الجامعة الافتراضية السورية

أمن الشبكات
Network and Infrastructure Security

د. محمد العصورة

Dr. Mohammed Assora

دكتوراه في امن شبكات الحواسب

PhD. In Computer Network Security

Objectives of Lecture

- Understanding the meaning of cryptography
- Understanding the main basics, advantages and disadvantages of Symmetric cryptography
- Realising the significance of cryptography mechanisms in the context of Information systems security

Contents

1. Cryptography
2. Symmetric Cipher systems
3. Stream Cipher
4. Block cipher
5. Modes of operation

Definitions

- Cryptography is the study of methods of sending messages in disguised form so that only the intended recipients can remove the disguise and read the message.
- The message to be sent is called *plaintext*
- The disguised message is called the *ciphertext*. In most encryption systems, the encoding and decoding depend on some *key*.

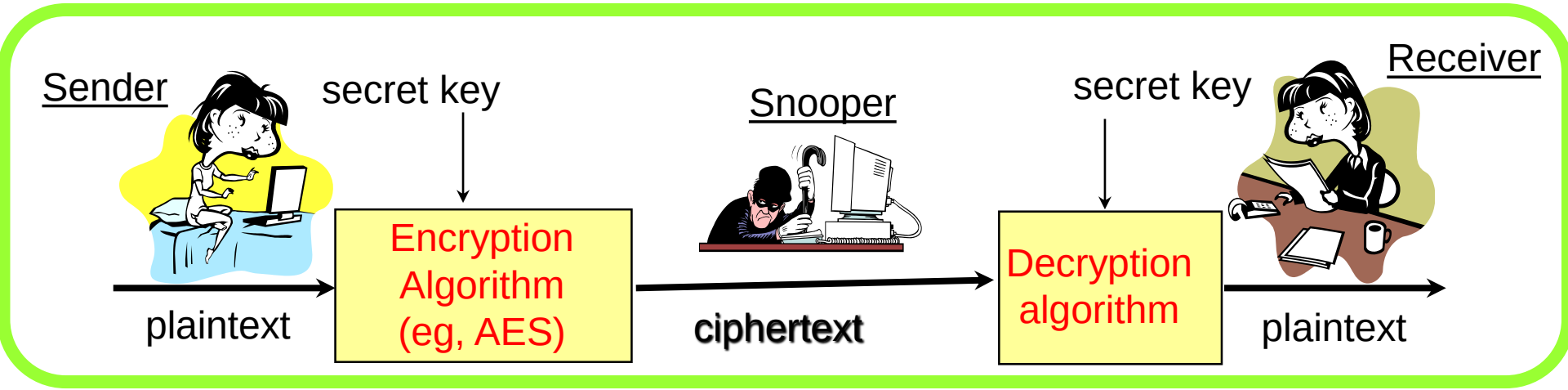
- Cryptanalysis is the process of deciphering a message by an unauthorised party

Cipher

- A cipher is a means for transforming plaintext (typically a message) into ciphertext under the control of secret key
- We write: $c = e_k(m)$, where m is the plain text, e is the cipher function , k is the secret key, and c is the cipher text

- Decipherment $m = d_k(c)$
- Typically e will be public, and secrecy of m (given c) depends totally on secrecy of k.

Cryptography



Cryptography

- Cryptographic techniques are divided into 3 types:
  - Symmetric-key Cryptography
    - Symmetric-key ciphers
      - Block ciphers
      - Stream ciphers
    - Message Authentication Codes (MACs)
  - Public-key Cryptography
    - Asymmetric-key ciphers
      - Integer Factorization
      - Discrete logarithm
    - Signatures
  - Keyless Cryptography
    - Hash (message digest) functions

Symmetric Encryption

- Symmetric (single-key, one-key, symmetric-key) encryption
- A type of encryption
- The same key is used to encrypt and decrypt the message.
- Differs from asymmetric (or public-key) encryption, which uses one key to encrypt a message and another to decrypt the message.

Types of Symmetric-key Algorithms

- Symmetric-key algorithms can be divided into:
  - Stream Ciphers
  - and Block Ciphers.

- Stream ciphers encrypt the bits of the message one at a time

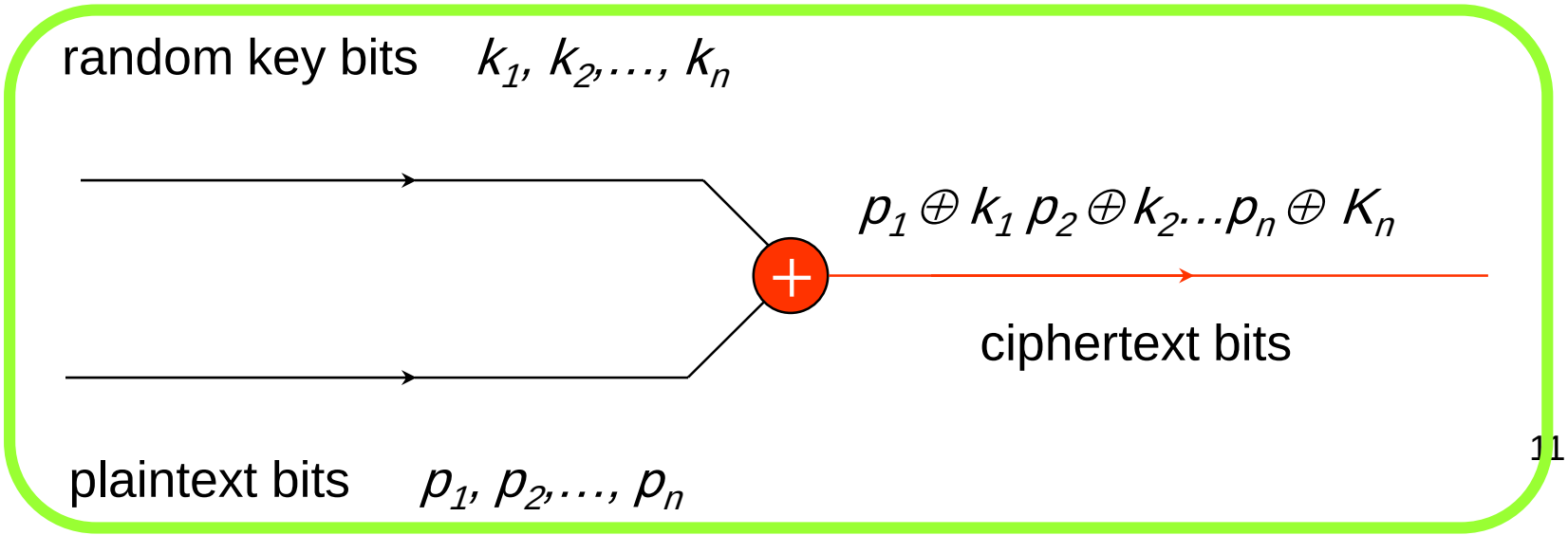
- Block ciphers take a number of bits and encrypt them as a single unit.

Stream Ciphers

- A ***stream cipher*** is an encryption scheme which treats the plaintext symbol-by-symbol (e.g., bit or character)
  - A ***keystream*** is a sequence of symbols $e_1e_2e_3\ldots \in K$ (the key space for a set of encryption transformations)
  - A an alphabet of definition of q symbols
  - Encryption: E_e is a simple ***substitution cipher*** with block length of 1, where $e \in K$, $E_e = E_{e_1}(m_1)\, E_{e_2}(m_2) \ldots = c_1c_2\ldots$
    - Plaintext $m = m_1 m_2 \ldots (m_i \in A)$
    - Ciphertext $c = c_1c_2\ldots$
  - Decryption: $D_d = D_{d_1}(c_1)\, D_{d_2}(c_2) \ldots = m_1m_2\ldots$, $d_i = e_i^{-1}$

Vernam Cipher

- *Vernam Cipher* A stream cipher defined on the alphabet $A=\{0,1\}$
- The *keystream* is a binary string ($k=k_1 \ldots k_t$) of the same length as the plaintext m ($=m_1 \ldots m_t$)
- Encryption $c_i=m_i \oplus k_i$, Decryption $m_i=c_i \oplus k_i$



One-time pad

- If the key string is randomly chosen and never used again then Vernam cipher is called a ***one-time pad***

✓ Perfect cryptosystem (No information at all is leaked)

✘ One-time pad's drawback: The keystream must be as long as the plaintext.

  – This increases the difficulty of key distribution and key management

Properties of stream ciphers

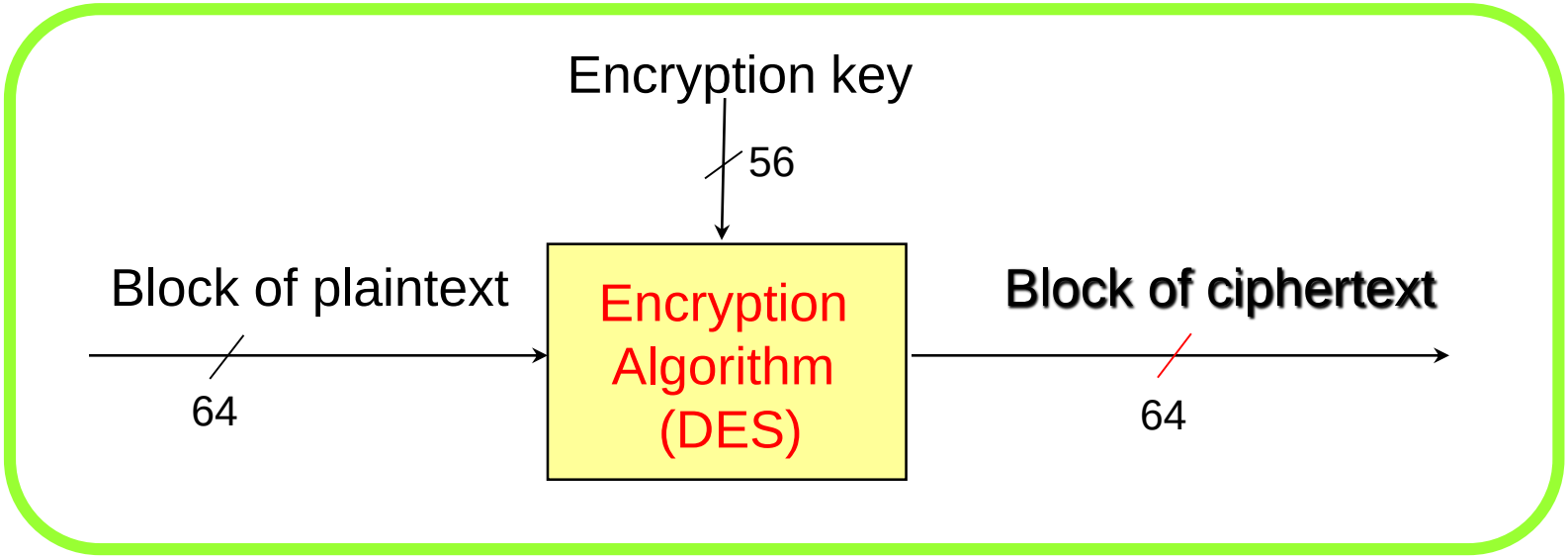
- Advantages:
  - ✓ No error propagation: a ciphertext digit is modified during transmission doesn't affect the decryption of other ciphertext digits
  - ✓ Easy for implementation and Fast
- Drawbacks:
  - ✘ Requirement for synchronization: sender and receiver must be synchronized
    - *ie*, they must use the same key and operate on the same position (digit),
    - if synchronization is lost due to digit insertion or deletion then re-synchronization is required.
- Application: GSM and phone networks.
- A Modern Stream cipher: RC4 (1987).

Block ciphers

- A ***block cipher*** encrypts one block at a time, using a complex encryption function
- Examples
  - DES: operates on blocks of 64 bits
  - AES: operates on blocks of 128 bits
- Block ciphers can be used in various modes (***modes of operation***).

Data Encryption Standard (DES)

- Adopted in 1977 by the National Bureau of Standards (US), nowadays NIST
  - FIPS 46

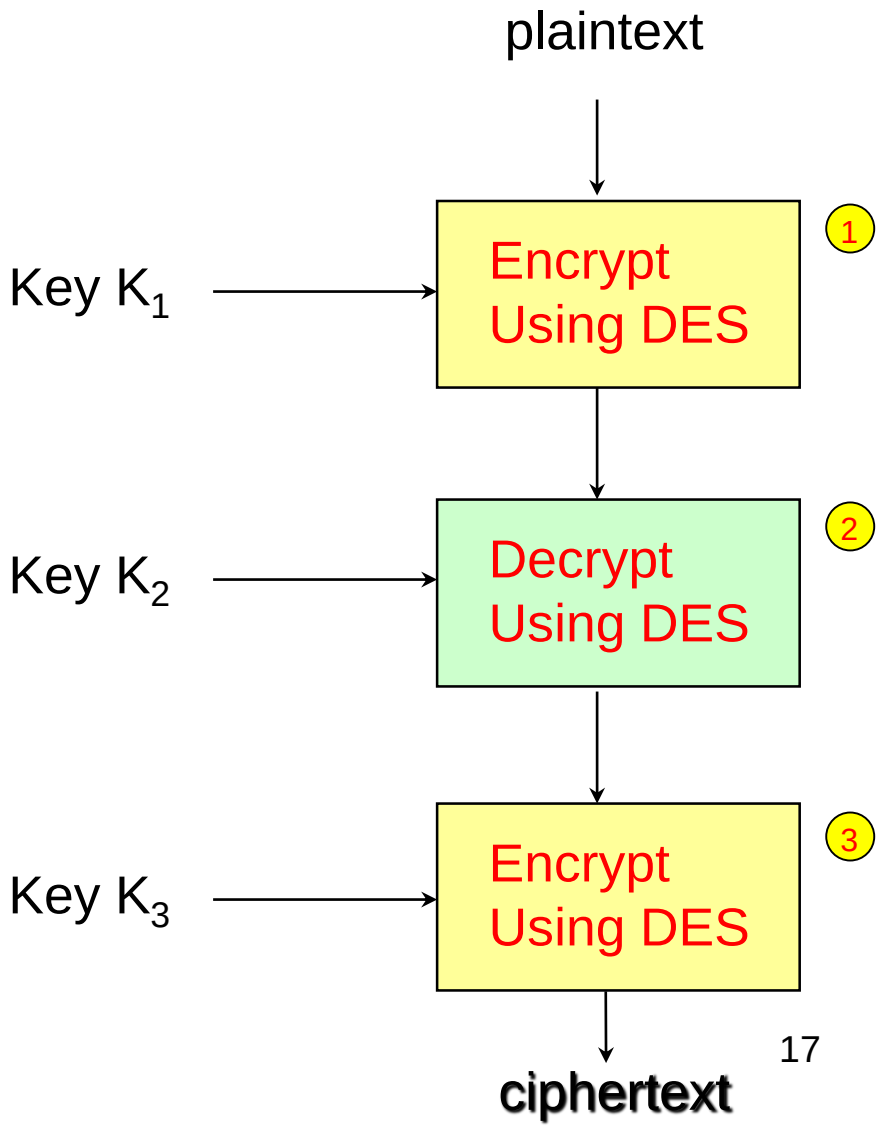


Data Encryption Standard (DES)

- DES exhaustive key search became feasible
- 1999: DES should only be used for legacy systems
- 3DES or AES are commonly recommended instead of DES.
- 2004: Withdrawn

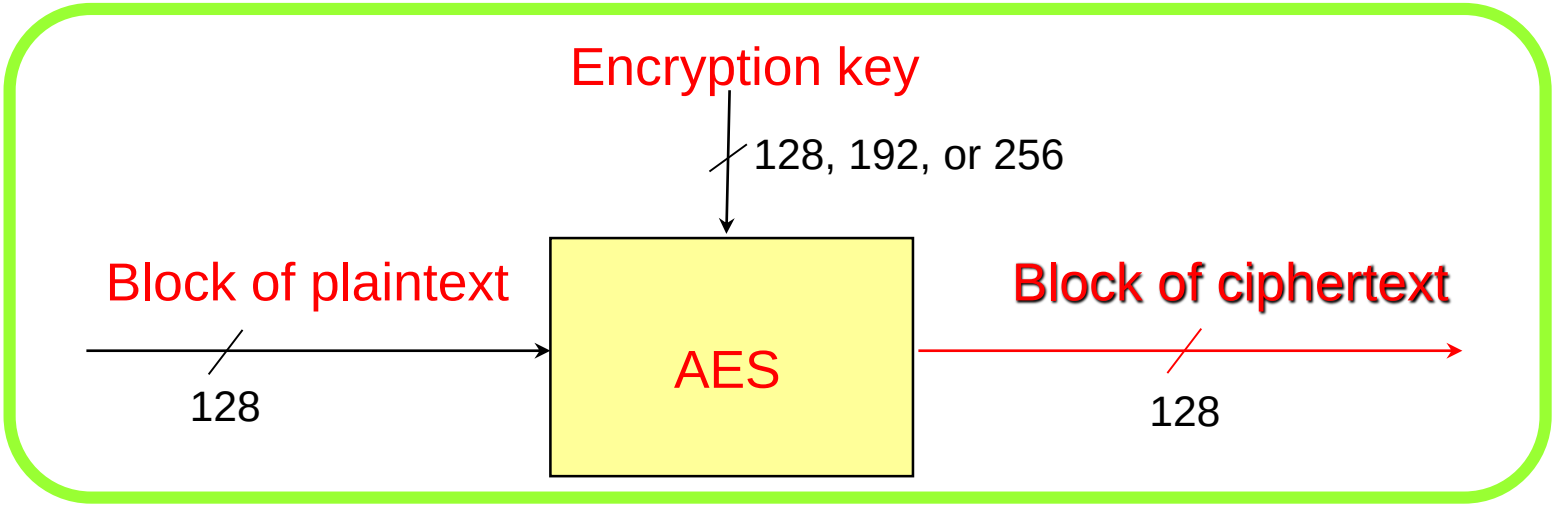
Triple DES (3DES)

- Key =$k_1k_2k_3$
- Key are longer (168 bits)
- Three times slower than DES



Advanced Encryption Standard (AES)

- In November 2001 the USA NIST announced *Rijndael* algorithm as the AES to replace DES as a FIPS 197
- Became effective in May 2002



AES

- For encryption, each round of a total of 10 consists of four stages:
  - Substitute Bytes — a non-linear substitution step where each byte is replaced with another according to a lookup table, an S-block.
  - ShiftRows — a transposition step where each row of the state is shifted cyclically a certain number of steps.
  - MixColumns — a mixing operation which operates on the columns of the state, combining the four bytes in each column using a linear transformation.
  - AddRoundKey — each byte of the state is combined with the round key; each round key is derived from the cipher key using a key schedule.
- Except for the last round in each case, all other rounds are identical.

AES-Encryption

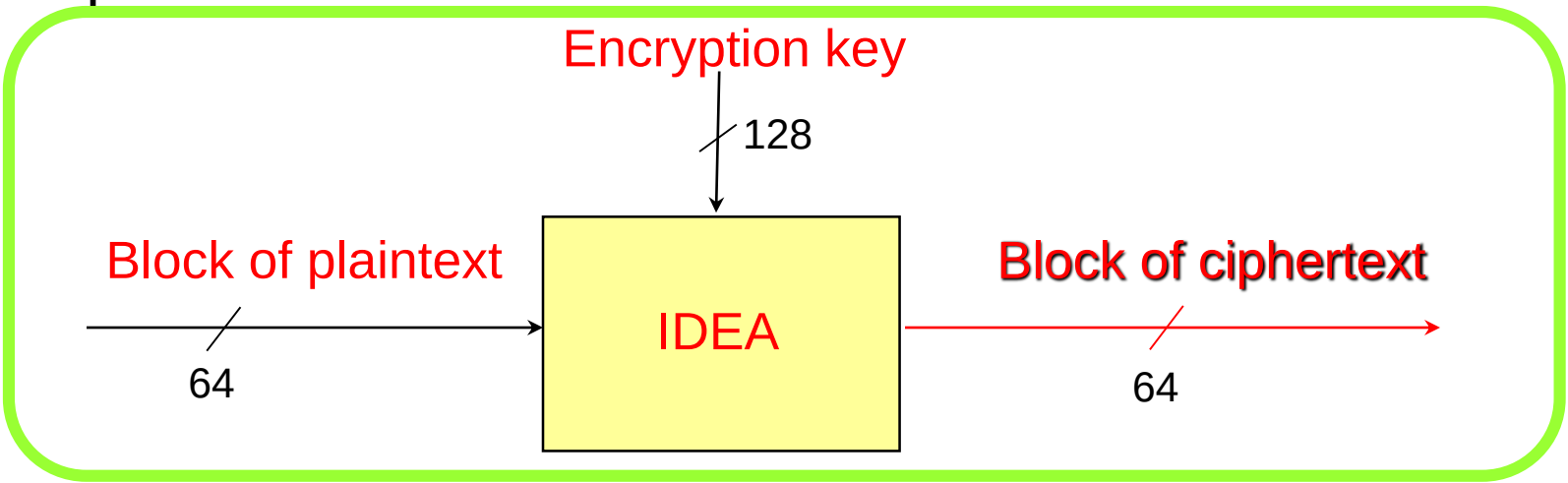
- The 128 bit plaintext block is depicted as a 4x4 matrix of bytes

byte0	byte4	byte8	byte12
byte1	byte5	byte9	byte13
byte2	byte6	byte10	byte14
byte3	byte7	byte11	byte15

- The block is copied into the **State** array, which is modified at each stage of encryption/decryption
  - After the final stage the State is copied into an output matrix
- The 128 bit key is expanded into an array of 44 words
- AES Animation

Other Block ciphers

- IDEA (International Data Encryption Algorithm)
  - Published in 1991
  - Operates on 64-bit blocks, and 128-bit key and produces blocks of 64 bits

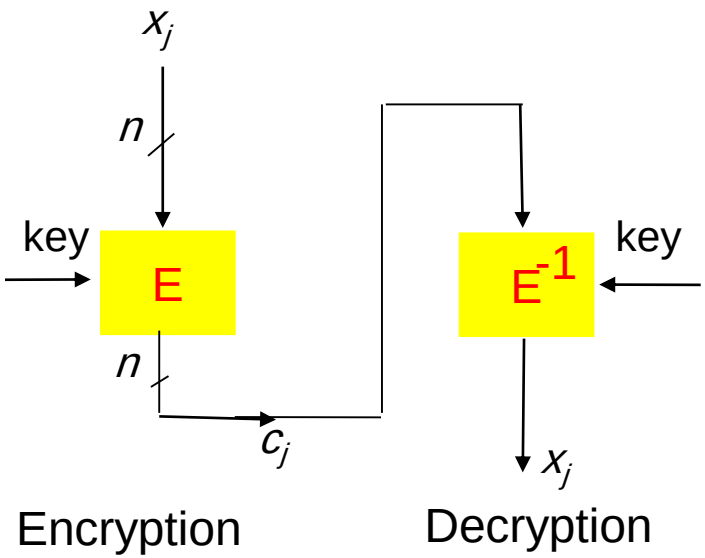


- Other ciphers: FEAL, SAFER, RC5, MARS, RC6, Serpent, Twofish….

Modes of operation

- NIST specifies five modes of operation
  - ECB -Electronic Code Book.
  - CBC -Cipher Block Chaining.
  - CFB -Cipher FeedBack.
  - OFB -Output FeedBack.
  - CTR – Counter

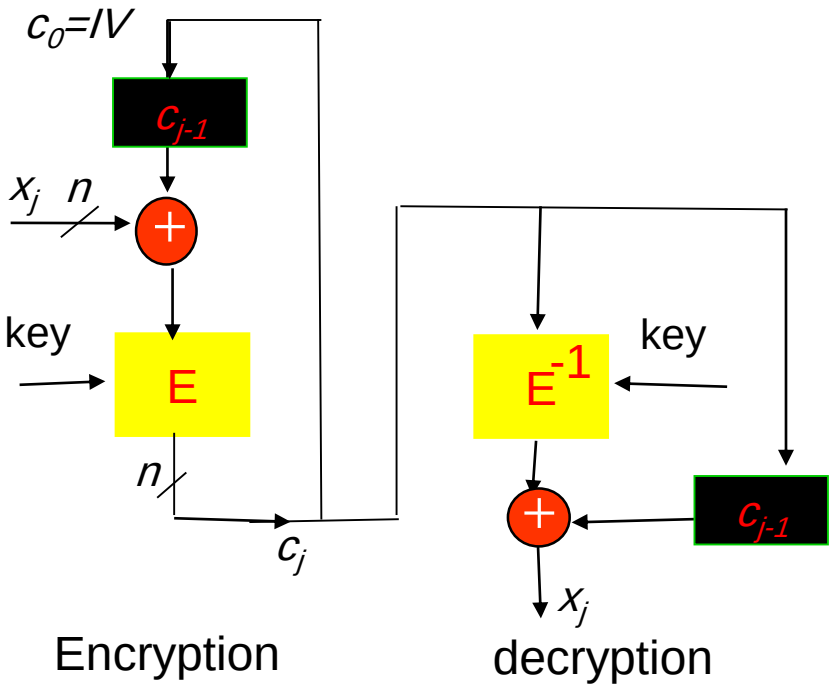
Electronic CodeBook (ECB)



ECB

- Identical plaintext blocks (under the same key) result in identical ciphertext.
- Chaining dependency: blocks are enciphered independently of other blocks.
- Error propagation: one or more bit errors in a single ciphertext affect decipherment of that block only.
- ECB is not recommended for messages longer than one block, or if keys are reused for more than one-block message
- Security of ECB may be improved by inclusion of random padding bits in each block.

Cipher-Block Chaining (CBC)



Cipher-Block Chaining (CBC)

CBC

- Identical plaintexts: identical ciphertext blocks result when the same plaintext is enciphered under the key and *IV*.

- Chaining dependency: a ciphertext c_j depends on x_j and all preceding plaintext blocks $\Rightarrow$ rearranging the order of ciphertext blocks affects decryption.

- Error propagation: a single bit error in ciphertext block c_j affects decipherment of c_j and c_{j+1}.

- Error recovery: CBC is *self-synchronizing* in the sense that if an error occurs in block c_j, c_{j+2} is correctly recovered.
- *IV* is not secret but needs integrity.

Properties of block ciphers

- The security of block ciphers mainly depends on the complexity of the encryption function whereas thus of stream ciphers depend on the keystream randomness.

- They can be used to provide confidentiality, data integrity, or authentication, and can even be used to provide the keystream generator for stream ciphers

Adv. and disadv. of symmetric cryptography

- Advantages
  - Fast
  - Reasonably well-understood
  - Standardized
  - Can be implemented in hardware easily
  - Exhaustive search attack hard (with large key size)
- Disadvantages
  - Key distribution
  - Single target
  - Still needs to be implemented in protocols