09/01/22. Modes of Encryption:-

1) Electronic code Book (ECB) mode.
   ↳ very Insecure.

2) stateless ciphertext Block chaining (CBC) mode.
   ↳ Randomization (or) Initialization vector (IV) should be different per message.

* Message Block → when a group of message blocks are divided as $(m_1, m_2, m_3 \ldots m_n)$ it is called as message Block.

* message → when a combination of different messages is combined to one, then it is called as a message. Ex:- $M = (m_1, m_2, m_3, \ldots, m_n)$

3) stateful ciphertext Block chaining (CBC) (or) chained CBC mode:

↳ We are chaining ciphertexts for blocks of messages.

$C_i' = E_K(C_n \oplus M_i')$; $IV' = M' = (M_1', \ldots, M_n')$.

↳ C_1, C_2, C_3 are generated by the challenger and is given to the adversary and also IV is also given.

$$C_1 = E_K(IV \oplus M_1')$$

$$C_2 = E_K(C_1 \oplus M_2)$$

$$C_3 = E_K(C_2 \oplus M_3)$$

$$M' = (M_4, M_5)$$

$$C_4 = E_K(C_3 \oplus IV \oplus M_1^0 \oplus C_3)$$

$$\therefore C_4 = E_K(IV \oplus M_1^0)$$

then if, $C_4 = C_1$, then $M_1^0 = M_1^b$ (i.e, $b=0$)

else, $C_4 \neq C_1$, then $M_1^0 \neq M_1^b$ (i.e, $b=1$)

09/06/22.

4.) Stateless output Feedback Mode (OFB):

↳ Cannot be done in parallel & the source should be given to every message.

5.) Stateless counter Mode (CTR):

↳ Take the initial counter value, and increament that counter value to 'n' times.

↳ Each counter value should be given to every message and can be done in parallel.