Cryptography

Lecture 9

Announcements

- HW4 due on Wednesday, 3/1

Agenda

- Last time:
  - Pseudorandom Functions (PRF) (K/L 3.5)
  - CPA-secure encryption from PRF (K/L 3.5)
- This time:
  - Class Exercise on PRF's
  - PRP (Block Ciphers) (K/L 3.5)
  - Modes of operation (K/L 3.6)

Block Ciphers/Pseudorandom Permutations

Definition: Pseudorandom Permutation is exactly the same as a Pseudorandom Function, except for every key k, F_k must be a permutation and it must be indistinguishable from a random permutation.

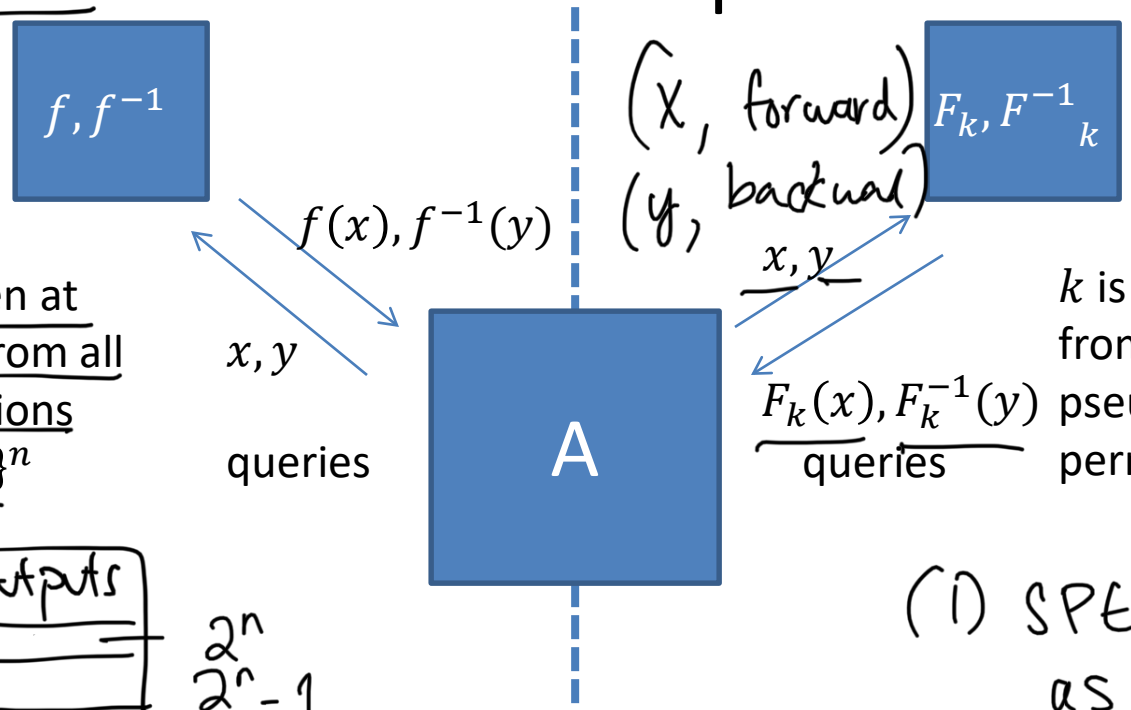
one-to-one/onto $\Leftrightarrow$ bijection

Strong

Ideal

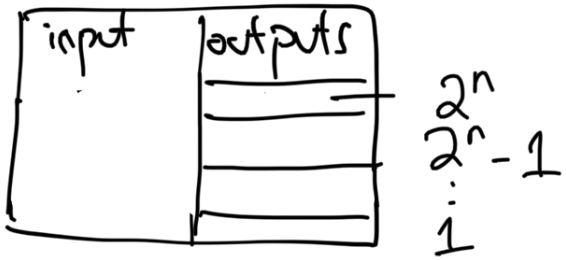
Pseudorandom Permutation (PRP) Block Cipher

Real



f is chosen at random from all permutations over $\{0,1\}^n$

k is chosen at random from $\{0,1\}^n$. F_k is the pseudorandom permutation indexed by k.



(1) SPEC of F as a 2-input is public

(2) Choose a random key k

PRP: Any efficient A cannot tell which world it is in.

$$\left|\Pr[A^{f}() = 1] - \Pr[A^{F_k}() = 1]\right| \leq negligible$$

PRF: $(2^n)^{2^n} \longrightarrow n2^n$

$(2^n)! \Rightarrow 2^n \log 2^n = n2^n$

$\log(N!) \sim N \log N$

Strong Pseudorandom Permutation

Definition: Let $F: \{0,1\}^* \times \{0,1\}^* \to \{0,1\}^*$ be an efficient, length-preserving, keyed permutation. We say that F is a strong pseudorandom permutation if for all ppt distinguishers D, there exists a negligible function $negl$ such that:

$$\left|\Pr\left[D^{F_k(\cdot),F^{-1}{}_k(\cdot)}(1^n) = 1\right] - \Pr\left[D^{f(\cdot),f^{-1}(\cdot)}(1^n) = 1\right]\right| \leq negl(n).$$

where $k \leftarrow \{0,1\}^n$ is chosen uniformly at random and f is chosen uniformly at random from the set of all permutations mapping n-bit strings to n-bit strings.

Modes of Operation—Block Cipher

Not Secure

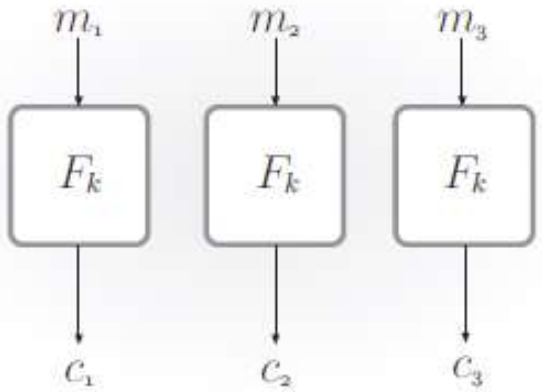


FIGURE 3.5: Electronic Code Book (ECB) mode.

$$c_i = F_k(m_i)$$

$$m_i = F_k^{-1}(c_i)$$

FIGURE 3.6: An illustration of the dangers of using ECB mode. The middle figure is an encryption of the image on the left using ECB mode; the figure on the right is an encryption of the same image using a secure mode.

Not indist. in presence of eavesdropper

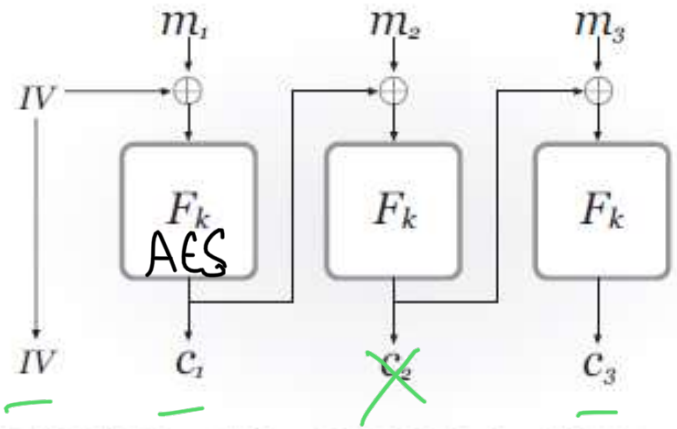


FIGURE 3.7: Cipher Block Chaining (CBC) mode.

Enc

$$c_0 = IV \text{ (rand chosen)}$$

$$c_i = F_k(c_{i-1} \oplus m_i)$$

Dec

$$m_i = F_k^{-1}(c_i) \oplus c_{i-1}$$

AES-128-CBC

Modes of Operation—Block Cipher

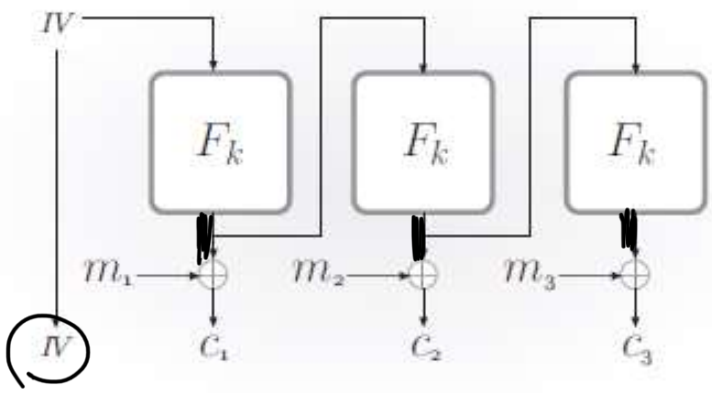


FIGURE 3.9: Output Feedback (OFB) mode.

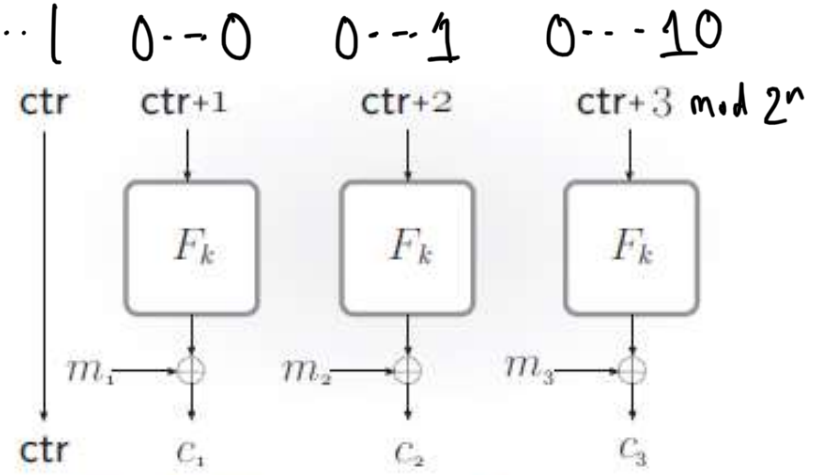


FIGURE 3.10: Counter (CTR) mode.

Enc: $S_0 = IV$, $S_i = F_K(S_{i-1})$, $c_i = m_i \oplus S_i$

Dec: $S_i = IV$, $S_i = F_K(S_{i-1})$, $m_i = c_i \oplus S_i$

Enc: $ctr \in [0, \ldots, 2^n - 1]$, $c_i = F_k(ctr+i) \oplus m_i$

Dec: $m_i = F_k(ctr+i) \oplus c_i$

Which ones have parallelizable Enc/Dec

Motivate Block Ciphers

We saw CPA secure enc w/ PRF

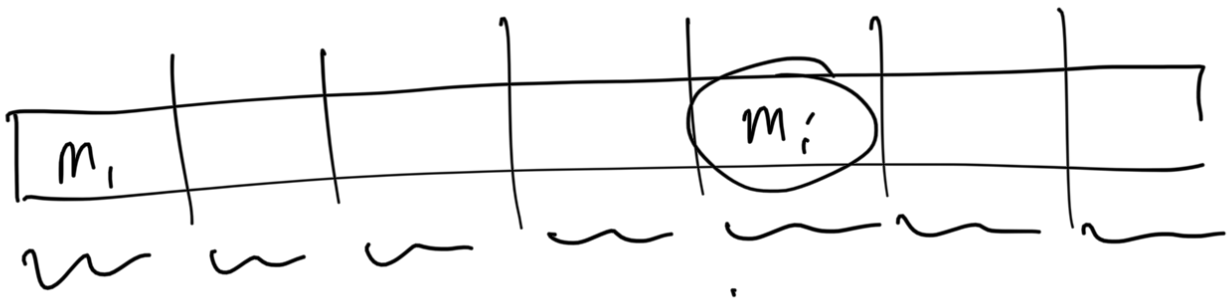
$m \in \{0,1\}^n$

$r \leftarrow \{0,1\}^n$

$c_1 = r$

$c_2 = m \oplus F_K(r)$

$m = \{0,1\}^{\ell \cdot n}$



$c_1^1 = r_1$

$c_2^1 = m_1 \oplus F_K(r_1)$

$c_1^i = r_i$

$c_2^i = m_i \oplus F_K(r_i)$

$\bar{c} \in \{0,1\}^{2\ell \cdot n}$

n bit key

n bit input

n bit output

$F: \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}^n$

block size