

Network Security

Sumeet P Dash

September 25, 2009

Key points

- PRG itself mightn't result in secure stream cipher.
- PRF used in conjunction with PRG helps devise secure stream cipher.
- PRF in CTR (counter) mode provides Real or Random (R-or-R) secure encryption.
- Semantic security is an important aspect of any cryptosystem. Some of its synonyms are R-or-R secure, Left-or-Right secure and IND – CPA (Indistinguishability under chosen plaintext attack).

PRP (Pseudo Random Permutation)

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

$$|\Pr[A^{F_k} = 1 \mid k \leftarrow \text{Keys}] - \Pr[A^P = 1 \mid P \leftarrow \text{Perm}(X)]| \leq \epsilon$$

Advantage of PRP is inevitability.

e.g.-

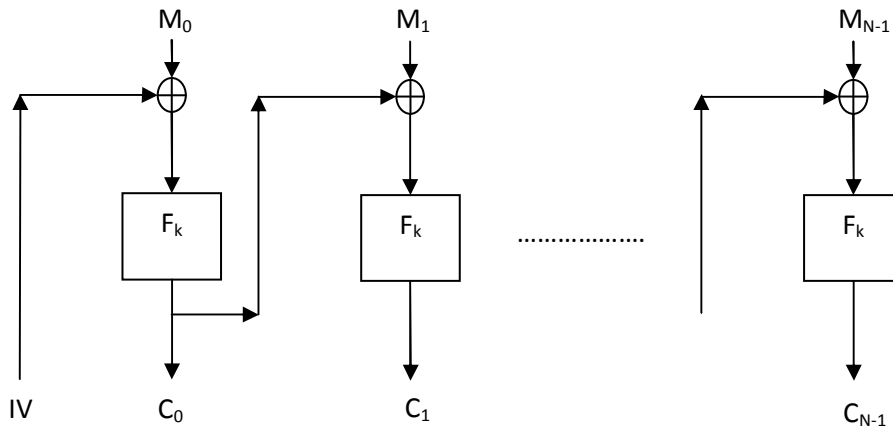
$$\text{AES: } \{0, 1\}^{128} \times \{0, 1\}^{128} \rightarrow \{0, 1\}^{128}$$

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

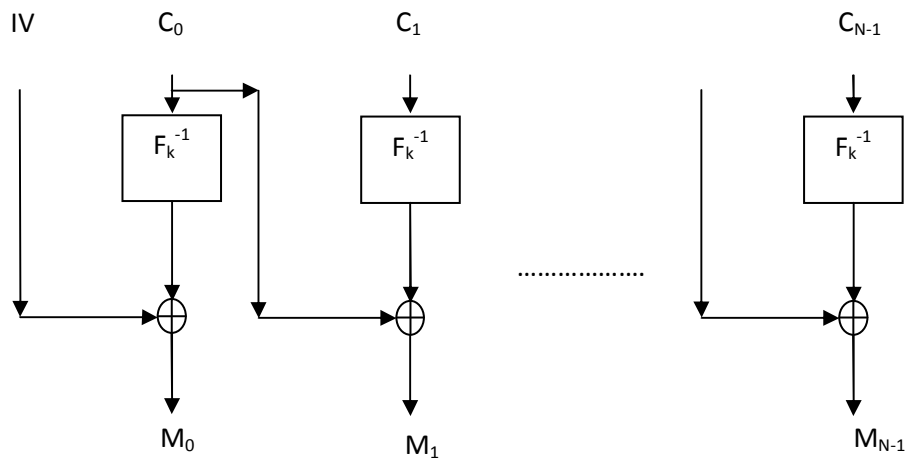
Cipher Block Chaining (CBC)

In the cipher-block chaining (CBC) mode, each block of plaintext is XORed with the previous ciphertext block before being encrypted.

CBC Encryption



CBC Decryption



It has two internal modes of operation.

- (i) CBC^F : The value of IV is chosen to be the current value of the counter and the counter is then increased stepwise for subsequent encryptions.
- (ii) $\text{CBC}^{\$F}$: IV is chosen randomly.

Theorem:

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