

Network Security Notes (September 25 2009)

By Supreet Padhi

- PRG \Rightarrow Stream cipher
- PRF with PRG \Rightarrow Stream cipher
- CTR with PRF \Rightarrow Real or Random (R-or-R) secure encryption
- CBC with PRP \Rightarrow (R-or-R) secure
- Semantic security \Rightarrow (R-or-R) secure
 - \Leftrightarrow Left-or-Right secure
 - \Leftrightarrow IND-CPA (Indistinguishability under chosen plain text attack)

Assume E_k be a symmetric encryption scheme and $\$ (x)$ = random string of the same length as x

$$E_k \sim E_k \circ \$$$

Adv A = $| P_r [A^{E_k} = 1] - P_r [A^{E_k \circ \$} = 1] |$ is small

$$\text{PRF: } | P_r [A^{F_k} = 1] - P_r [A^R = 1] | \leq \epsilon$$

PRP: A function $F: \text{Keys} \circ X \rightarrow X$ is a (t, q, ϵ) pseudo random permutation if for all adversaries A running in time $\leq t$ and making at most q oracle queries.

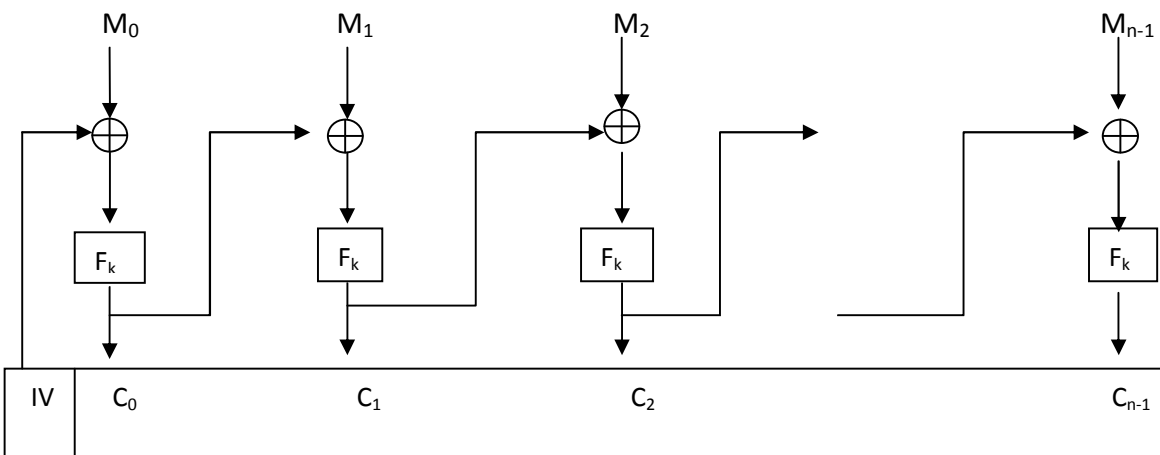
$$| P_r [A^{F_k} = 1 \mid K \leftarrow \text{Keys}] - P_r [A^P = 1 \mid P \leftarrow \text{Perms}(X)] | \leq \epsilon$$

Advantage of PRP is invertible

$$\text{AES: } \{0,1\}^{128} \times \{0,1\}^{128} \rightarrow \{0,1\}^{128}$$

$$\text{DES: } \{0,1\}^{56} \times \{0,1\}^{64} \rightarrow \{0,1\}^{64}$$

Cipher Block Chaining(CBC)



There are two modes for CBC

- CBC^F – IV is set to current value of the counter. The counter is then incremented each time a message is encrypted.
- $\text{CBC}\F – IV is chosen at random by encryption algorithm. This choice is made independently each time the algorithm is invoked.

Theorem: $\text{CBC}\F is $(t-O(q), q, \epsilon + \frac{q^2}{2^{n+1}})$ R-or-R secure if F is a (t, q, ϵ) PRP, where n is the length of the IV.