Chapter Four
Modern Symmetric Ciphers
(Stream Cipher and Block Cipher)

Stream cipher

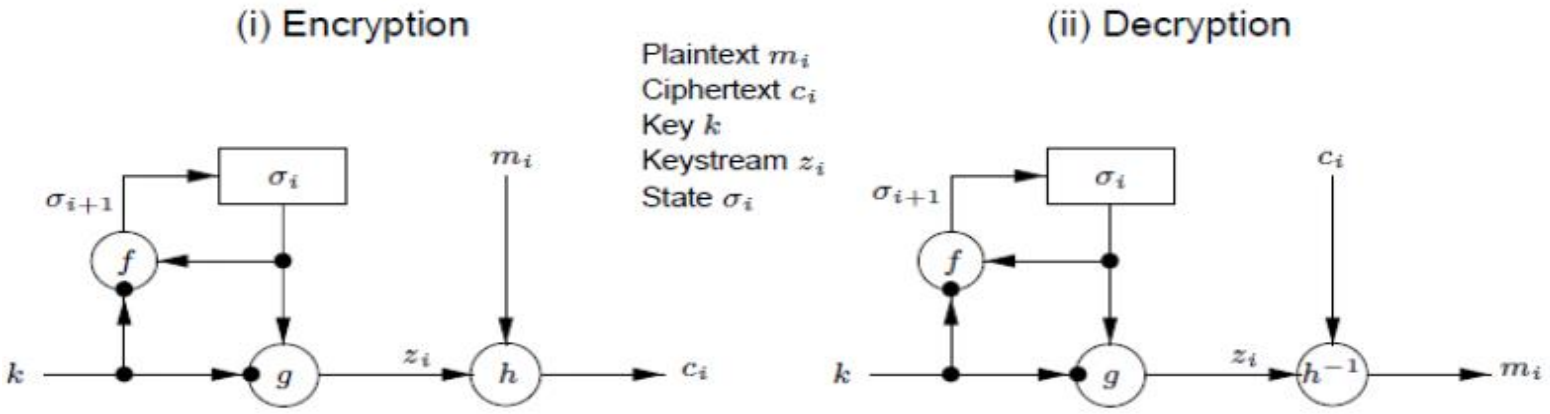
- Basic Idea of stream cipher comes from One-Time-Pad cipher: -

$$\text{Encryption} : c_i = m_i \oplus k_i \qquad i = 1,2,3,\ldots$$

m_i : plain-text bits.
k_i : key (key-stream) bits
c_i : cipher-text bits.

$$\text{Decryption} : m_i = c_i \oplus k_i \qquad i = 1,2,3,\ldots$$

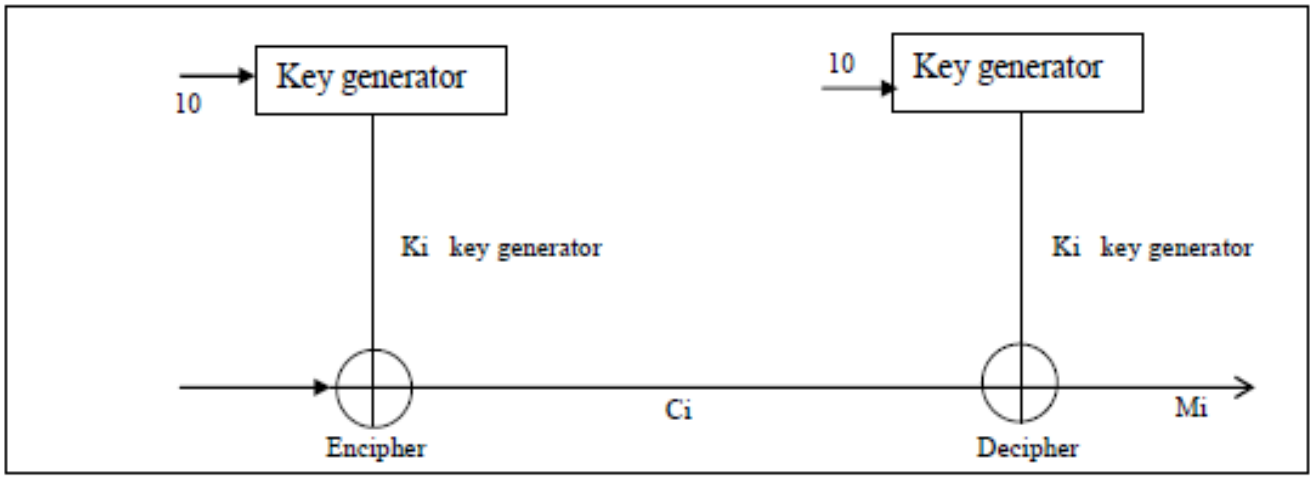
- The **drawback of** One-Time-Pad cipher is that key-stream should be as long as plain-text. Key distribution & Management difficult.
- **Stream Cipher** is the solution (in which key-stream is generated in pseudo-random fashion from relatively short *secret key*.
- **Pseudo-randomness :** sequences appears random to a computationally bounded adversary.



There are two different approaches to stream encryption they are; **synchronous methods** and **self-synchronous methods**.

1. Synchronous Stream Ciphers

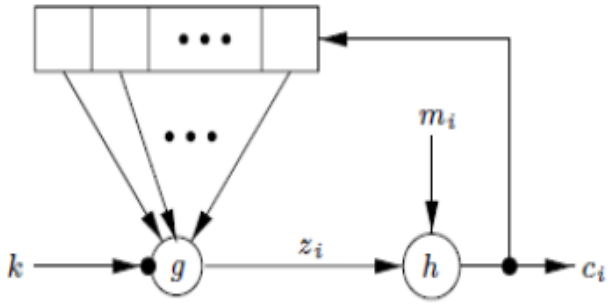
- Key-stream is independent of plain and cipher-text.
- Both sender &receiver must be synchronized.
- Resynchronization can be needed (This means that if a ciphertext is lost during transmission, the sender and receiver must resynchronize their key generators before they can proceed).
- Synchronous stream ciphers have the advantage of not propagating errors. A transmission error effecting one character will not affect subsequent characters. From another point of view; this is a disadvantage in that it is easier for an opponent to modify (with out detection) a single ciphertext character.
- Active attacks can easily be detected (disadvantage).



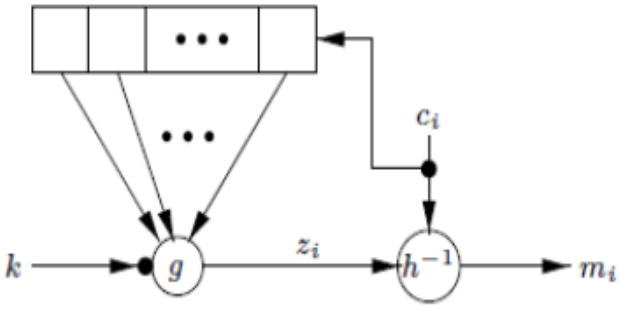
2. Self-Synchronizing Stream Ciphers

- Key-stream is a function of fixed number *t* of cipher-text bits. This is done by using a cipher feed back mode (CFB) because the ciphertext characters participate in the feed back loop.
- It is some times called **chaining**, because each ciphertext character depend on preceding cipher-text character (chain) the feed back
- Limited error propagation (up to *t* bits).
- Active attacks cannot be detected.
- At most *t* bits later, it resynchronizes itself when synchronization is lost.
- It helps to diffuse plain-text statistics.

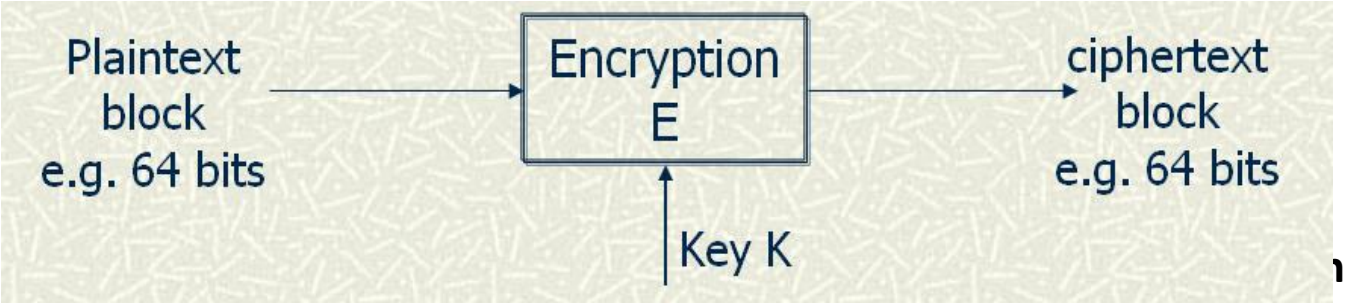
(i) Encryption



(ii) Decryption



- **Block cipher : -** an encryption scheme that encrypts a block of clear text into a block of cipher text of the same length. In this case, a block cipher can be viewed as a simple substitute cipher with character size equal to the block size.



- **n modes: -**

ECB Operation Mode. .١

– ECB stands for **Electronic Code Book.** Blocks of clear text are encrypted independently.

– Strength: it's simple.

– Weakness :

1- Repetitive information contained in the plaintext may show in the ciphertext, if aligned with blocks.

2. If the same message is encrypted (with the same key) and sent twice, their ciphertext are the same.

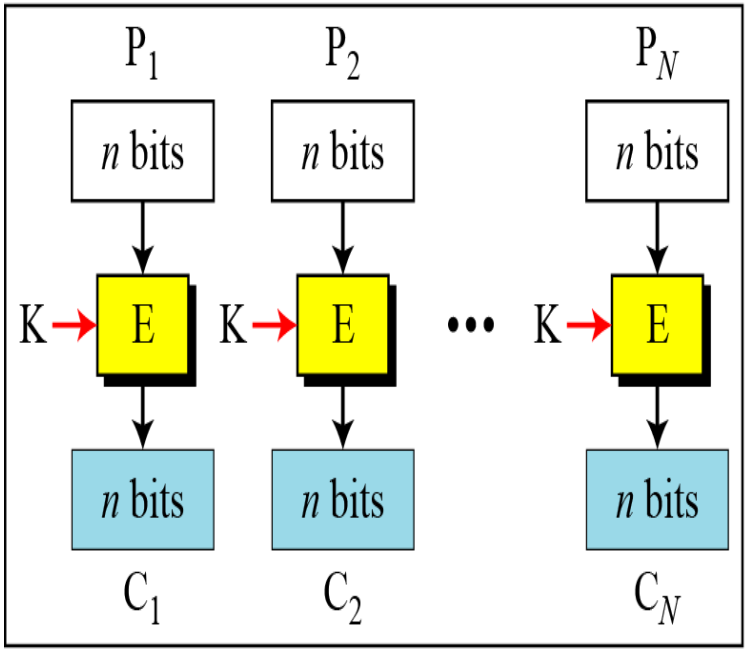
– Typical application: secure transmission of short pieces of information (e.g. a temporary encryption key)

Encryption: $C_i = E_K(P_i)$ Decryption: $P_i = D_K(C_i)$

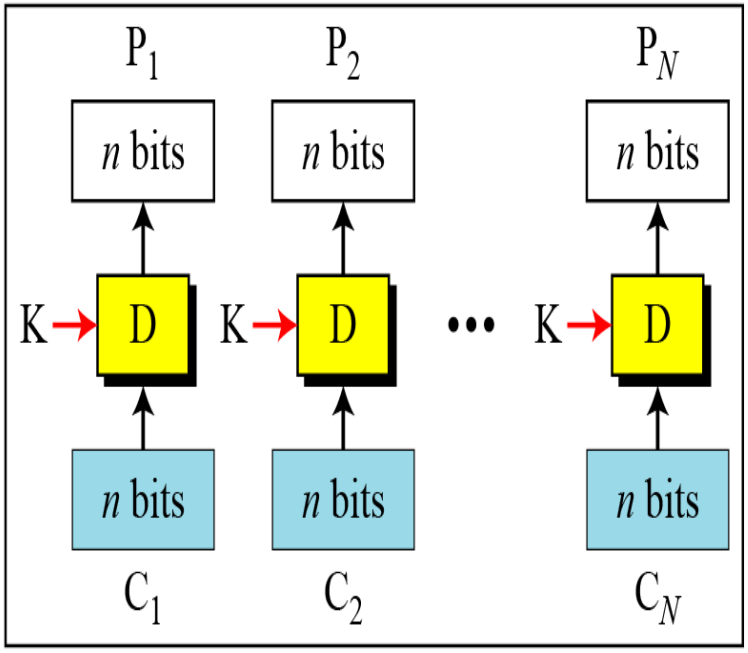
E: Encryption D: Decryption

P_i: Plaintext block i C_i: Ciphertext block i

K: Secret key



Encryption



Decryption