Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

# Symmetric Encryption

***Facilitating GDPR compliance for SMEs and promoting Data Protection by Design in ICT products and services*** *([www.bydesign-project.eu](http://www.bydesign-project.eu))*

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

ΚΕΝΤΡΟ ΕΡΕΥΝΩΝ ΠΑΝΕΠΙΣΤΗΜΙΟΥ ΠΕΙΡΑΙΩΣ

ICT abovo Information & Communication Technologies

*This presentation has been based on material provided by Dr. K. Limniotis (HDPA)*

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

# Cryptography is present in…

- Surfing the Internet (see https)
- Mobile communications
- Wireless networks (802.11x, Bluetooth, …)
- Electronic payments
- Electronic mail
- Enterprise security
- Military networks
- E-voting
- Teleconferences (VoIP applications)
- Virtual Private Networks (VPN)
- Cryptocurrency (Bitcoin,…) – Distributed Ledger Technology
- Internet of Things – IoT
- eHealth applications

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

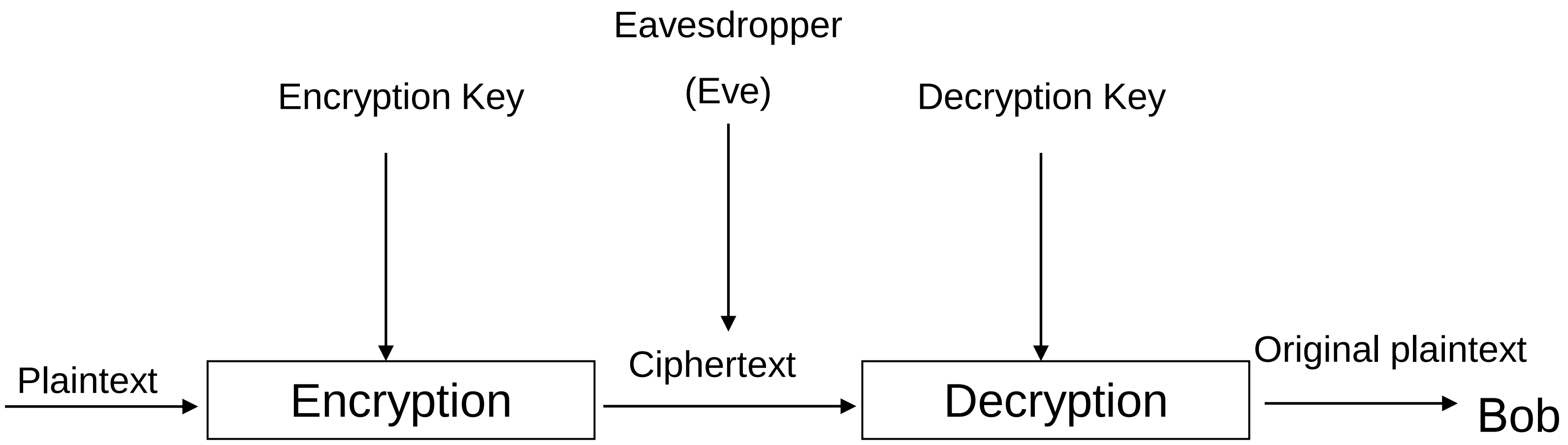
# Basic Terminology

- **plaintext** - the original message
- **ciphertext** - the coded message
- **cipher** - algorithm for transforming plaintext to ciphertext
- **key** - info used in cipher known only to sender/receiver
- **encipher (encrypt)** - converting plaintext to ciphertext
- **decipher (decrypt)** - recovering ciphertext from plaintext
- **cryptography** - study of encryption principles/methods
- **cryptanalysis (codebreaking)** - the study of principles/ methods of deciphering ciphertext without knowing key
- **cryptology** - the field of both cryptography and cryptanalysis

Το έργο χρηματοδοτήθηκε από το
Πρόγραμμα Δικαιώματα,
Ισότητα και Ιθαγένεια 2014-2020
της Ευρωπαϊκής Ένωσης

# Key-based ciphers

- Ciphers use one (or more) keys.




- The security rests with the secrecy of the key – the encryption and decryption algorithms can be publically known (Kerchoff's principle).

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

# Types of Cryptographic Algorithms

- Symmetric (or private) key algorithms
  - The same key is being used for both encryption and decryption
  - Examples: AES, DES, 3DES, RC4, …
- Asymmetric (or public key) algorithms
  - The decryption key is different from the encryption key
  - A totally different underlying idea from the symmetric cryptography
  - Examples RSA, Ellliptic curve cryptography, …

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

# A Mathematical Formulation

If E and D denote the encryption and decryption respectively, then:

- $E_{K1}(m) = c$
- $D_{K2}(c) = m$

where m and c are the plaintext and the ciphertext respectively.

The indexes Ki imply that the results are dependent on the key each time.

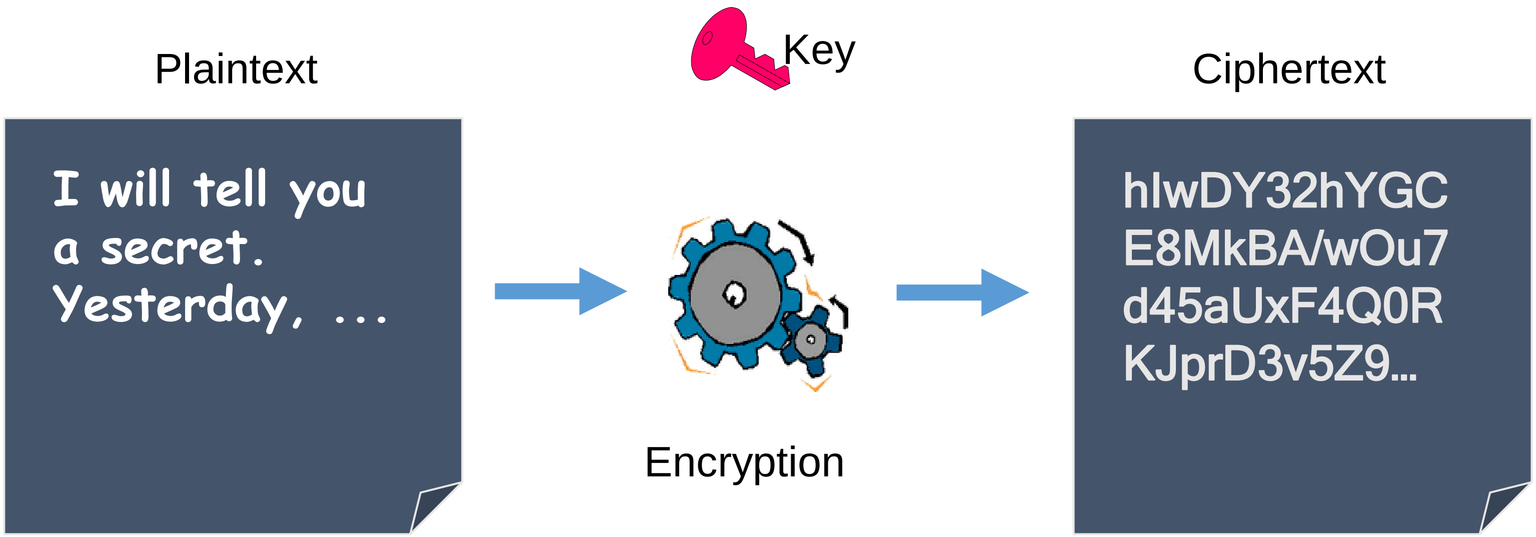
The following property holds:

$$D_{K2}(E_{K1}(m)) = m$$

In symmetric-key ciphers, we have K1 = K2

# Symmetric encryption

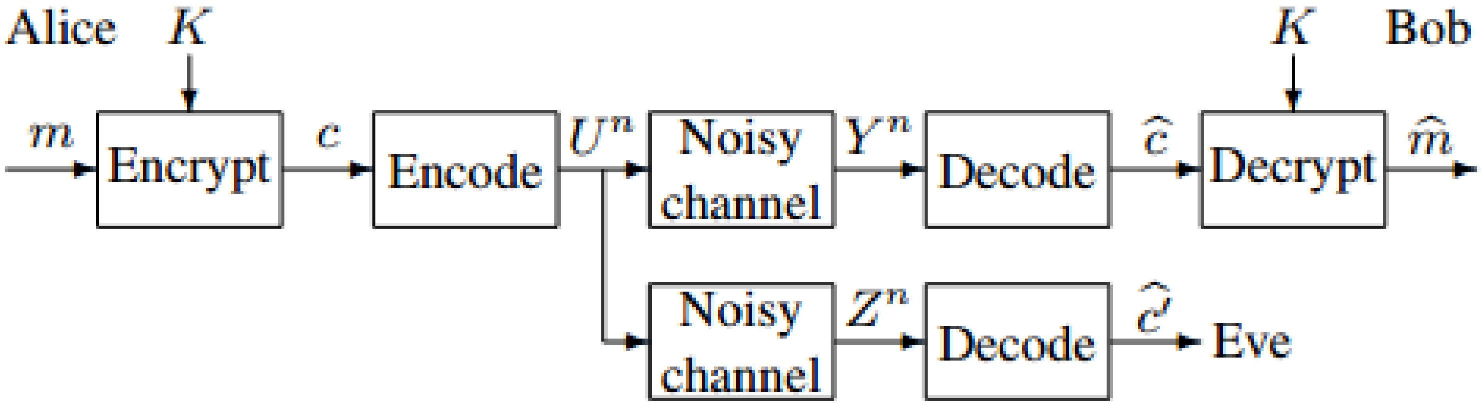
- The security rests with the secrecy of the key – the encryption and decryption procedures (algorithms) are public!



Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

# Encryption in a telecommunications channel

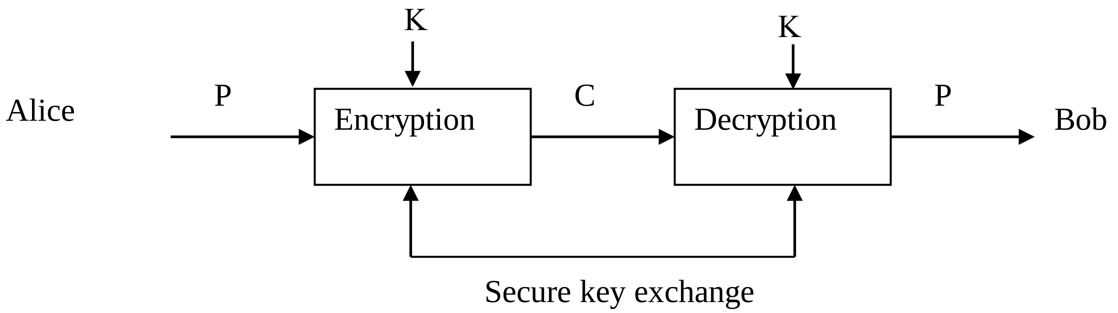
- Typical case: the message is encrypted and subsequently encoded (error-control coding), to  detect/correct errors introduced by the channel
- However, there are also other options:
  - Encryption after the error control coding
  - Simultaneous encryption and error-control coding
    - Physical-layer encryption



Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

# How to securely exchange the secret key?

- A «secure channel» is needed for performing key exchange
  - Great challenge – if a secure channel was in place, then we would not need encryption at all



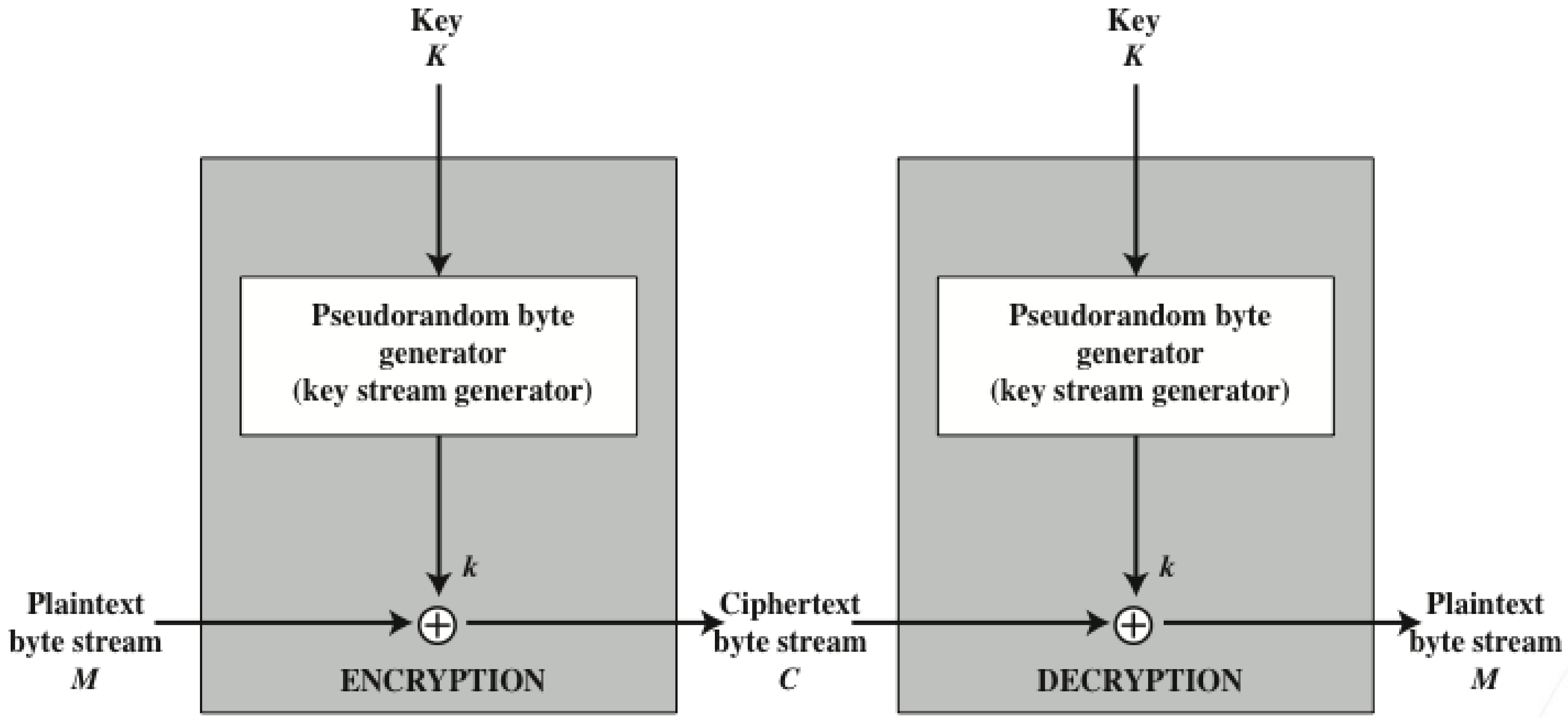
Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

# Defining the strength of a cipher

- **Unconditional security**
  - no matter how much computer power is available, the cipher cannot be broken since the ciphertext provides insufficient information to uniquely determine the corresponding plaintext
- **Computational security**
  - given limited computing resources (e.g. time needed for calculations is greater than age of universe), the cipher cannot be broken

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

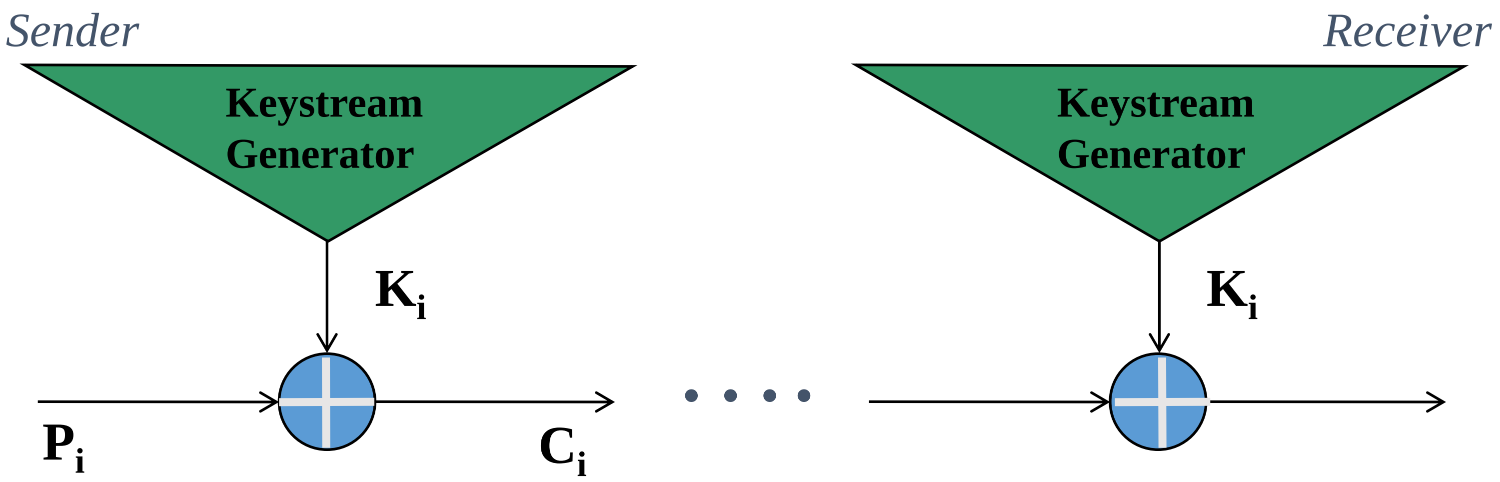
# Stream Ciphers




They try to resemble the one-time pad

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

# A typical case of a stream cipher




- Encryption is being performed bit-by-bit (or byte-by-byte)
  - A keystream generator is being used, to produce a "random" sequence (keystream)
  - Keystream bits are being XOR-ed with the bits of the plaintext, so as to produce the ciphertext
  - Encryption: $C_i = P_i \oplus K_i$
- The decryption is similarly performed (the recipient has the same keystream generator, producing the same keystream):
  - Decryption: Pi = Ci ⊕ Ki
- Example: For keystream 00110010….. and plaintext 11000110, the ciphertext will be 11110100

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

# Applications of stream ciphers

- Suitable in applications with memory and power restrictions, as well as with requirements for high speed
- Examples
  - WiFi networks
  - (Older) Mobile communications (GSM, 3G)
  - Bluetooth
  - RFID networks
  - <u>IoT</u>
- Also used in Web (RC4, ChaCha20)

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

# Known stream ciphers

- Probably the most known is RC4
- Used for more that 2 decades in several applications
  - WEP, WPA, TLS, …
- However, some weaknesses were known
  - Some non-random properties of the keystream, etc.
  - For vulnerabilities of RC4 in Microsoft Office products, see https://www.schneier.com/blog/archives/2005/01/microsoft_rc4_f.html
- RC4 found insecure in 2013, with regard to the security protocol SSL/TLS
  - For more information: http://www.isg.rhul.ac.uk/tls/
- Later on, several other weaknesses have been found out (https://www.rc4nomore.com/)
- Not is it well-known that RC4 should not be used
- RFC 7465 (February 2015): RC4 is considered to be “on the verge of becoming practically exploitable...[and] can no longer be seen as providing a sufficient level of security for TLS sessions.”
- In TLS 1.3 (latest version), RC4 has been replaced by Chacha20

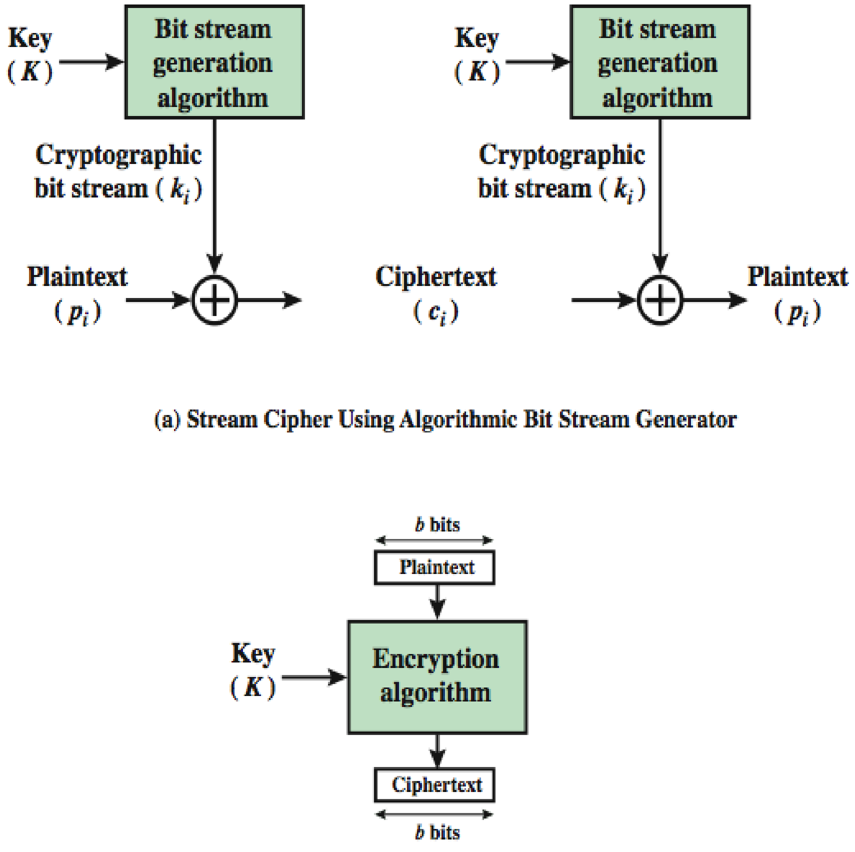
Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

# The RC4 cipher

- Variation in key sizes
  - From 40 up to 256 bits
- The keystream generator is mainly based on a register S with 256 entries, which initially contains the numbers from 0 to 255 in an ordered fashion (each entry corresponds to 1 byte = 8 bits)
- Based on the key, the entries of S are being permuted
- The keystream is being obtained by a specific rule (described next), based on this permutated version of the register

# From stream ciphers to block ciphers

- Block ciphers perform encryption on a block (and not on a bit) basis
- Encryption is much more complex than a simple XOR addition



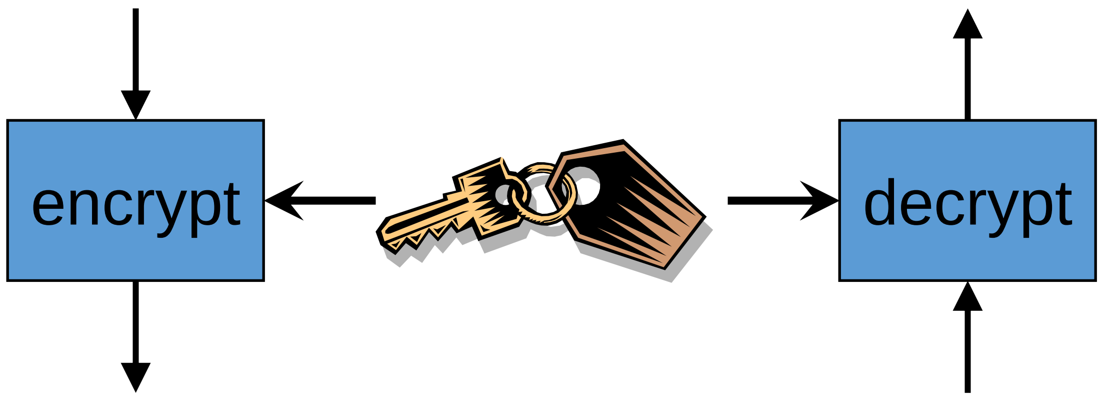

(b) Block Cipher

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

# Block ciphers

- The initial message is being “splitted” into blocks of fixed size, whereas each block is being encrypted separately
  - Typical size of block: 128 bits
- Encryption (and decryption) is a complex operation over the input block

Block of plaintext, of length n




Block of ciphertext, of length n

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

# Motivation

- A block cipher operates on a block of n bits.
- It produces a ciphertext block of n bits.
- There are $2^n$ possible different plaintext/ciphertext blocks.
- The encryption must be reversible. i.e.
  - decryption to be possible.
  - each plaintext must produce a unique ciphertext block. (one-to-one correspondence)

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

# Reversible vs. Irreversible

**Reversible Mapping**

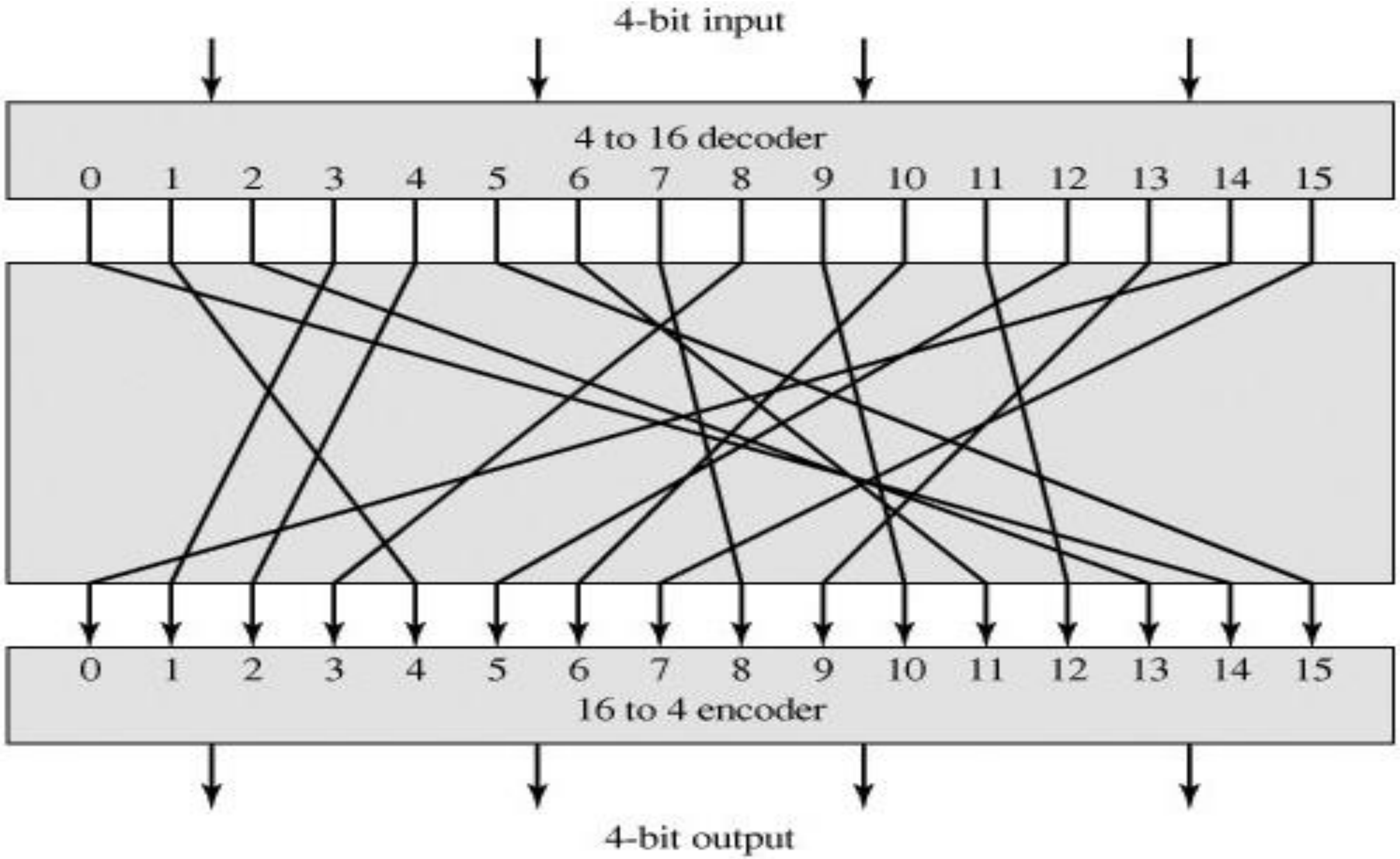
| Plaintext | Ciphertext |
|---|---|
| 00 | 11 |
| 01 | 10 |
| 10 | 00 |
| 11 | 01 |

**Irreversible Mapping**

| Plaintext | Ciphertext |
|---|---|
| 00 | 11 |
| 01 | 10 |
| 10 | 01 |
| 11 | 01 |

# Ideal Block Cipher
# (a general substitution cipher)





Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

# Encryption/Decryption Table for Substitution Cipher

| 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 |

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

# Problems with Ideal Cipher

- If a small block size, such as n = 4, is used, then the system is equivalent to a classical substitution cipher → Easy attack (statistical analysis of the plaintext)
- If large block size is used → not practical (for implementation and performance)
  - Huge encryption/decryption tables
  - → Huge key:
    - for n = 4, key size = 4 bits x 16 rows = 64 bits
    - for n = 64, key size = 64 x $2^{64} = 2^{70} = 10^{21}$ bits

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

# Block ciphers in practice

- Aim: Easily implementable structures that resemble somehow the ideal cipher
- A key of size k bits is being used
  - Hence, the possible mappings are $2^k$ είναι οι πιθανές αντιστοιχίσεις (less than $2^n!$ which is the number of all possible mappings)
- The encryption process is being iterated many times
- Key-dependent permutations and substitutions are involved in this process

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

# Data Encryption Standard (DES)

- most widely used block cipher in world for almost two decades
- adopted in 1977 by NBS (now NIST)
  - as FIPS PUB 46
- encrypts 64-bit data using 56-bit key
- has widespread use
- has been considerable controversy over its security
- Now deprecated due to short key

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

# DES History

- IBM developed Lucifer cipher
  - by team led by Feistel
  - used 64-bit data blocks with 128-bit key
- then redeveloped as a commercial cipher with input from NSA and others
- in 1973 NBS issued request for proposals for a national cipher standard
- IBM submitted their revised Lucifer which was eventually accepted as the DES
  - Accepted as standard by NIST in 1976
  - Reniew every five years

Το έργο χρηματοδοτήθηκε από το
Πρόγραμμα Δικαιώματα,
Ισότητα και Ιθαγένεια 2014-2020
της Ευρωπαϊκής Ένωσης

# Data Encryption Standard (DES)

64-Bit DES symmetric key
(56 bits + 8 parity bits)

64-Bit Block
(plaintext)

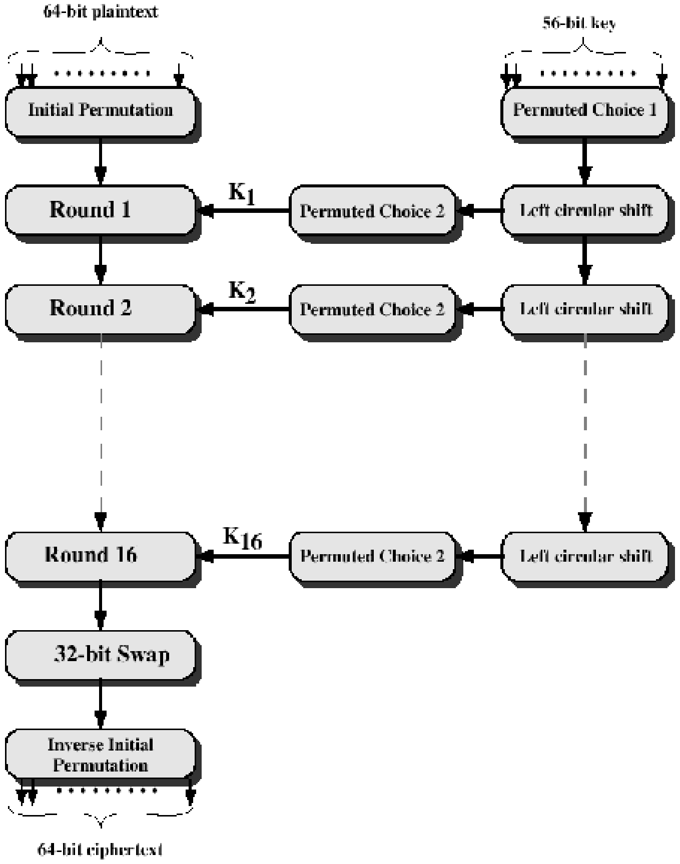
DES
Encryption

↓

64-Bit Block
Ciphertext

# Data Encryption Standard (DES)

- Feistel networks
- 64-bit blocks
- 56-bit key
- 16 rounds
- An initial permutation at the beginning (and the reverse permutation at the end)
- At each round, a 48-bit subkey is being used




Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

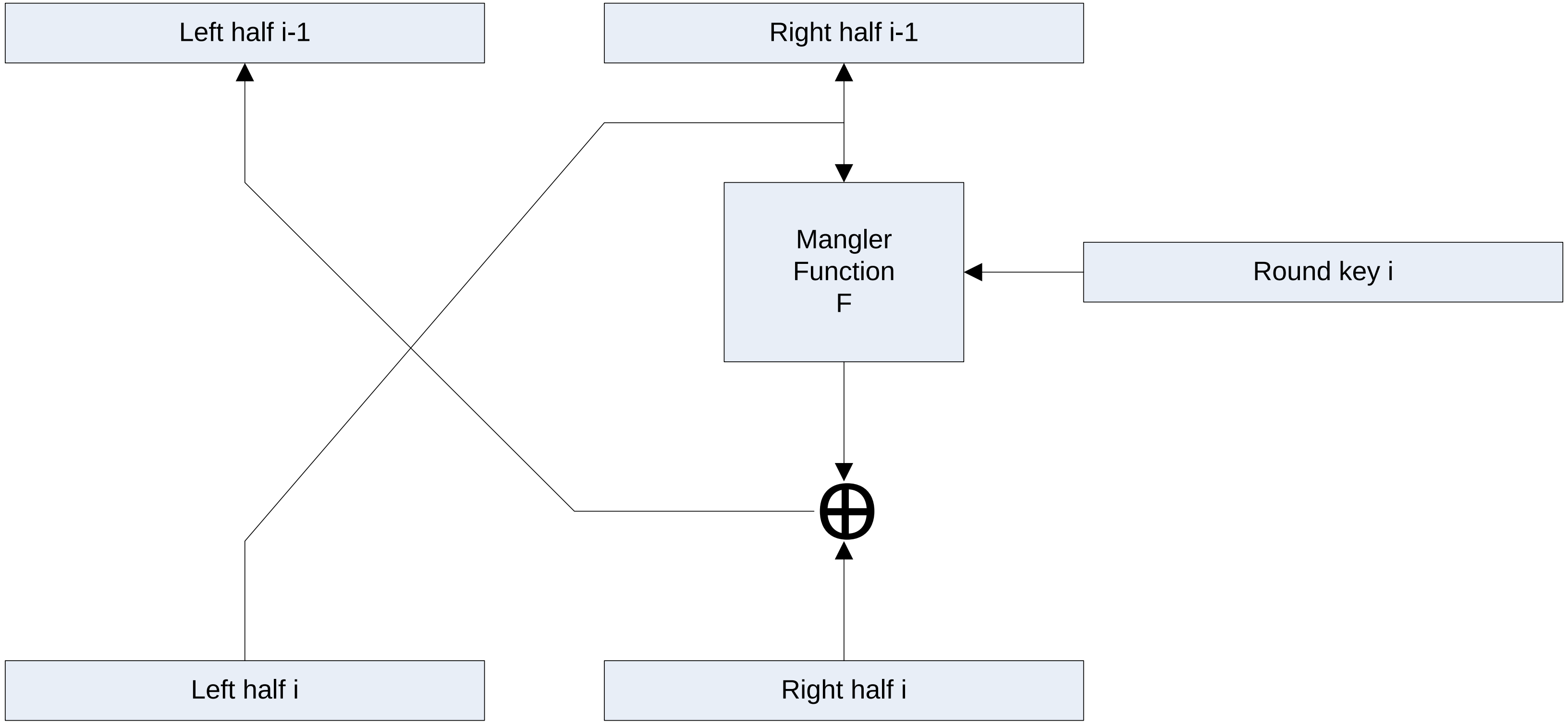
# DES Decryption

- decrypt must unwind steps of data computation
- with Feistel design, do encryption steps again using subkeys in reverse order (SK16 … SK1)
  - IP undoes final FP step of encryption
  - 1st round with SK16 undoes 16th encrypt round

    ….
  - 16th round with SK1 undoes 1st encrypt round
  - then final FP undoes initial encryption IP
  - thus recovering original data value

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

# DES Round Decryption




Decryption

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

# DES Example

| Round | $K_i$ | $L_i$ | $R_i$ |
|---|---|---|---|
| IP | | 5a005a00 | 3cf03c0f |
| 1 | 1e030f03080d2930 | 3cf03c0f | bad22845 |
| 2 | 0a31293432242318 | bad22845 | 99e9b723 |
| 3 | 23072318201d0c1d | 99e9b723 | 0bae3b9e |
| 4 | 05261d3824311a20 | 0bae3b9e | 42415649 |
| 5 | 3325340136002c25 | 42415649 | 18b3fa41 |
| 6 | 123a2d0d04262a1c | 18b3fa41 | 9616fe23 |
| 7 | 021f120b1c130611 | 9616fe23 | 67117cf2 |
| 8 | 1c10372a2832002b | 67117cf2 | c11bfc09 |
| 9 | 04292a380c341f03 | c11bfc09 | 887fbc6c |
| 10 | 2703212607280403 | 887fbc6c | 600f7e8b |
| 11 | 2826390c31261504 | 600f7e8b | f596506e |
| 12 | 12071c241a0a0f08 | f596506e | 738538b8 |
| 13 | 300935393c0d100b | 738538b8 | c6a62c4e |
| 14 | 311e09231321182a | c6a62c4e | 56b0bd75 |
| 15 | 283d3e0227072528 | 56b0bd75 | 75e8fd8f |
| 16 | 2921080b13143025 | 75e8fd8f | 25896490 |
| $IP^{-1}$ | | da02ce3a | 89ecac3b |

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

# Undesirable properties of DES

- 4 weak keys
  - (e.g. 00….011…1)
  - They produce identical subkeys

- 12 semi-weak keys
  - Key pairs that encipher a plaintext into the same ciphertext

- Complementary property
  - $\text{DES}_k(m) = c \Rightarrow \text{DES}_{k'}(m') = c'$

- NIST had changed the initial S-boxes as submitted by the IBM, and this raised some concerns (for possible trapdoors)
  - However, the subsequent research analysis indicated that S-boxes have nice cryptographic properties

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

# Cryptanalysis in DES

- Being international standard for almost two decades, many researchers focused on fully analysing the cryptographic strength of DES
- Two important cryptanalytic techniques occurred (they will not be studied here):
  - Differential cryptanalysis – Biham and Shamir (1990)
  - Linear cryptanalysis – Matsui (1993)
- Any new cipher should be examined against these techniques
  - DES proved to be secure against them
  - DES designers stated that differential cryptanalysis had been already considered when designing their cipher, almost 15 years before Biham and Shamir come up with it!
    - But linear cryptanalysis was something new

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

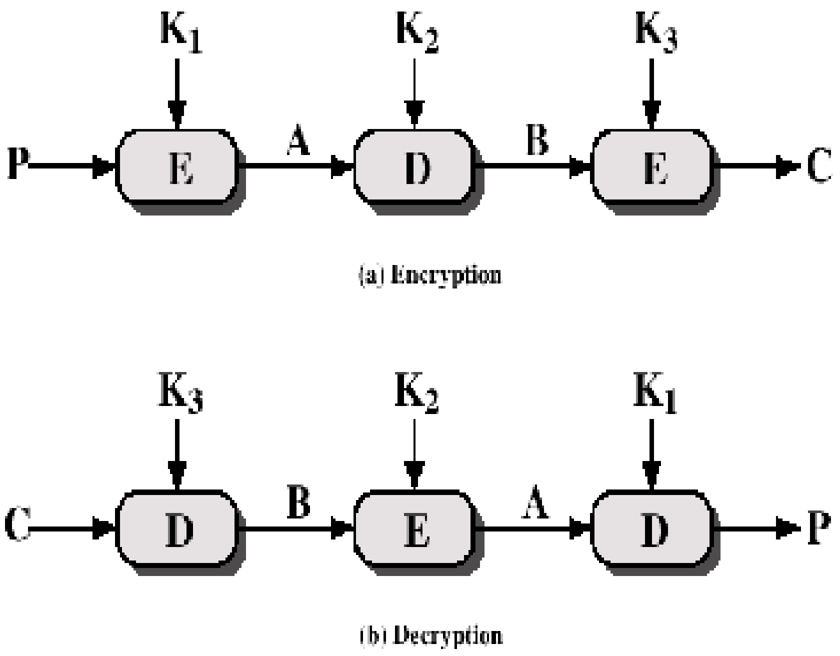
# Strength of DES today – Insecure

- 56-bit keys have $2^{56} = 7.2 \times 10^{16}$ values
- brute force search looked hard in 1976, but:
  - in 1997 on Internet in a few months
  - in 1998 on dedicated h/w (EFF) in a few days
  - in 1999 above combined in 22hrs!
- NIST officially announced the end of DES in 2004
  - See also Bruce Schneier's blog: http://www.schneier.com/blog/archives/2004/10/the_legacy_of_d.html

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

# Triple DES (3DES) - 168

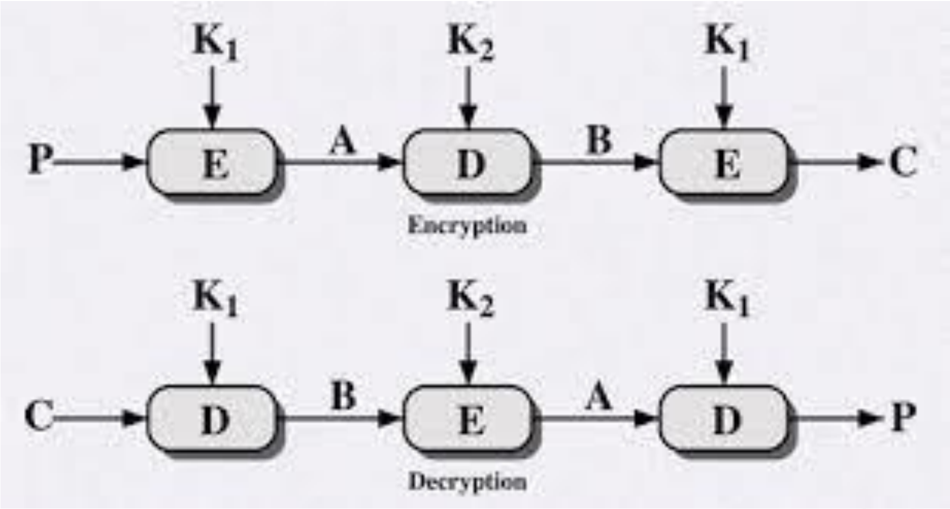
- 3 encryptions, with 3 distinct keys
- Hence, the key size in 3DES είναι 3x56=168 bits.
- The middle stage performs decryption and not encryption, so as to ensure that 3DES can decrypt a message that has been encrypted by simple DES
- Encryption:
  - $C=E_{k3}(D_{k2}(E_{k1}(P)))$
- Decryption:
  - $P=D_{k1}(E_{k2}(D_{k3}(C)))$
- If K1=K2, then 3DES=DES



Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

# Triple DES (3DES) - 112

- The same 56-bit key can be used at the first and third stage
- In this case, the key size is 2x56=112 bits.
- Again, 3DES can decrypt ciphertexts that have been produced the simple DES
- Encryption:
    - $C=E_{k1}(D_{k2}(E_{k1}(P)))$
- Decryption:
    - $P=D_{k1}(E_{k2}(D_{k1}(C)))$
- Again, if K1=K2, then 3DES=DES



Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

# AES (Advanced Encryption Standard) Requirements

- Private key symmetric block cipher
- 128-bit data, 128/192/256-bit keys
- stronger & faster than Triple-DES
- active life of 20-30 years (+ archival use)
- provide full specification & design details
- both C & Java implementations
- NIST have released all submissions & unclassified analyses

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

# AES parameters

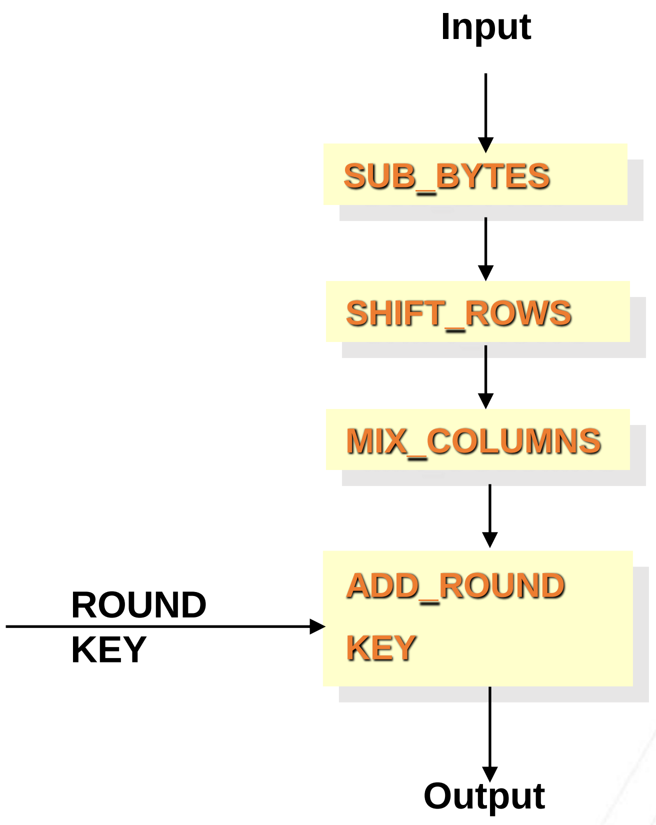
| | AES-128 | AES-192 | AES-256 |
|---|---|---|---|
| Key size (bits) | 128 | 192 | 256 |
| Plain text block size (bits) | 128 | 128 | 128 |
| Number of rounds | 10 | 12 | 14 |
| Round key size (bits) | 128 | 128 | 128 |
| Expanded key size (bytes) | 176 | 208 | 240 |

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

# A typical AES encryption round

- SUB_BYTES: Substitution of bytes
- SHIFT_ROWS: Shifting of bytea
- MIX_COLUMNS: “Mixing”
- ADD_ROUND_KEY:  XOR addition with key

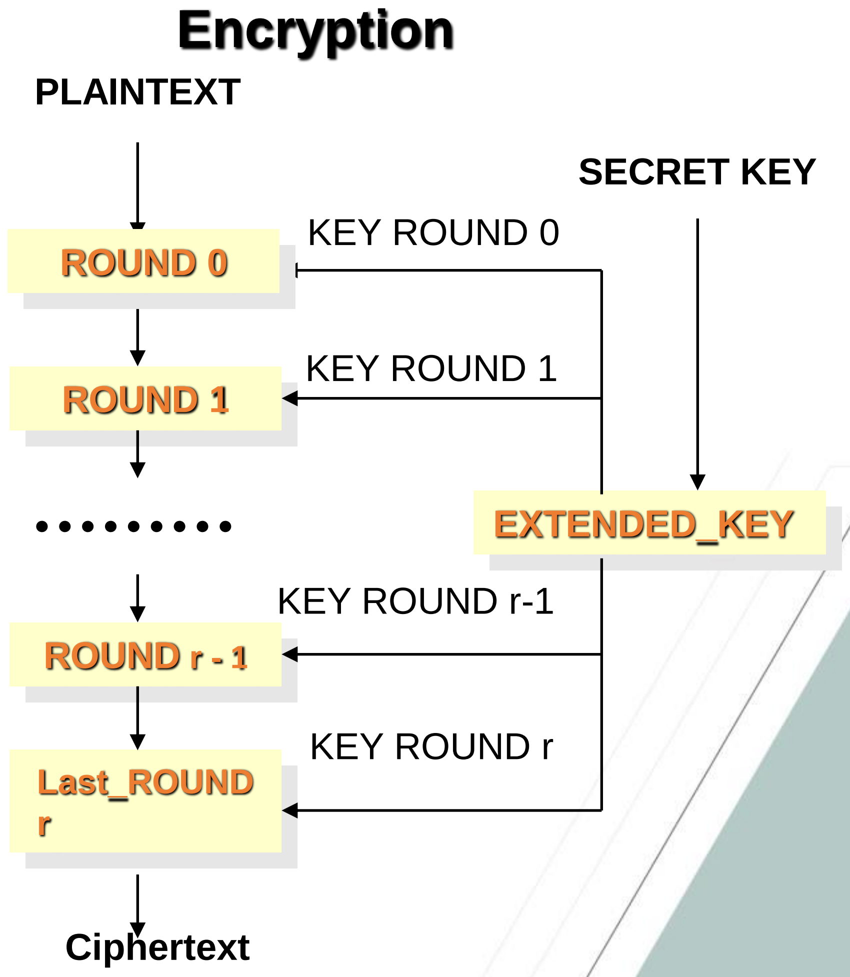
- Basic assumption: Each block is being considered as a 4x4 array of bytes (8 bit): 4x4x8= 128 bits in total.
- The inputs and outputs of each round are such types of blocks



Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

# A typical AES encryption round

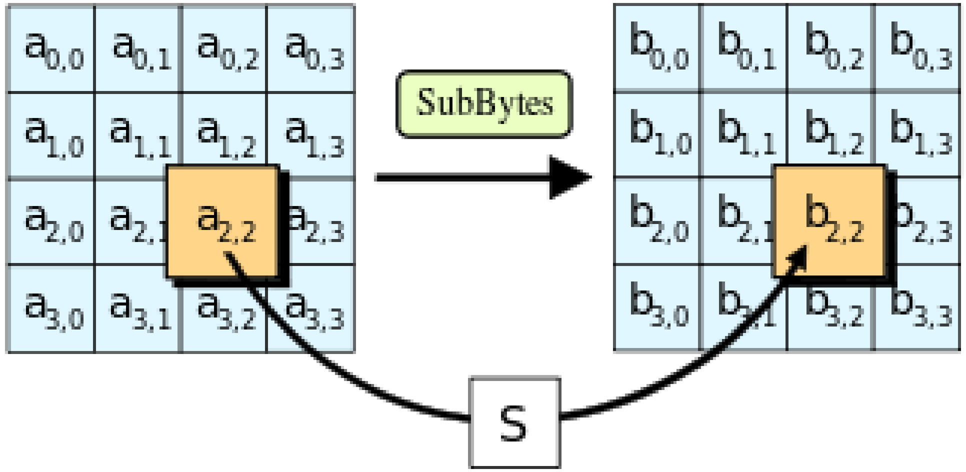
- Round 0 is simply an XOR addition with the round key
- The next r-1 rounds are identical , consisting of the four stages
- The last round r is slighlty different, as discussed next.
- The secret key is being extended (with a well-determined procedure); from this extended key, a key scheduling procedure derives the sub-keys for each round



Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

# Byte substitution

- Plaintext is usually 128 bits, or 16 bytes




- Each byte (out of 16) is being substituted by another byte, under a highly nonlinear transformation (function S) with nice mathematical properties from a cryptographic point of view

Το έργο χρηματοδοτήθηκε από το
Πρόγραμμα Δικαιώματα,
Ισότητα και Ιθαγένεια 2014-2020
της Ευρωπαϊκής Ένωσης

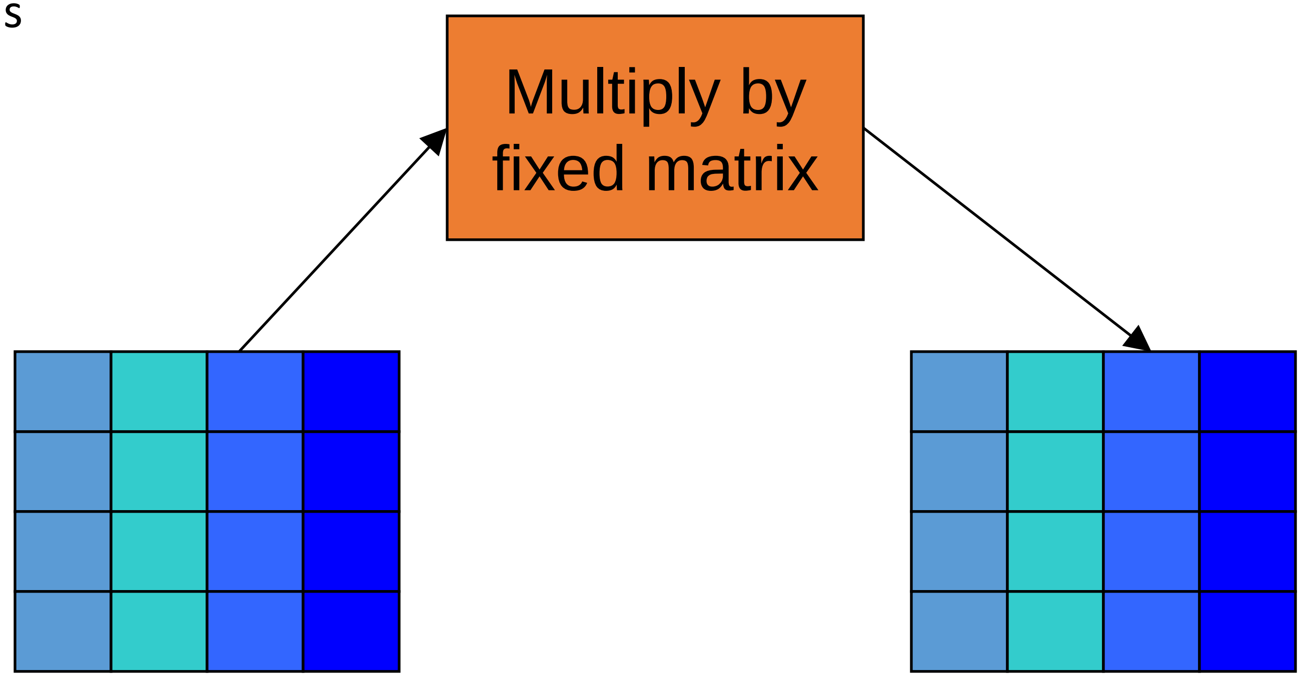
# Shift rows and mix columns

- Diffusion is reached in two steps
  - Shift rows

Το έργο χρηματοδοτήθηκε από το
Πρόγραμμα Δικαιώματα,
Ισότητα και Ιθαγένεια 2014-2020
της Ευρωπαϊκής Ένωσης

# Shift rows and mix columns

- Diffusion is reached in two steps
  - Mix columns

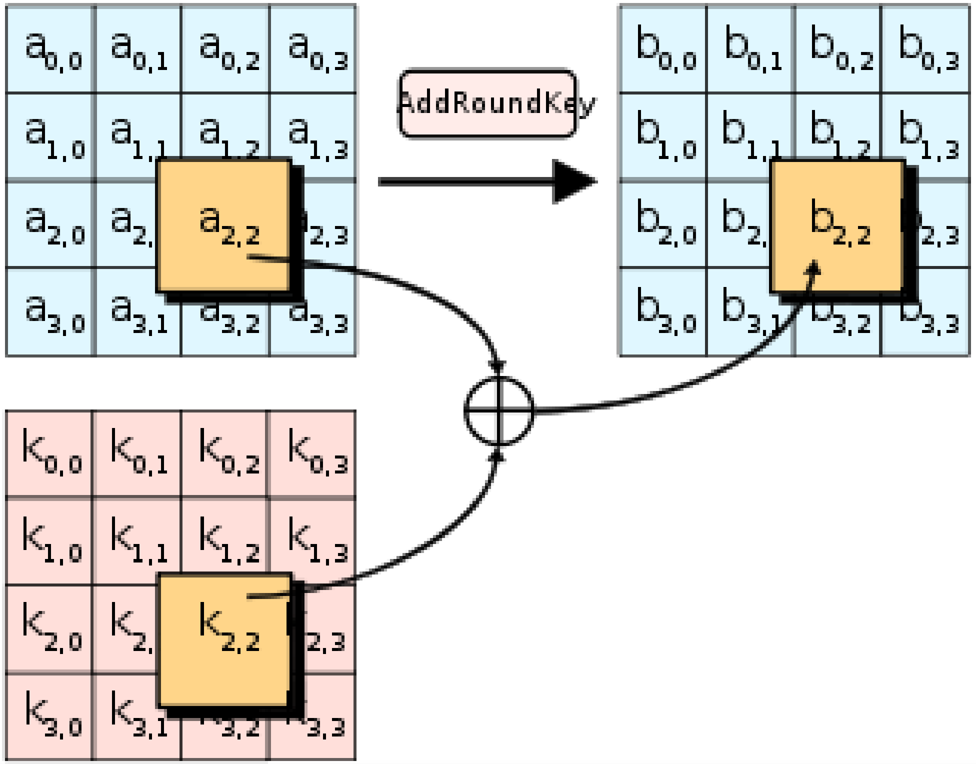



- Each column (4 bytes) is being transformed into another column (of 4 bytes)
- This is not performed in the last round

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

# Round key addition

- Finally, the round key is XOR-ed with the state
- It is the only stage that key is being used!



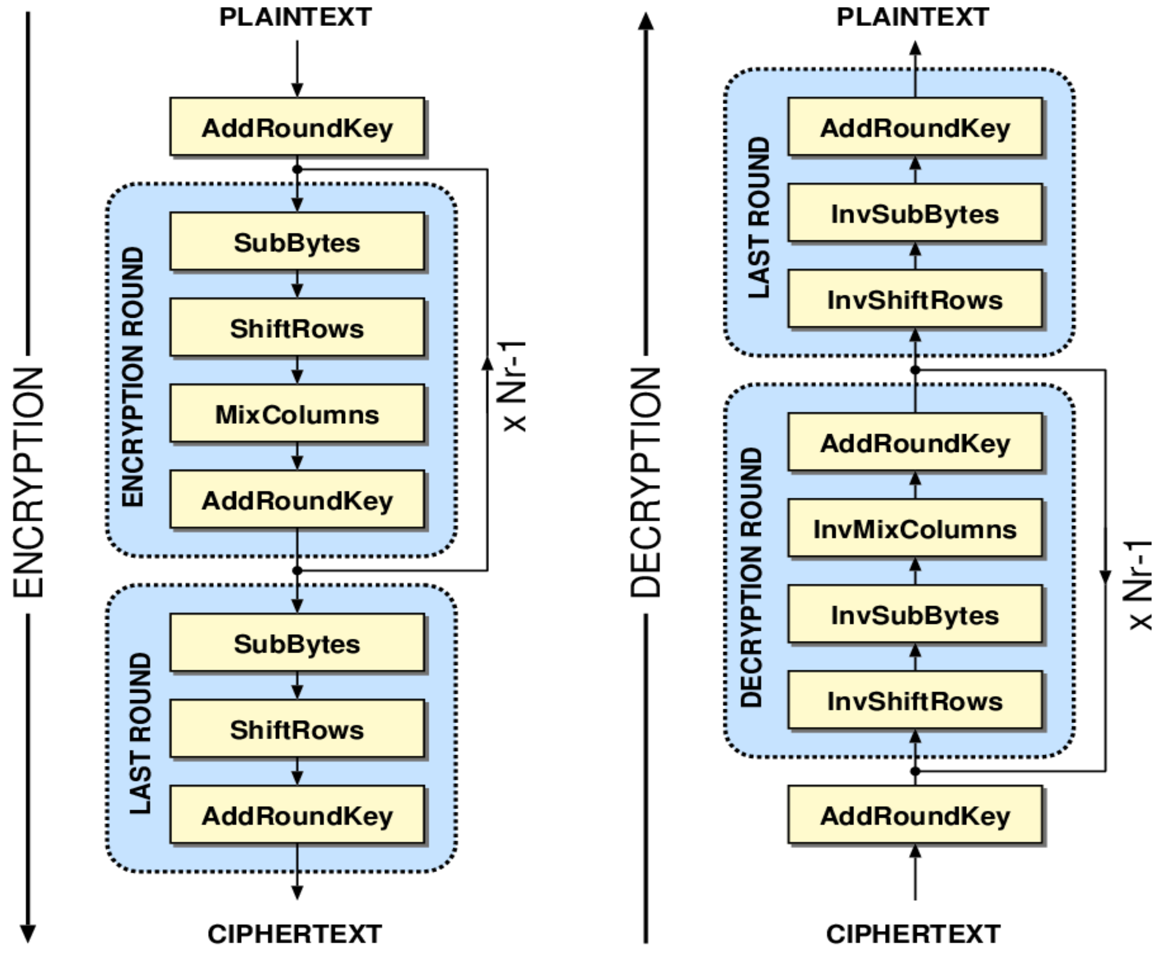
Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

# Decryption

- The inverse transformations are employed (Inv_Mix_Columns, Inv_Shift_Rows κτλ.)
- Only the Inv_Add_Round_Key is (obviously) the same with the Add_Round_Key
- AES decryption is slower than AES encryption. However:
  - The decryption is still fast, compared to other block ciphers
  - The speed in encryption is more important than the speed in decryption, as discussed next

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

# Encryption vs. Decryption



Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

# A security comparison

- "Assuming that one could build a machine that could recover a DES key in a second (i.e., try 255 keys per second), then it would take that machine approximately 149 thousand-billion (149 trillion) years to crack a 128-bit AES key."
- AES remains secure today
  - And it will remain secure even in the era of post-quantum computing (for key size 256 bits)