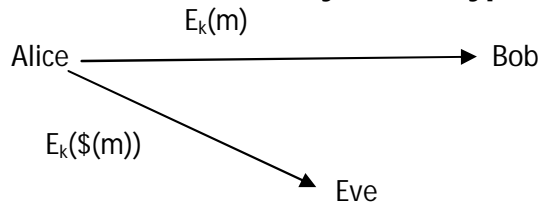


**Definition of Security for Encryption**

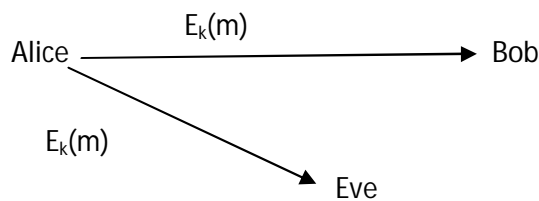


**IDEAL WORLD**

In Ideal, Eve learns only the following things

- 1) Message was sent
- 2) Length of message
- 3)  $\$(x)$  = a random string of same length as  $x$  and is non deterministic

Eve received a random string of length  $m$ .



**REAL WORLD**

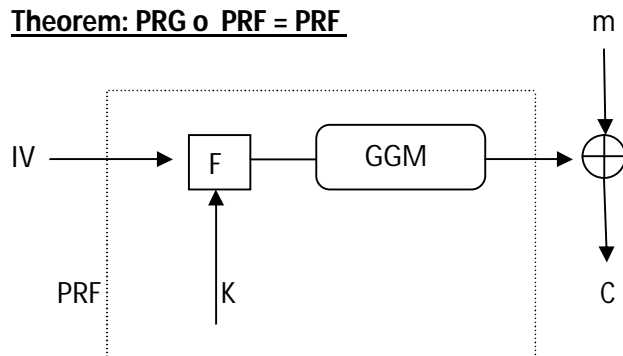
Eve can do chosen plain text attack but Eve should not be able to decide in which world she is.

**Definition.-** An encryption scheme is  $(t, q, \epsilon)$  is real or random (R or R)secure if for every A running in time  $\leq t$  and making at most  $q$  bits total oracle queries.

$$\text{Adv } A = |[\text{Pr}[A^{E_k} = 1 \mid k \leftarrow U_{\text{keys}}] - \text{Pr}[A^{E_k.\$} = 1 \mid k \leftarrow U_{\text{keys}}]| \leq \epsilon$$

Note: A is given oracle access to  $E_k$ , Plaintext attack is done and A recovers  $m$ . In second case, When A gives plaintext message to encryption oracle, Encryption oracle chooses completely string and then encrypts it. So even if A decrypts it, A gets random string.

**Theorem: PRG o PRF = PRF**

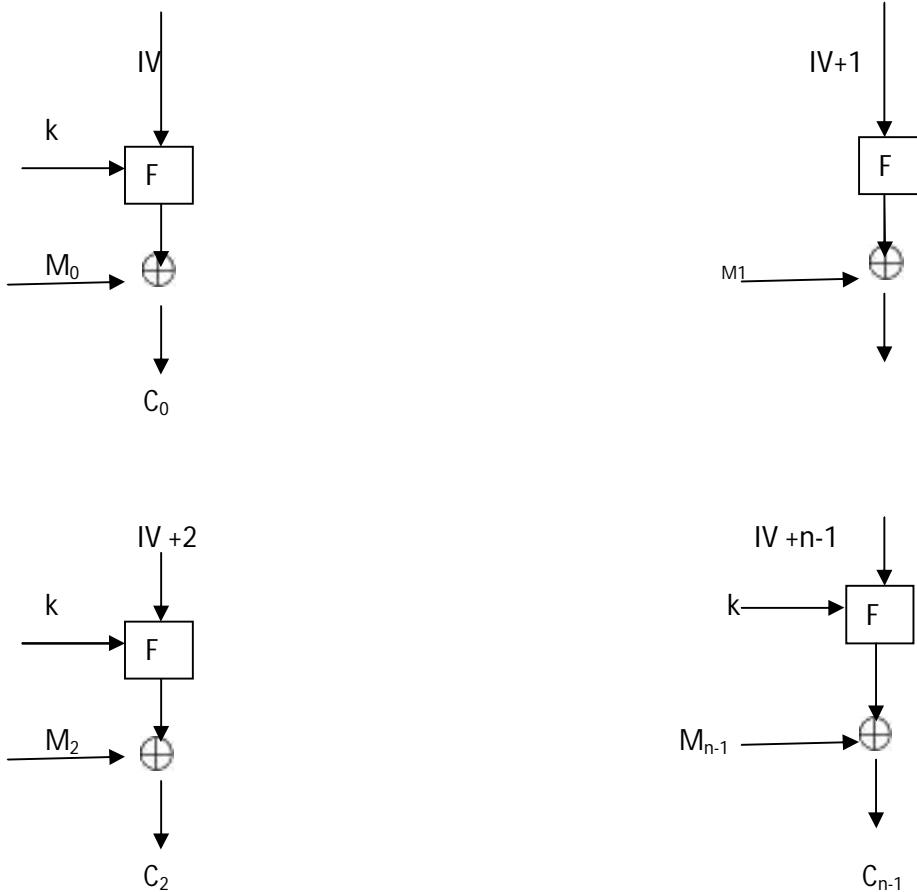


A PRF is  $F\{0,1\}^{128} * \{0,1\}^{128} \rightarrow \{0,1\}^{128}$

Output :Keystream is only 128 bits.

Hence **GGM is used to expand the keystream**

### Modes of operation

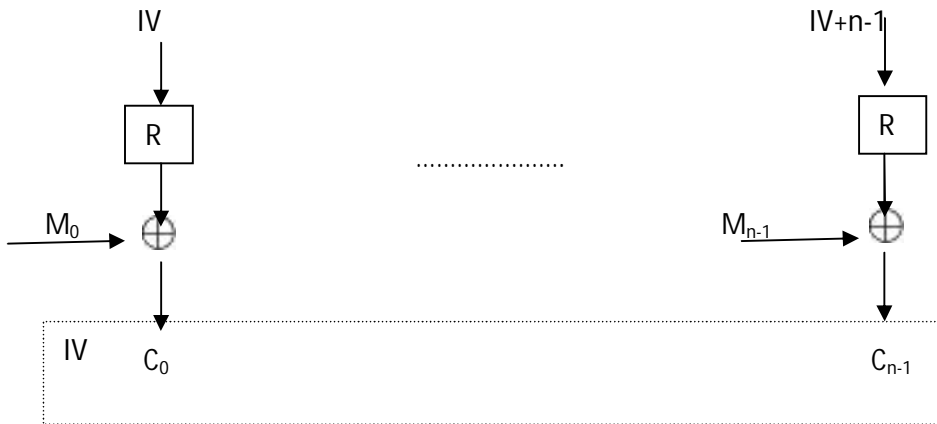


### CTR mode

- 1)  $CTR^F$  mode – Pick Random IV at boot time.  
It is complex to implement as it has to deal with Synchronization recovery if crash occurs.  
It provides better security.
- 2)  $CTR^S$  mode.- Pick Random IV per message.  
It is simple but less secure because of Birthday Paradox.

**Theorem** – If  $F$  is a  $T, q, \epsilon$  secure PRF, then  $CTR^F$  is  $t-O(q), \min(q, |ctr s|), \epsilon$  R or R secure  
 Note:  $q$  is total no of message block.

**Fact**  $U_i \text{ XOR } D_i = U_i$



Is equivalent to



By Data Processing inequality

$$CTR^R \sim CTR^{F(k)}$$

By Logic  $CTR^R = CTR^{F(k) \circ \$}$  { using the above fact}

Therefore  $\text{CTR}^{F(k)} \sim \text{CTR}^{F(k) \circ \$}$

**Hence we can't distinguish whether in REAL WORLD or IDEAL WORLD WITH ENCRYPTED  
RANDOM MESSAGE**

**Theorem:**

If  $F$  is a  $t, q, \epsilon$  secure PRF then  $\text{CTR}^F$  is  $t - O(q)$ ,  $q, \epsilon + q^2 / 2^{|ctr|}$  R or R secure

Note :  $q^2 / 2^{|ctr|}$  is Probability that after  $A$  makes  $q$  queries, there is a collision.