08/25/22:- **Block Cipher:-**

**Formal definition:**

$$E: \{0,1\}^k \times \{0,1\}^\lambda \rightarrow \{0,1\}^l$$

where,

$k$ → denotes the length of the key in the block.
$l$ → denotes the length of the bits in the block.

09/01/2022.

**Types of Attacks in Cryptography:-**

1.) Known cipher Text Attack. (KCA) → least dangerous.

2.) Known Plain Text Attack. (KPA)

3.) Choosen Plain Text Attack. (CPA)

4.) Adaptive CPA.

5.) Choosen cipher Text Attack. (CCA)

6.) Adaptive CCA. → most dangerous.

7.) Brute Force Attack (or) Exhaustive search Attack.