KF School of Computing and Information Sciences
Florida International University

CNT 4403
Computing and Network Security

Cryptography – Symmetric Crypto

Dr. Kemal Akkaya

E-mail: *kakkaya@fiu.edu*

Cryptography

- ***Cryptography*** **is the study of mathematical techniques in the provision of information security services. It is the strongest and most widely used tool for defending against many kinds of security threats.**
- **Goals of cryptography**
  - ***Confidentiality***: keeping information secret from all but those who are authorized to see it
  - ***Integrity***: ensuring information has not been altered by unauthorized or unknown means
  - ***Authentication***: corroborating the source of information or the identity of an entity
  - ***Non-repudiation***: preventing the denial of previous commitments or actions

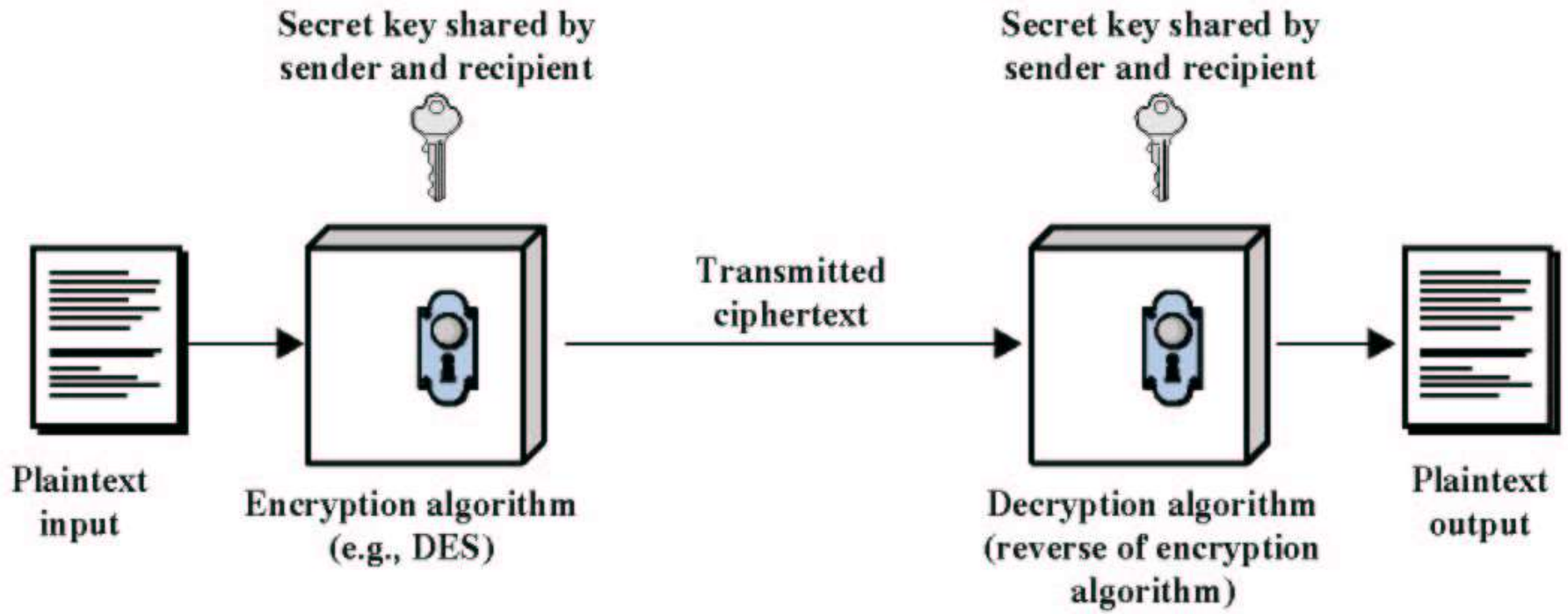
Symmetric-Key Encryption

- **A *symmetric-key encryption scheme*, or a *cipher*, consists of:**
  - a secret key K shared by the sender and the receiver,
  - an *encryption algorithm* E_K that, with a message M (called the *plaintext*) and the secret key K as input, produces the encrypted message $C = E_K(M)$ as output (called the *ciphertext*), and
  - a *decryption algorithm* D_K that, with a ciphertext C and the secret key K as input, outputs the original message $M = D_K(C)$; i.e., given any key K,

    $$D_K(E_K(M)) = M$$

    for all messages M.

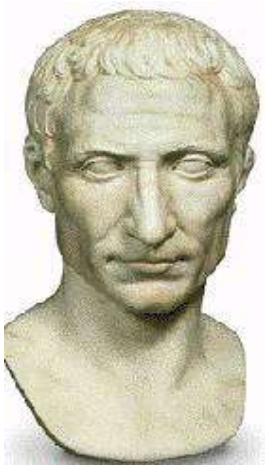
Symmetric-Key Encryption



Cryptanalysis

- ***Cryptanalysis*** **is the science of recovering the plaintext or deducing the key without access to the key.**
- **A *brute-force attack*, also called *exhaustive key search*, attempts to decrypt a given ciphertext message with every possible key until the resulting plaintext is meaningful (identified by means of *frequency analysis*).**
- **In general, a brute-force attack on a cipher with an *n*-bit key requires at most 2^n trials. Therefore, the longer the key length, the more secure the cipher.**

Caesar Cipher



- **The *Caesar cipher* (also called the *shift cipher*) replaces each letter of a message with another letter a fixed number of places after it in the alphabet (the alphabet is wrapped around).**
- **Mathematical description**
  - Assign a numerical equivalent to each letter: A – 0, B – 1, C – 2, D – 3, E – 4, F – 5, G – 6, H – 7, I – 8, J – 9, K – 10, L – 11, M – 12, N – 13, O – 14, P – 15, Q – 16, R – 17, S – 18, T – 19, U – 20, V – 21, W – 22, X – 23, Y – 24, Z – 25
  - Encrypt: for each plaintext letter M_i, the ciphertext letter is

  $C_i = E_K(M_i) = (M_i + K) \bmod 26$

  where the secret key K is the *shift amount* (which is a number between 1 and 25)
  - Decrypt: $M_i = D_K(C_i) = (C_i - K) \bmod 26$
- **Example: *M* = KEMAL, *C* = NHPDO, *K* = 3**
- **Cryptanalysis: *brute-force attack* (there are only 25 possible keys)**

Vigenère Cipher

- **The *Vigenère cipher*, invented by Giovan Batista Belaso in 1553 (but misattributed to Blaise de Vigenère in the 19th century), works as follows:**
  - Let $K = K_0\ K_1 \ldots K_{d-1}$, where d is the number of letters in K. The key K is usually a word with 5 – 8 letters.
  - Encrypt: $C_i = (M_i + K_{i \bmod d}) \bmod 26$
  - Decrypt: $M_i = (C_i - K_{i \bmod d}) \bmod 26$

- **Example: *K* = FALSE**

```
Plaintext    KENNYISTHEGREATESTMANINTHEWORLD
Key          FALSEFALSEFALSEFALSEFALSEFALSEF
Ciphertext   PEYFCNSEZILRPSXJSEEESIYLLJWZJPI
```

Block Ciphers

- **A *block cipher* encrypts the plaintext message one block at a time (every block has the same fixed size).**
- **Most contemporary ciphers are block ciphers:**
  - Data Encryption Standard (DES)
    - ✓ Key length: 56 bits, block length: 64 bits
  - Advanced Encryption Standard (AES)
    - ✓ Key length: 128/192/256 bits, block length: 128 bits
  - Triple DES
  - International Data Encryption Algorithm (IDEA)
  - Blowfish
  - Ron's Code 5 (RC5)

Block Ciphers Strength

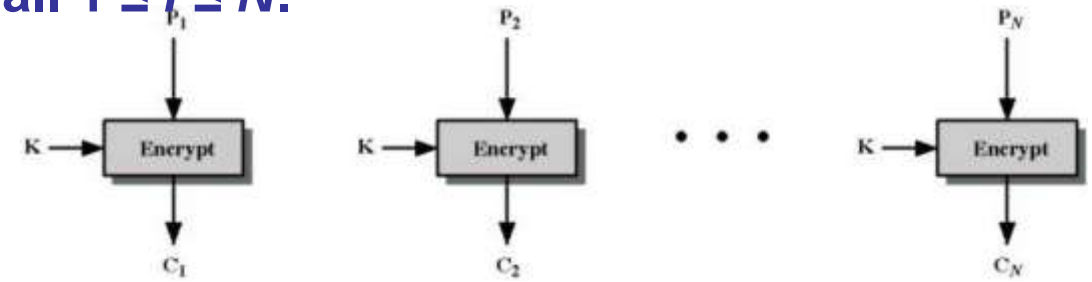
- **Block ciphers generally apply the techniques of *substitution (confusion)* and *permutation (diffusion)* to complicate the statistical relationship between the ciphertext and the plaintext, thereby thwarting cryptanalysis based on statistical analysis.**
- **Confusion:**
  - If one bit of the key changes, the ciphertext changes significantly
- **Diffusion:**
  - If one bit of the plaintext changes, the ciphertext changes significantly
- **Identified by Shannon in 1948**

Modes of Operation

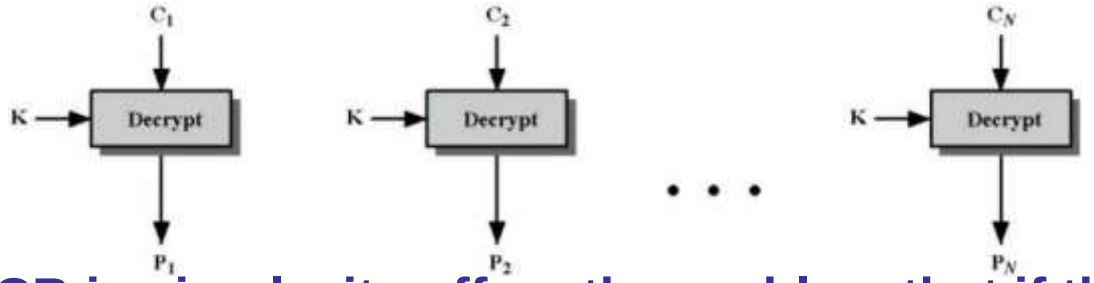
- A *mode of operation* specifies how a block cipher with a fixed block size (e.g., 128 bits for AES) can be extended to process messages of arbitrary length.
- Most of the modes of operation partition a message P in the most straightforward way: $P = P_1 P_2 \ldots P_N$, where P_i is an m-bit block for all $1 \leq i \leq N$ and m is the block size of the block cipher used, padding the last block P_N if necessary.
- 5 modes:
  - ECB (Electronic Code Book)
  - CBC (Cipher Block Chaining)
  - CFB (Cipher Feedback)
  - OFB (Output Feedback)
  - CTR (Counter)

Electronic Codebook Mode (ECB)

- Encrypt: The ciphertext to be sent is $<C_1, C_2, \ldots, C_N>$, where $C_i = E_K(P_i)$ for all $1 \le i \le N$.



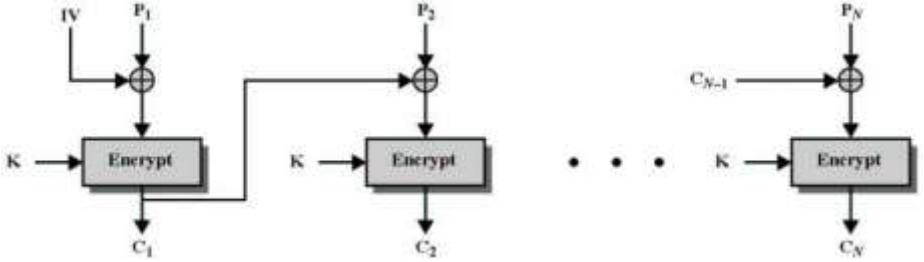
- Decrypt: $P_i = D_K(C_i)$ for all $1 \le i \le N$.



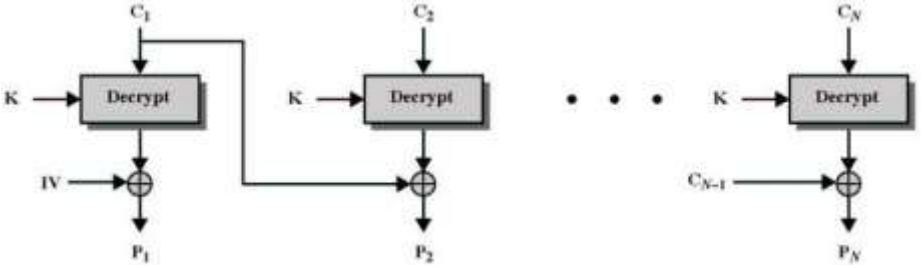
- Though ECB is simple, it suffers the problem that if the same plaintext block appears more than once in the message, ECB always produces the same ciphertext block, allowing an adversary to gain some knowledge by observing repetitions in lengthy messages.

Cipher Block Chaining Mode (CBC)

- Precomputation: an *m*-bit initialization vector IV is randomly selected, where *m* is the block size.
- Encrypt: The ciphertext to be sent is <IV, C_1, C_2, …, C_N>, where C_0 = IV and $C_i = E_K(C_{i-1} \oplus P_i)$ for all $1 \le i \le N$.



- Decrypt: $P_i = C_{i-1} \oplus D_K(C_i)$ for all $1 \le i \le N$, *where* C_0 = IV.

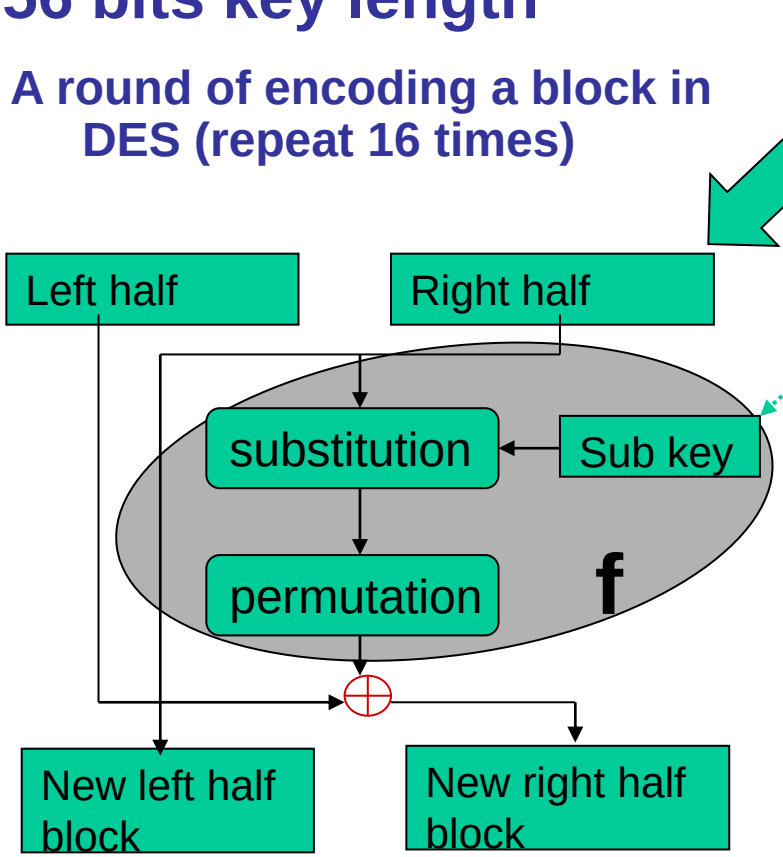


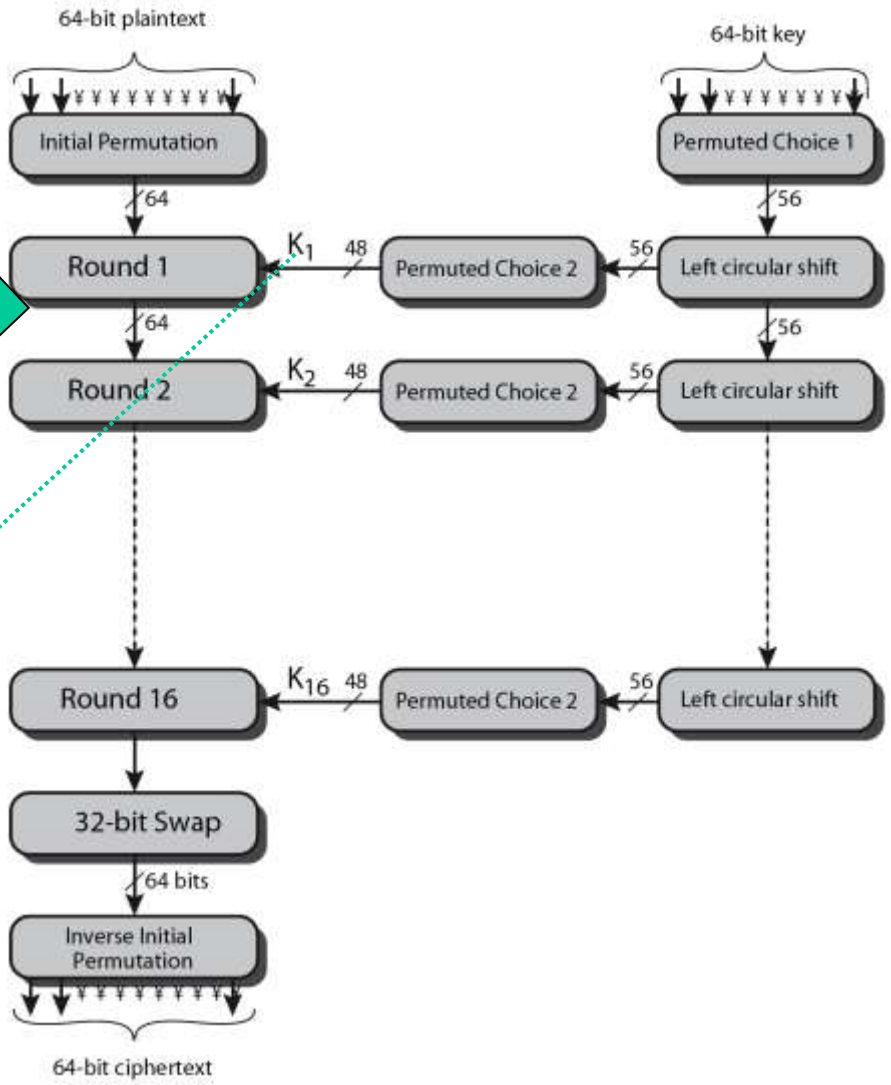
- The same plaintext block may not be encrypted to the same ciphertext block in CBC, because the i^{th} ciphertext block depends on the i^{th} plaintext block and all the previous plaintext blocks. However, unlike ECB, CBC encryption is not parallelizable (but CBC decryption is parallelizable).

Data Encryption Standard (DES)

- Adopted in 1977 by NIST
- Block cipher with 64 bits of blocks
- 56 bits key length

A round of encoding a block in DES (repeat 16 times)





Weakness of DES

- 56 bit key is too short
  - Can be broken on average in 2^55 ≈3.6*10^16 trials
- Moore's law: speed of processor doubles per 1.5 years
- 1997: 3500 machines broke DES in about 4 months
- 1998: 1M dollar machine broke DES in about 4 days
- 1999: Deep Crack and distributed.net broke a DES key in 22 hours and 15 minutes
- Today you can break it on your laptop
- May 26, 2002, DES was superseded by AES

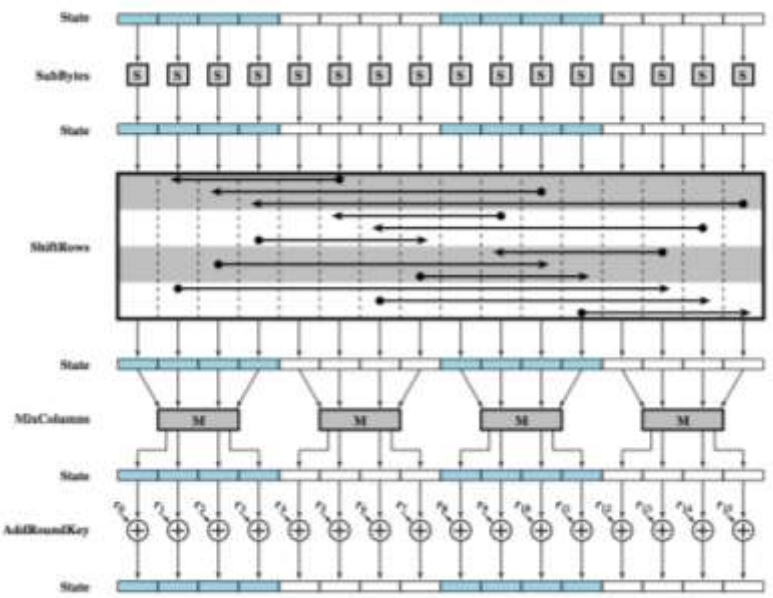
Triple DES (3DES)

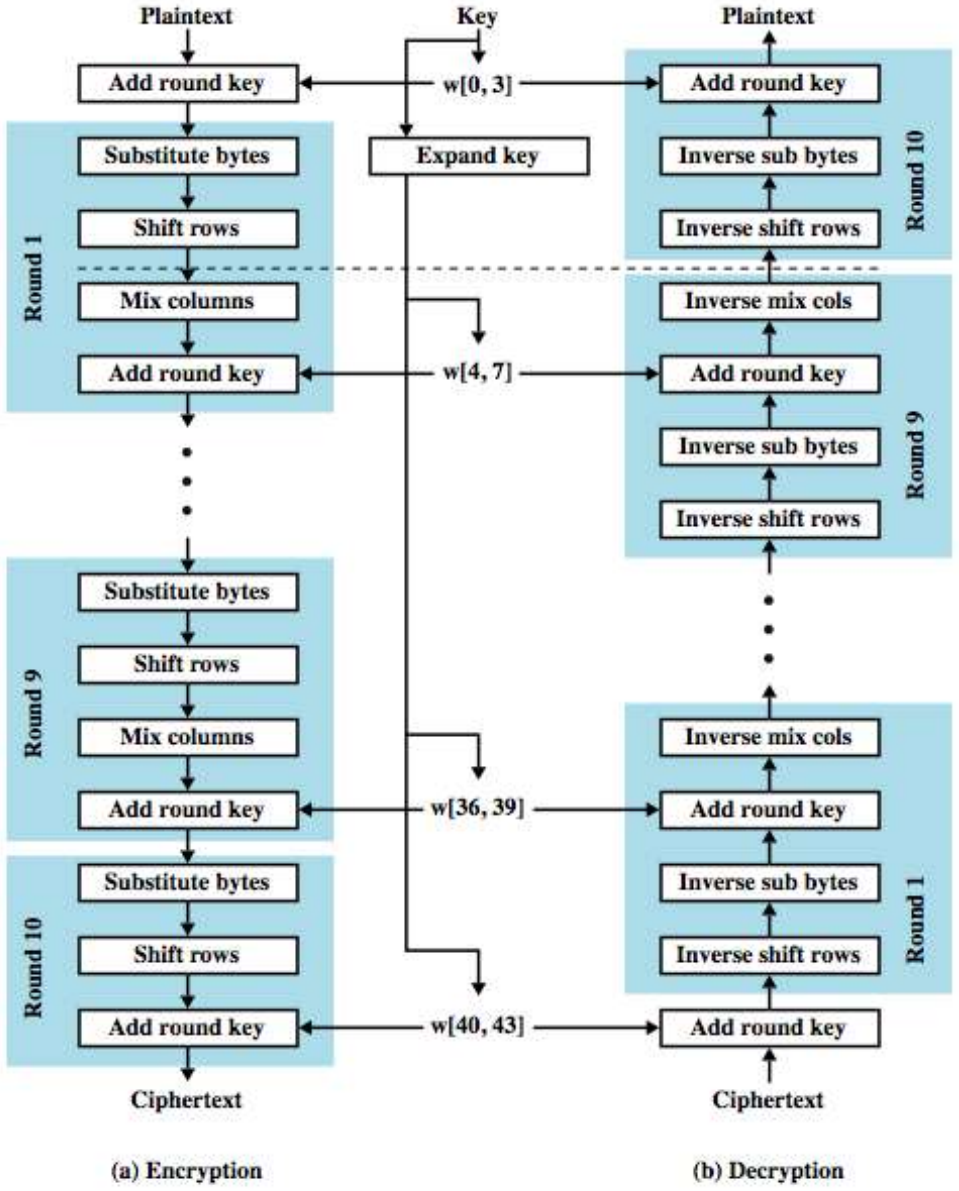
- **First used in financial applications**
- **Initial Versions**
  - *2 keys, 2 encryption (double DES)*
  - *2 keys, 2 encryption, 1 decryption : C* = E(K_1, D(K_2, E(K_1, *P*)))
- **Final Version: DES FIPS PUB 46-3 standard of 1999**
  - uses three keys & three DES executions: *C* = E(K_3, D(K_2, E(K_1, *P*)))
  - decryption same with keys reversed
  - use of decryption in second stage gives compatibility with original DES users
  - effective 168-bit key length, slow, secure
- **1998 3DES → valid till 2030**

Advanced Encryption Standard (AES)

- **1997 NIST call for a competition**
- **Final five**
  - Rijndael (Joan Daemen and Vincent Rijmen),
  - Serpent (Ross Anderson),
  - Twofish (Bruce Schneier),
  - RC6 (Don Rivest, Lisa Yin),
  - MARS (Don Coppersmith, IBM)
- **2000 Rijndael won**
- **2002 Rijndael became AES**
- **Key length increased to at least 128bits**
- **Block length also 128bits**

AES Structure





AES vs DES

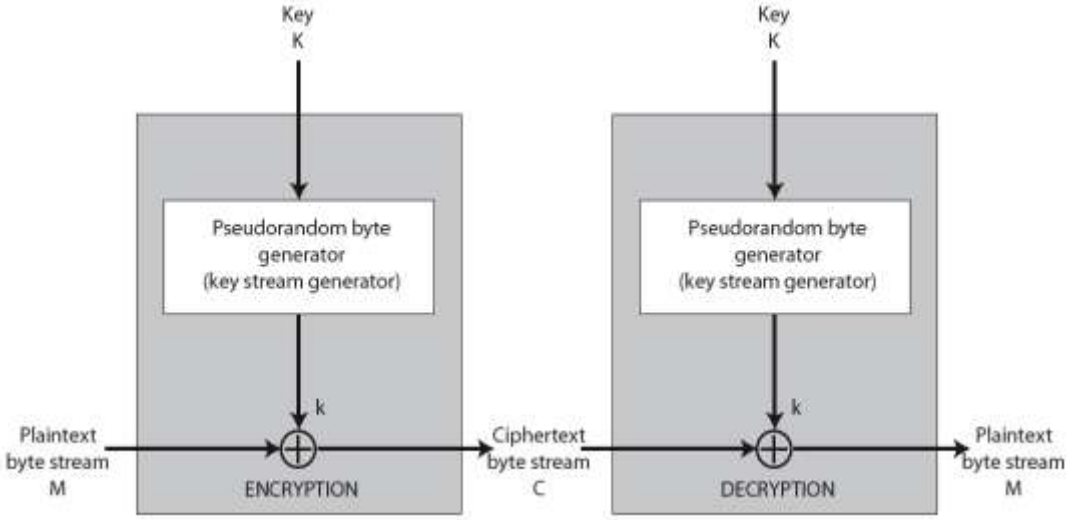
	DES	AES
Date	1976	1999
Block size	64	128
Key length	56	128, 192, 256
Number of rounds	16	9,11,13
Encryption primitives	Substitution, permutation	Substitution, shift, bit mixing
Cryptographic primitives	Confusion, diffusion	Confusion, diffusion
Design	Open	Open
Design rationale	Closed	Open
Selection process	Secret	Secret, but accept open public comment
Source	IBM, enhanced by NSA	Independent cryptographers

Post-Quantum Encryption

- **In a decade, quantum computers will be available for computations**
- **Their speed will make some of the existing encryption algorithms useless**
  - They will be able to crack these algorithms
  - Will check these later
    - ✓Asymmetric cryptography and signatures
- **AES will be quantum-secure if used with 256 bits**
  - AES is considered one of the post-quantum crypto solutions

Stream Ciphers

- **Processes input elements continuously**
  - Bit by bit (or byte)
- **Key is input to a pseudorandom bit generator (PRNG)**
  - Produces stream of random like numbers (keystream)
  - Unpredictable without knowing input key
- **Keystream is combined (XORed) one byte at a time with the plaintext stream**



Stream Ciphers

- **Are faster and use far less code**
- **Design considerations:**
  - Keystream should have a large period (should not repeat frequently)
  - Keystream approximates random number properties
  - Uses a sufficiently long key (i.e., 128 bits)
- **RC4 is the most common**
  - Used in WEP
- **Others: SEAL, A5/1, FISH, Helix, ISAAC, MUGI, Panama**
- **Speed Comparisons**
  - from Crypto++ 5.1 benchmarks, on a 2.1 GHz P4:

Algorithm	Speed (MByte/s.)
DES	22
AES	62
RC5-32/12	79
RC4	111
SEAL	920