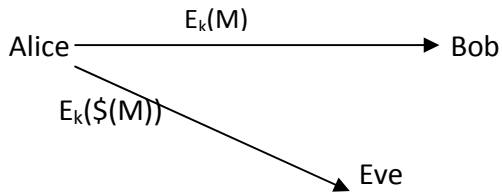


Network Security Notes (September 21 2009)

By Supreet Padhi

Definition of Security for encryption

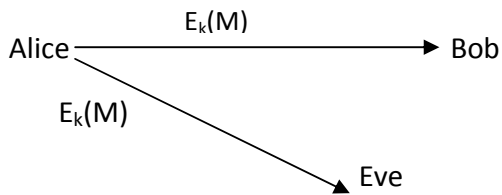
Ideal World



In ideal world scenario Eve is allowed to learn following things

- A message was sent.
- Length of the message
- $\$(x)$ =a random string of same length of x.

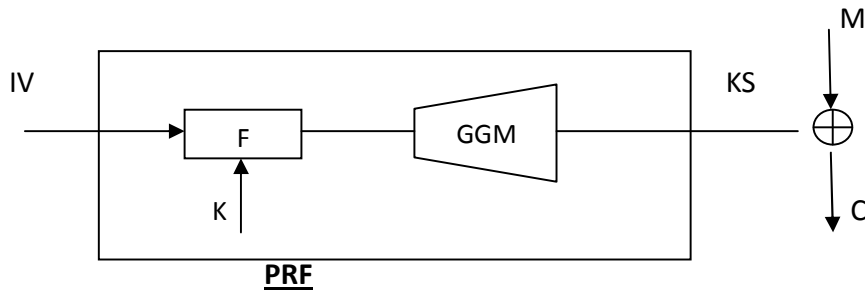
Real World



Definition: An encryption scheme is (t, q, ϵ) – real or random (R-or-R) if for all A running in time $\leq t$ and making at most q oracle queries.

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

Theorem : PRG . PRF = PRF

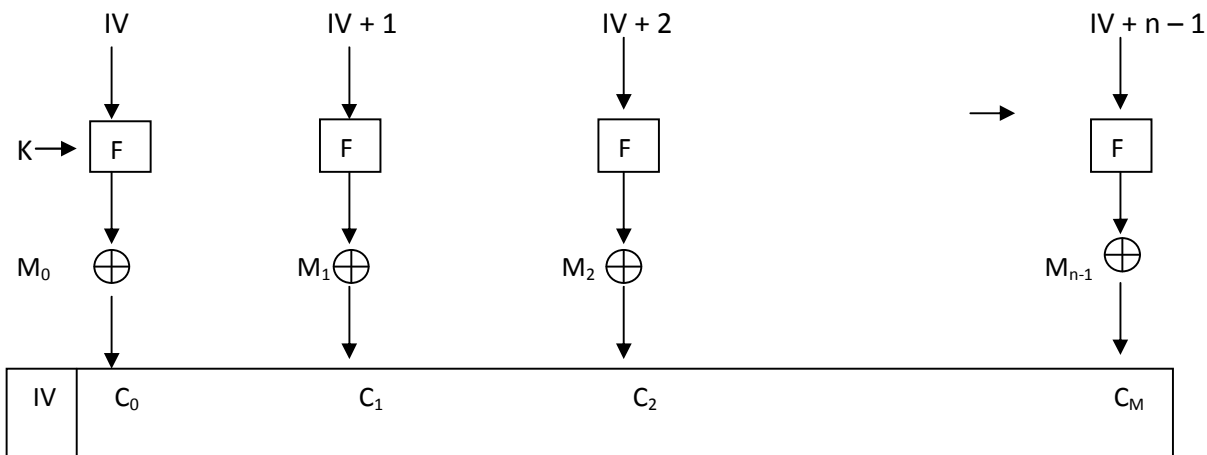


IV choice can be

- Random
- Counter

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

Here the KS will be always 128 bits.



Modes of Operation

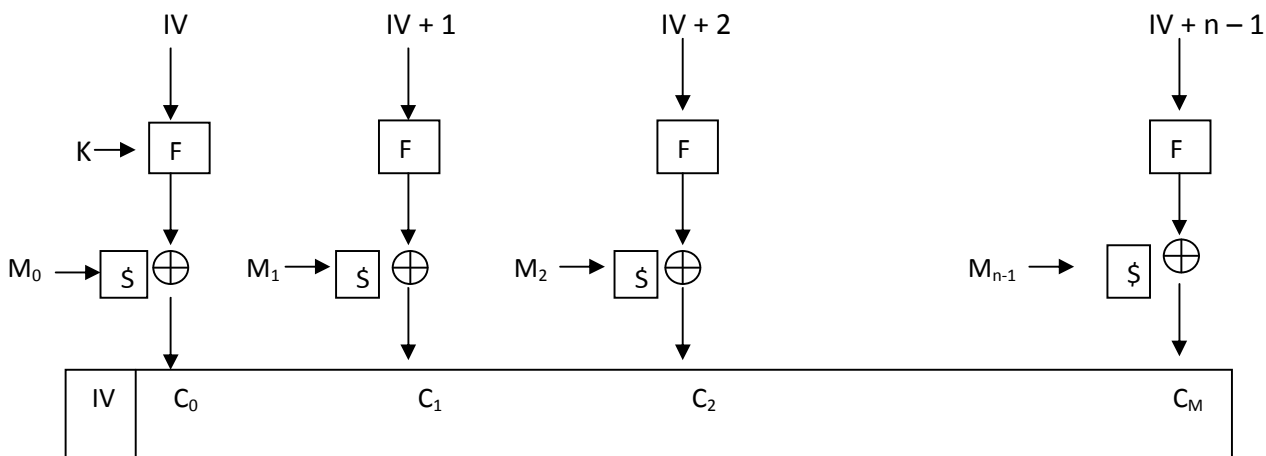
- CTR^F mode - Random IV is picked at start. It is secure and complex. But synchronization problem may occur if the system goes down.
- CTR^F o \$ mode – Random IV is picked per message. It is simple but may suffer from birthday paradox.

Theorem: If F is (t,q, ε) secure PRF then CTR^F is (t - O(q), min(q, |ctr s|), ε) is R or R secure
 Note- q is total number of message blocks. |ctr s| is the counter space

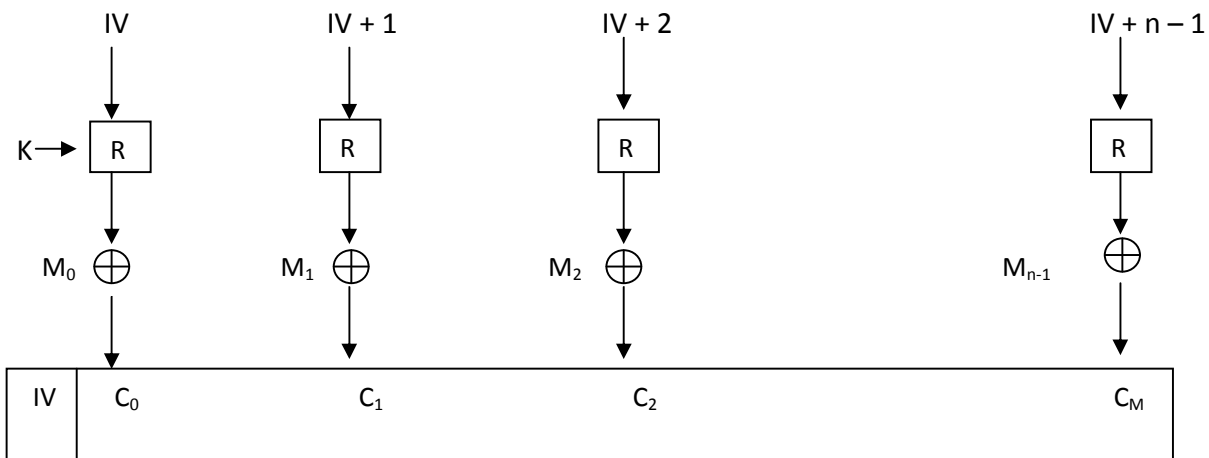
Proof:

Fact: $U_i \oplus D_i = U_i$

CTR^{Fk} o \$ mode



CTR^R mode



By DPI- PRF

$$\text{CTR}^R \sim \text{CTR}^{F_k}$$

By logic and using above fact, random function R produces random uniform output and $F_k \circ \$$ also produces random uniform output thus

$$\text{CTR}^R = \text{CTR}^{F_k} \circ \$ \text{ if } (q \leq | \text{ctr s} |)$$

Hence $\text{CTR}^{F_k} \sim \text{CTR}^{F_k} \circ \$$.

Theorem: if F is a (t, q, ϵ) secure PRF, then $\text{CTR}^{F_k} \circ \$$ is $(t - O(q), q, \epsilon + \frac{q^2}{2 \cdot |\text{ctr s}|})$ R or R secure.