

Cryptography

Lecture 8

Announcements

- HW2 due on Monay, 2/26

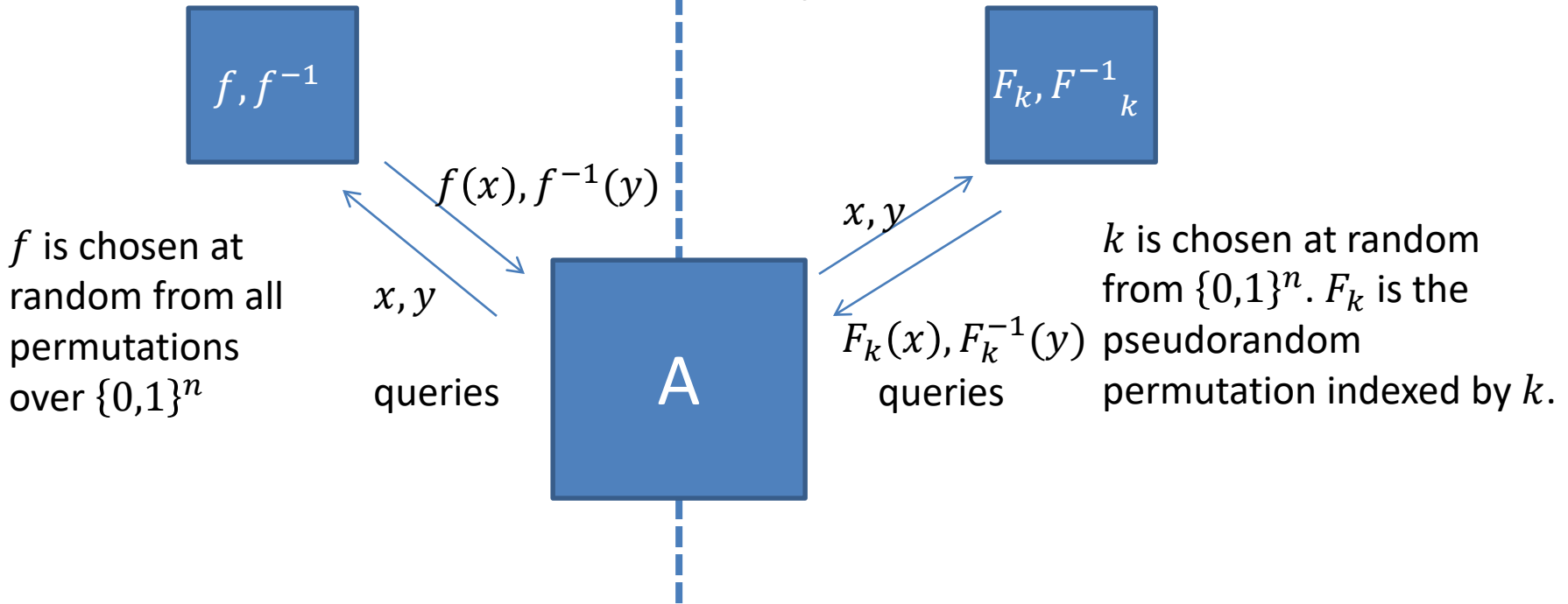
Agenda

- 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.

Pseudorandom Permutation (PRP) Block Cipher



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

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

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:

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

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

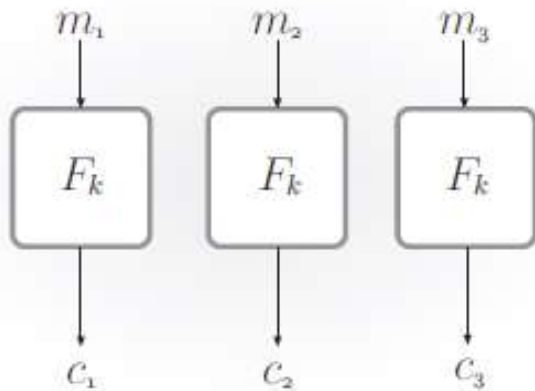


FIGURE 3.5: Electronic Code Book (ECB) mode.

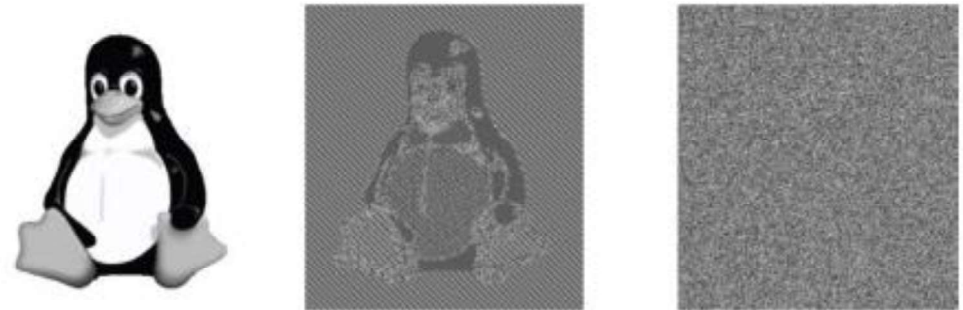


FIGURE 3.6: An illustration of the dangers of using ECB mode. The middle figure is an encryption of the image on the left using ECB mode; the figure on the right is an encryption of the same image using a secure mode.

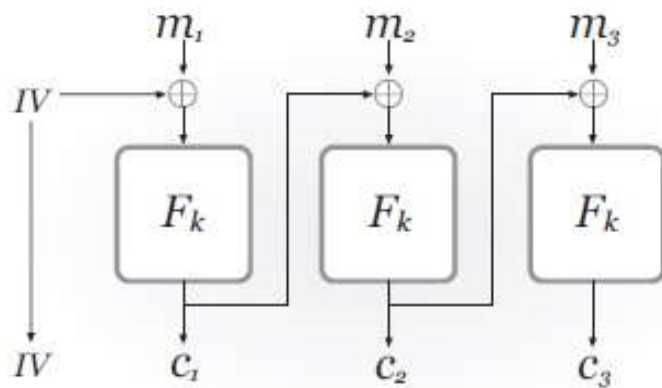


FIGURE 3.7: Cipher Block Chaining (CBC) mode.

Modes of Operation—Block Cipher

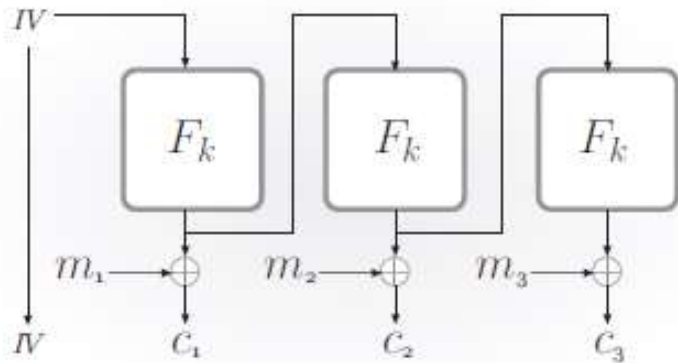


FIGURE 3.9: Output Feedback (OFB) mode.

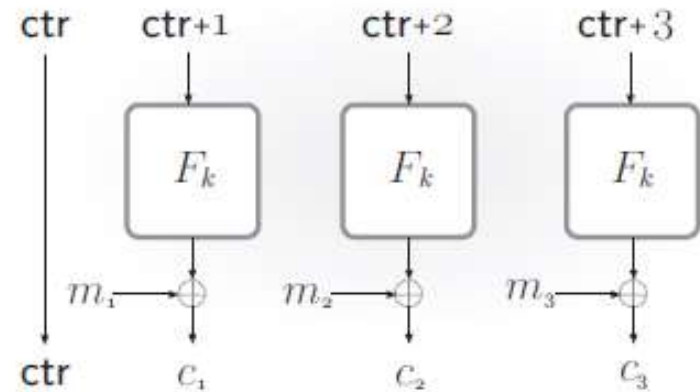


FIGURE 3.10: Counter (CTR) mode.

