearson

Block Ciphers - Transformation

- A 4-bit block produces 16 input configurations that can be (reversibly) mapped to any of the 16 output configurations.
- One of the possible mapping is reported on the right.
- The shared (64 bit) key is the cyphertext column

Plaintext	Ciphertext
0000	1110
0001	0100
0010	1101
0011	0001
0100	0010
0101	1111
0110	1011
0111	1000
1000	0011
1001	1010
1010	0110
1011	1100
1100	0101
1101	1001
1110	0000
1111	0111

Issues with Block Ciphers

- Small blocks are subject to frequency analysis
- Large blocks give rise to many possible pairings and thus to very long keys (the cyphertext column is the key!).
- For a 4 bits block like the one on the right the key is 64 bits long
- For a block of n bits the key is n x 2^n long and thus for an ideal block of 64 bits a key of about 10^{21} bits is needed.
- Variants of the ideal block cipher that mix permutations and replacements are on demand!

Plaintext	Ciphertext
0000	1110
0001	0100
0010	1101
0011	0001
0100	0010
0101	1111
0110	1011
0111	1000
1000	0011
1001	1010
1010	0110
1011	1100
1100	0101
1101	1001
1110	0000
1111	0111

Feistel's cipher

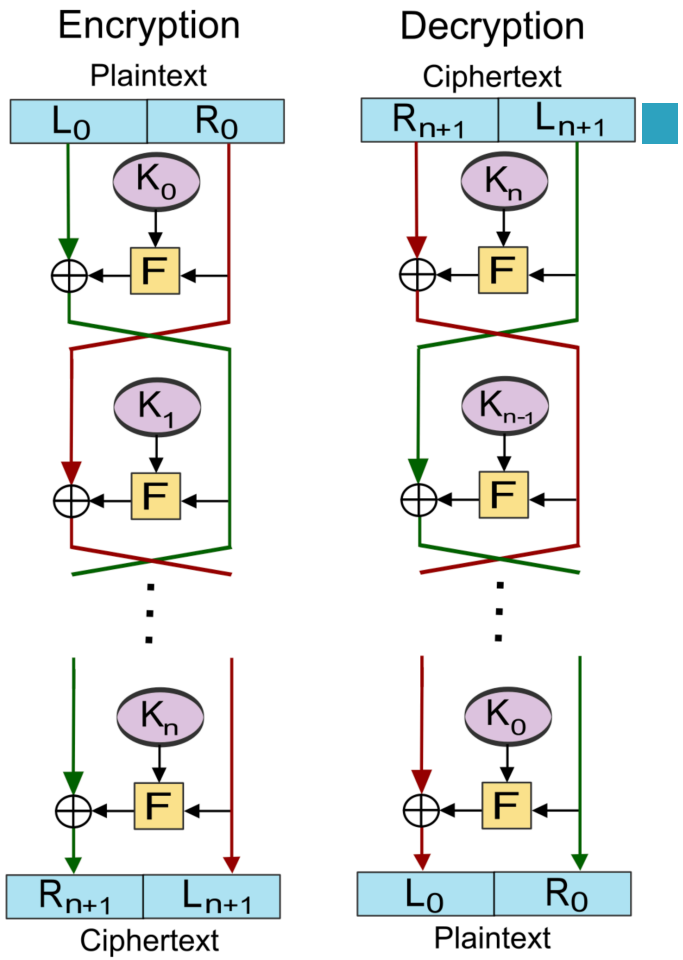
- Many block ciphers, including the well known Data Encryption Standard (DES) use Feistel's cipher
- Encryption and decryption operations are similar, in some cases identical, only keys are used in reverse order.
- Relies on reversible product cipher: combination of simple transformations such as substitution (S-box), permutation (P-box), and on modular arithmetic.
- Implements Shannon's Substitution and Permutation network concept by partitioning input blocks into two halves and going through multiple rounds

Feistel's cipher: principles

- Techniques:
  - Substitution: Each plaintext element or group of elements is uniquely replaced by a corresponding ciphertext element or group of elements
  - Permutation: No element is added or deleted or replaced in the sequence, rather the order in which the elements appear in the sequence is changed
- Shannon's Principles:
  - Diffusion: dissipates the statistical structure of plaintext over the bulk of the ciphertext
  - Confusion: each bit of the ciphertext depends on several parts of the key, obscuring the connections between the two.

Feistel's cipher

- Feistel ciphers are a special class of iterated block ciphers where the ciphertext is calculated from the plaintext by repeated application of the same transformation or round function.
- The text being encrypted is split into two halves. The round function F is applied to one half using a subkey and the output of F is XOR-ed with other half.
- The two halves are then swapped. Each round follows the same pattern except for the last round there is no swap
- Encryption and decryption are structurally identical, but the subkeys used during encryption at each round are taken in reverse order during decryption



Feistel's cipher: design features

- Block size: Larger block sizes mean greater security but reduced enc/decryption speed
- Key size: Larger key size means greater security but decreases en/decryption speed
- Number of rounds: A single round offers inadequate security; multiple rounds offer increasing security. A typical size is 16 rounds.
- Subkey generation algorithm: Greater complexity in this part of the algorithm leads to greater difficulty of cryptanalysis
- Round function F: Greater complexity means greater resistance to cryptanalysis
- Fast software encryption/decryption: If encrypting is embedded in applications, hardware implementations are impossible and good software is needed
- Ease of Analysis: Concisely and clearly algorithms are easier to analyze for cryptanalytic vulnerabilities and guarantee for its strength

DES (Data Encryption Standard)

Symmetric block with 64-bit blocks and 64-bit keys, of which only 56 bits are used (the remaining 8 serve as parity checks)

- In 1973, the National Bureau of Standards (NBS) published a "call for proposals" and IBM proposed a system similar to its product "Lucifer" based on Feistel Cipher.
- Shortly afterwards NSA certified Lucifer as DES and after some investigations DES was certified and made public in 1977.
- First example of a robust (NSA-certified) cipher that could be analyzed.
- Robusteness has been certified almost every 5 years, since then.

Basic ingredients of DES

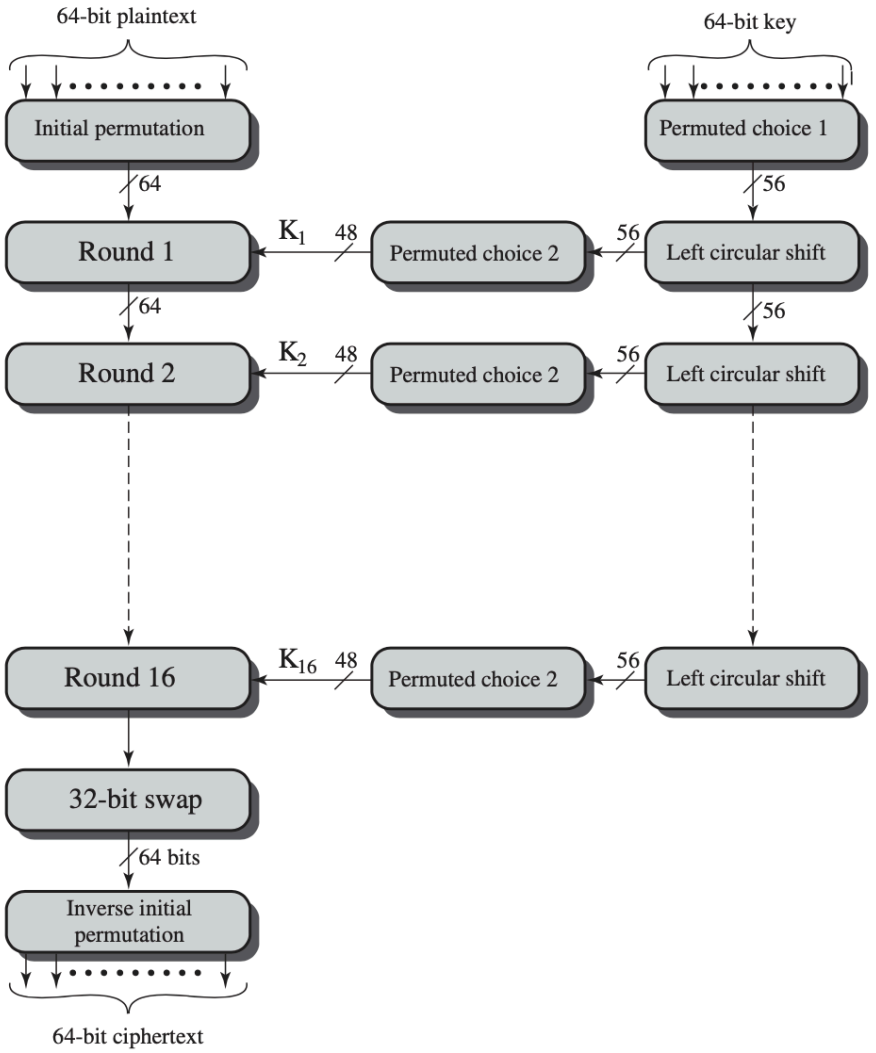
- Permutation: One bit of input determines one bit of output.
- Substitution: One block of input bits replaced by a unique block of output bits.
- Expansion: Certain bits of the input are repeated multiple times in the output.
- Choice (contraction); Certain input bits do not appear int the output (they are ignored).
- Circular shift (left or right): 48 bits of the 56-bit key are circularly selected and used.

DES Algorithm

- Take the 64-bit block of message (M) and the 64-bit key
- Rearrange the bits of M (Initial Permutation - IP).
- Split IP into two 32-bit blocks (L & R).
- Shift the key bits and take a 48-bit portion from the key.
- Save the value of R into R_{old}.
- Expand R via a permutation to 48 bits.
- XOR R with the 48-bit key and transform via eight S-boxes into a new 32-bit chunk.
- R takes on the value of the new R XOR-ed with L.
- L takes on the value of R_{old}.
- Repeat this process 15 more times (total 16 rounds).
- Join L and R.
- Reverse the permutation IP (final permutation, FP).

DES (Data Encryption Standard)

- It uses 56-bit keys, divides plaintext into 64-bit blocks, performs initial and final permutations and a cycle of 16 iterations of permutations and xor (Feistel network, confusion and diffusion techniques).
- The key is actually 64 bits, of which only 56 of are significant and 48 bits are used at each round.
- The algorithm originally had a 128-bit key, but the size of the key was reduced by NSA (for some reason)



W. Stalling: Cryptography and Net - work Security, Int'l Edition, Pearson

Weaknesses of DES

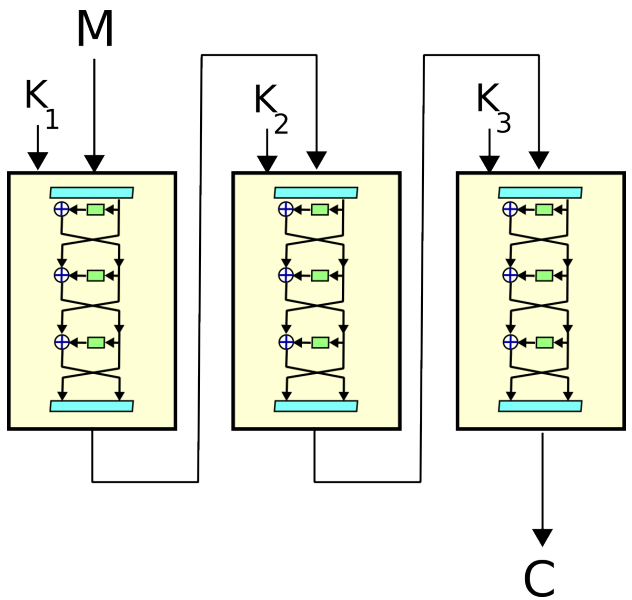
- DEA the algorithm behind DES (with its variants Triple DES and Advanced ES) is the most studied encryption algorithm.
- Despite numerous attempts, no one has so far reported a fatal weakness in the algorithm.
- But with a 56-bit key, there are 2^{56} ($\cong 7{,}2 * 10^{16}$) possible keys, which, with today computers, is breakable
- *The Electronic Frontier Foundation (EFF) announced in July 1998 that it had broken a DES encryption.*
- *If the only form of attack to an encryption algorithm is brute force, then "use longer keys!"*

After DES

- As of 1999, DES is considered insecure due to its short key size
- More-recent symmetric ciphers that have replaced DES are:
  - Triple-DES — effectively triples the DES key size
  - Blowfish — variable key sizes from 32 bits up to 448 bits
  - International Data Encryption Algorithm (IDEA) —128-bit keys
  - Advanced Encryption Standard (AES) — key sizes of 128, 192 or 256 bits

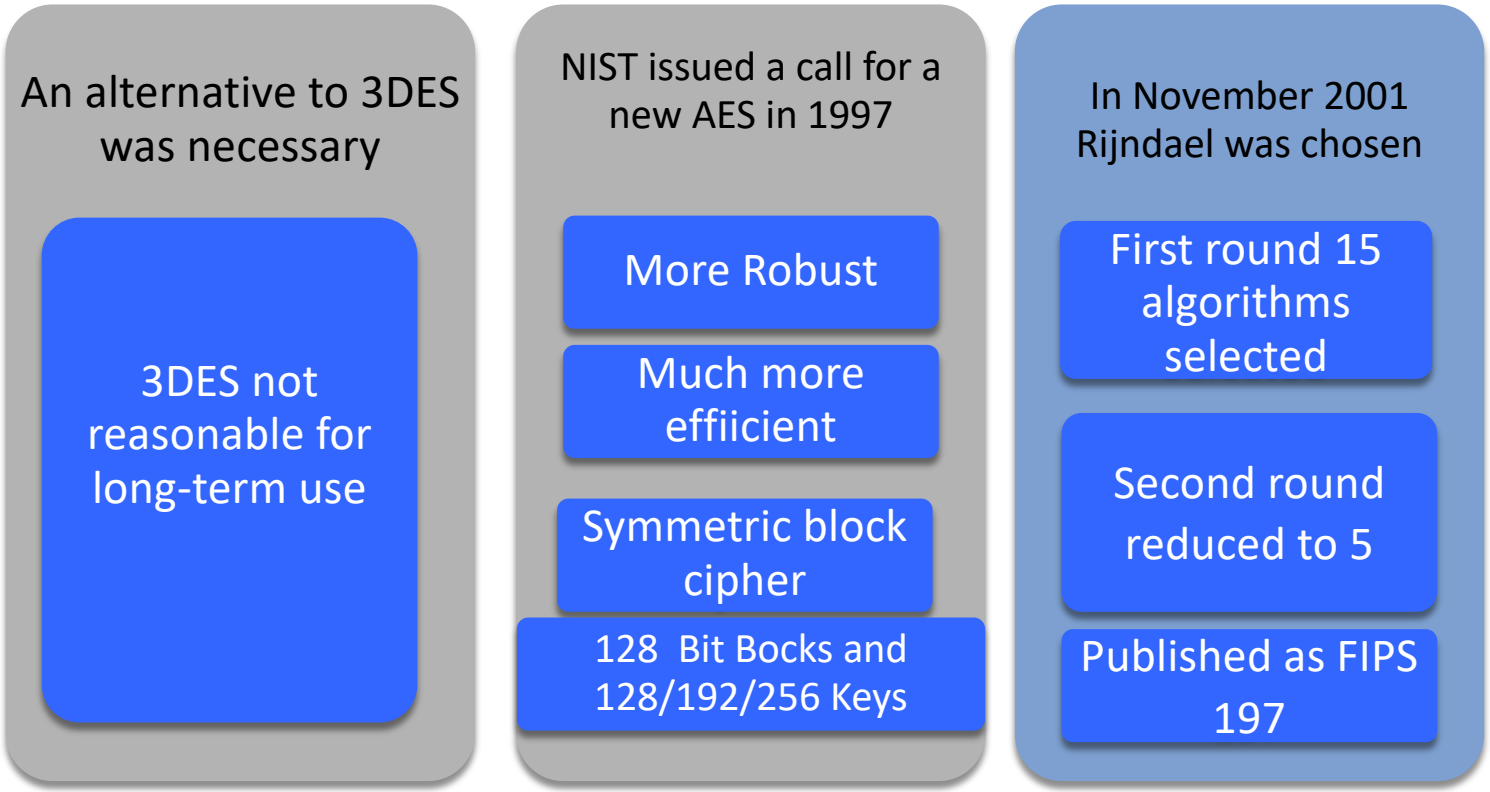
Triple DES (3DES)

Repeats the basic DES algorithm three times using one, two or three keys, for a key size of 168 bits



- With 3 keys, the robustness against brute force attacks increases.
- But it does not support efficient software coding
- Uses 64-bit blocks (but for robusteness larger blocks would be better)

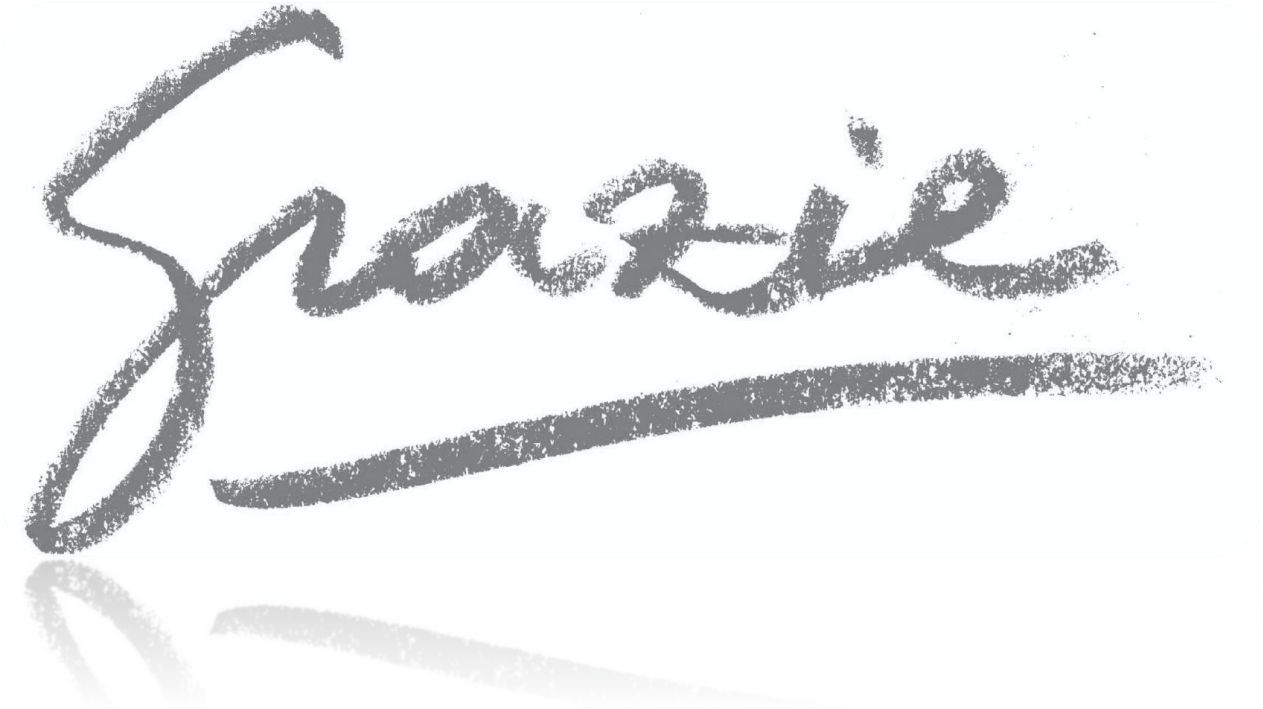
Advanced Encryption Standard (AES)



 Rel. 10.03.2020

Time needed for attacks

Key size (bits)	Cipher	Number of Alternative Keys	Time Required at 10^9 decryptions/sec Personal Computer	Time Required at 10^{13} decryptions/sec Super Computer
56	DES	$2^{56} \approx 7.2 \times 10^{16}$	2^{55} ns = 1.125 years	1 hour
128	AES	$2^{128} \approx 3.4 \times 10^{38}$	2^{127} ns = 5.3×10^{21} years	5.3×10^{17} years
168	Triple DES	$2^{168} \approx 3.7 \times 10^{50}$	2^{167} ns = 5.8×10^{33} years	5.8×10^{29} years
192	AES	$2^{192} \approx 6.3 \times 10^{57}$	2^{191} ns = 9.8×10^{40} years	9.8×10^{36} years
256	AES	$2^{256} \approx 1.2 \times 10^{77}$	2^{255} ns = 1.8×10^{60} years	1.8×10^{56} years



CYBER CHALLENGE
CyberChallenge.IT

 Rel. 10.03.2020

cini
Cybersecurity National Lab

CYBER CHALLENGE
CyberChallenge.IT

cini
Cybersecurity National Lab

SPONSOR PLATINUM

accenturesecurity

aizoon AUSTRALIA EUROPE USA
TECHNOLOGY CONSULTING

B5

EY Building a better working world

eni

exprivia | ITALTEL

IBM

KPMG

LEONARDO

NTT DATA
Trusted Global Innovator

NUMERA
SISTEMI E INFORMATICA S.p.A.

Telsy

SPONSOR GOLD

bip.

cisco

MONTE DEI PASCHI DI SIENA
BANCA DAL 1472

negg

NOVANEXT
connecting the future

pwc

SPONSOR SILVER

DiGi ONE
the leading digital company

ICT CYBER CONSULTING