

Review of last class

- PRG did not work for stream cipher
- PRF with PRG is good for stream cipher
- CTR with PRF provides Real or Random Secure Encryption
- Assume E_k is deterministic in the definition of security for encryption
If \$ is randomized: - Deterministic encryption is not secure, infact we want it to be non secure.
 Eve will always get a randomized string
If \$ is deterministic- If IV repeats , Eve can tell in which world she is because she will receive same output for same M.
Hence \$ is Randomized

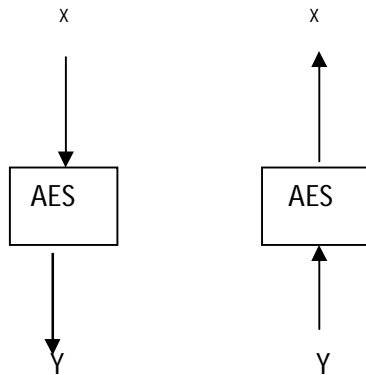
PRP:-A function $F:Keys * X \rightarrow X$ is a (t, ϵ) secure pseudo random permutation if for all adversaries A running in time $\leq t$ and making at most q oracle queries

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

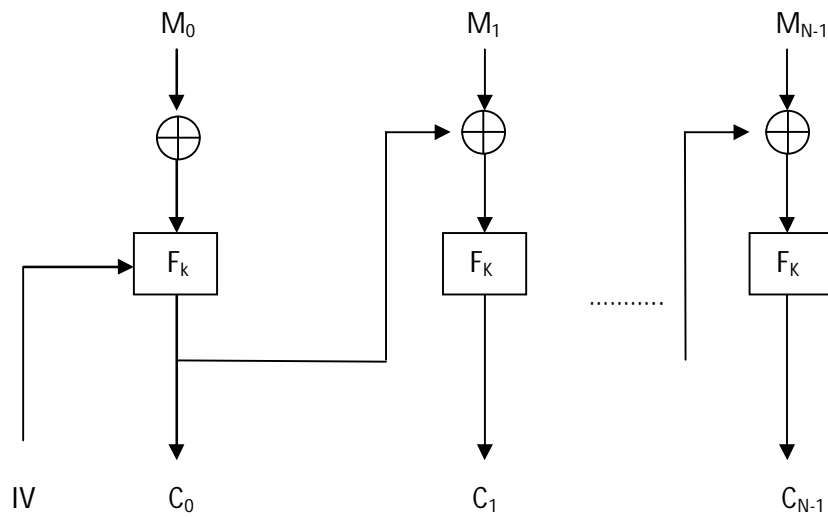
Advantage of PRP- Invertibility

Note:- AES $\{0,1\}^{128} * \{0,1\}^{128} \rightarrow \{0,1\}^{128}$

DES $\{0,1\}^{56} * \{0,1\}^{64} \rightarrow \{0,1\}^{64}$

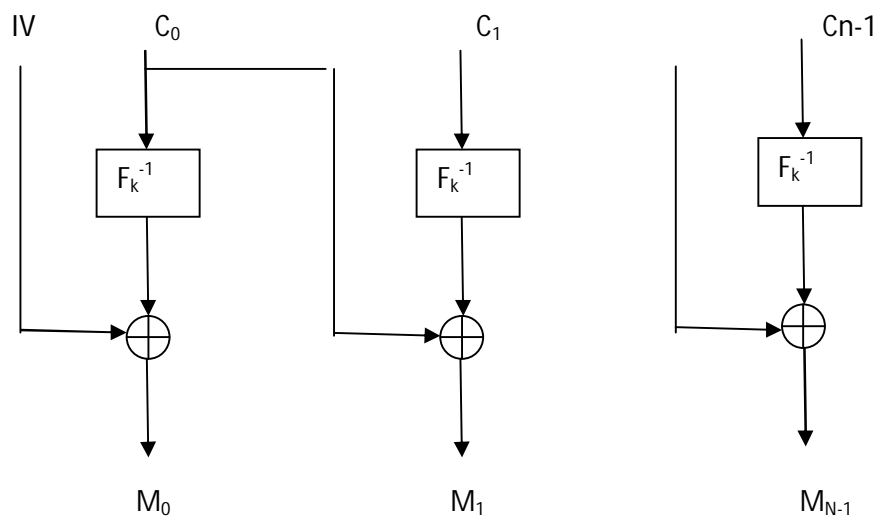


CBC with PRP is Real or random secure and can be run backwards



Encryption in CBC mode

Note:- F_k is PRP here



DECRYPTION IN CBC MODE

CSE 508 Network Security
09-25 lecture notes
Submitted by Vijit Kharbanda

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