Cryptography

Lecture 8

Announcements

- HW2 due on Monay, 2/26

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.

F_k

input	output

2^n

$F_k : \{0,1\}^n \rightarrow \{0,1\}^n$

$F_k(x) = y$

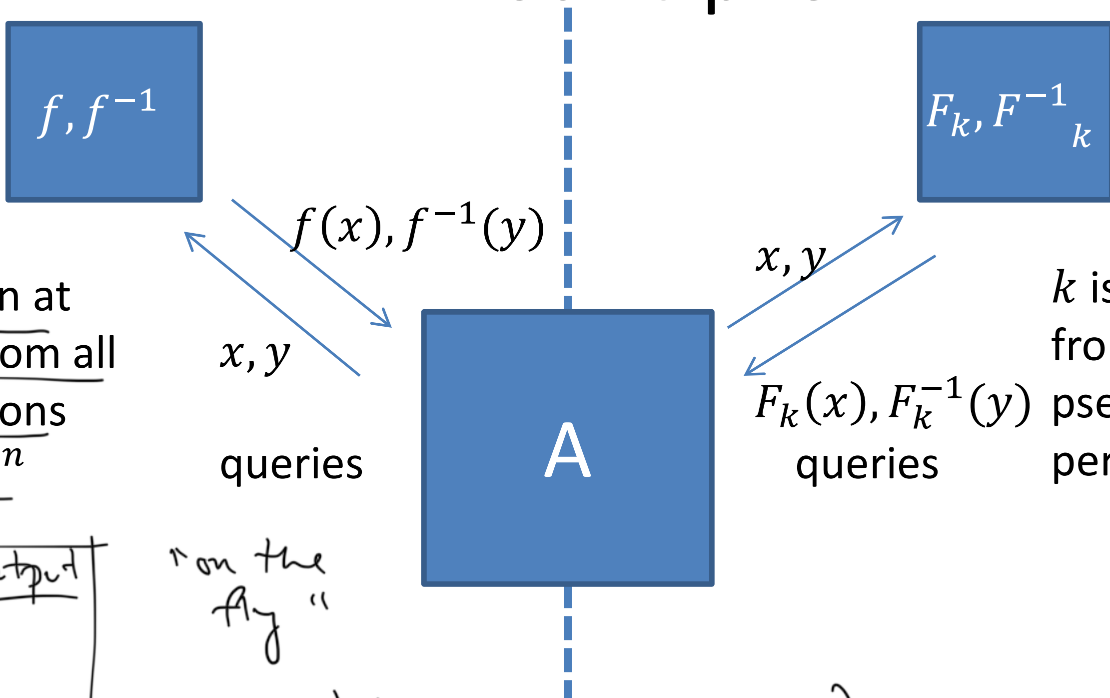
$F_k^{-1}(y) = x$

(Strong)

Pseudorandom Permutation (PRP) Block Cipher

Ideal

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.

input	output

"on the fly"

Stirling:

$\log_2(N!) \approx N \log_2(N)$

$(2^n)!$ $\quad \log_2((2^n)!) \approx n \cdot 2^n$

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

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

$2^{(2^n)}$

Motivation: Modes of Operation

outputted: $(\underbrace{r}_{n\text{bits}}, \underbrace{F_k}_{n\text{bits}}(r) \oplus \underbrace{m}_{n\text{bit}})$

$100 \cdot n$

m | m_1 | m_2 | $\cdots$ | m_{100} |

$c = (r_1, F_k(r_1) \oplus m_1) \cdots\cdots (r_{100}, F_k(r_{100}) \oplus m_{100})$

Drawbacks: ① As much rand. as the message

② Rate 2 encoding

(ciphertext length is 2x message length).

Want: $\lim_{m \to \infty} \frac{c_\ell}{m_\ell} = 1.$

Strong Pseudorandom Permutation

Definition: Let $F: \{0,1\}^* \times \{0,1\}^* \rightarrow \{0,1\}^*$ 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.

$F_k(m_1) \oplus F_k(m_1) = 0$

Modes of Operation—Block Cipher

Not Secure

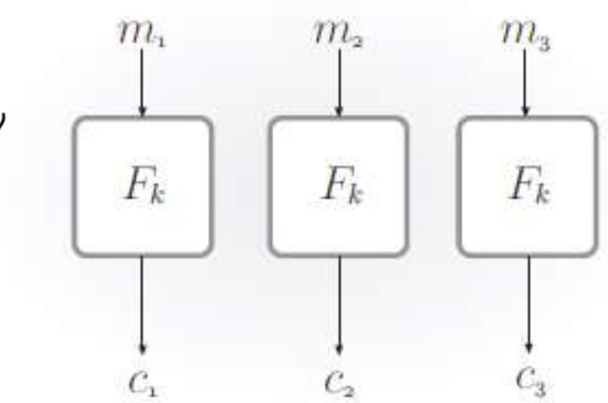


FIGURE 3.5: Electronic Code Book (ECB) mode.

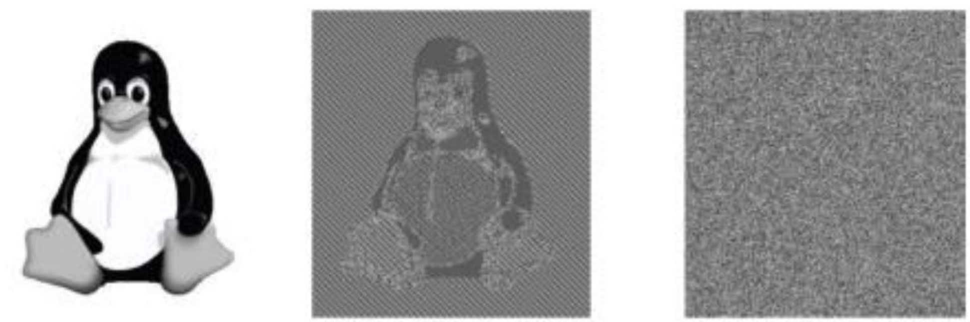
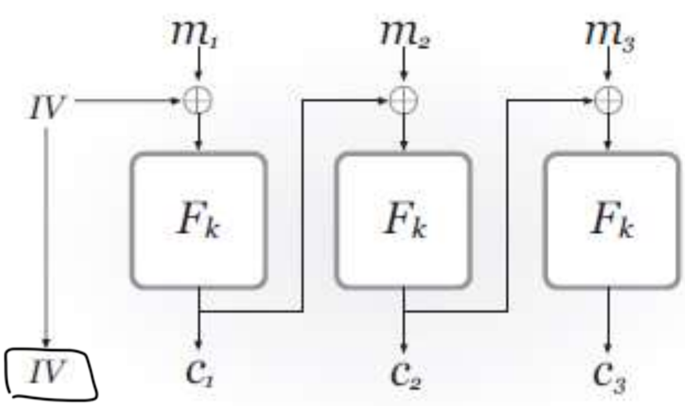


FIGURE 3.6: An illustration of the dangers of using ECB mode. The middle figure is an encryption of the image on the left using ECB mode; the figure on the right is an encryption of the same image using a secure mode.



rand from $\{0,1\}^n$

FIGURE 3.7: Cipher Block Chaining (CBC) mode.

$c_0 = IV$

$c_{i+1} = F_k(c_i \oplus m_{i+1})$

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

Modes of Operation—Block Cipher

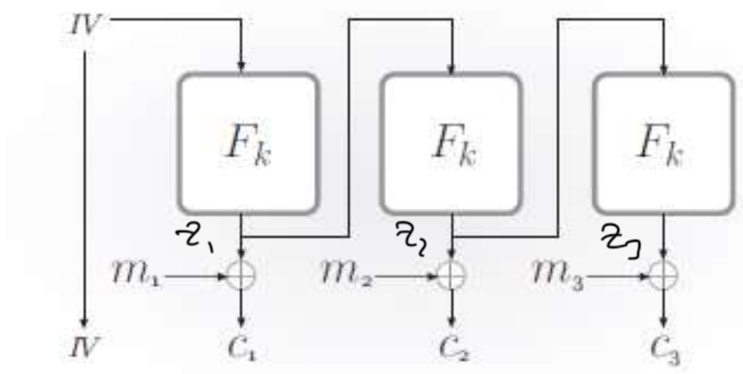


FIGURE 3.9: Output Feedback (OFB) mode.

$\mathbb{Z}_{2^n}$

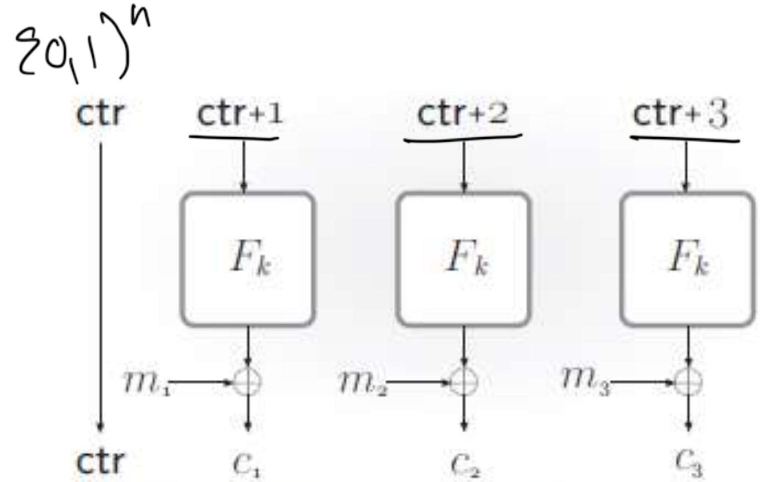


FIGURE 3.10: Counter (CTR) mode.

$z_0 = IV$

$z_{i+1} = F_k(z_i)$

$c_{i+1} = m_{i+1} \oplus z_{i+1}$

$m_{i+1} = c_{i+1} \oplus z_{i+1}$

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

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

fully parallelizable

* Which ones require PRP
  Which ones work with PRF

(CFB - Cipher Feedback Mode)