Introduction to Cryptology

Lecture 10

Announcements

- HW4 due today
- HW5 up on course webpage, due 3/8
  - Canvas Discussion set up
- Midterm: coming up on 3/10
  - Canvas survey to determine review session held by Mukul

Agenda

- Last time:
  - CPA-secure encryption from PRF (Sec. 3.5)
- This time:
  - PRP (Block Ciphers) (3.5)
  - Modes of operation (3.6)
  - New topic:
    - Message Authentication Codes (MAC) (4.2)
    - Constructing MAC from PRF (4.3)

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.

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.

Modes of Operation—Stream Cipher

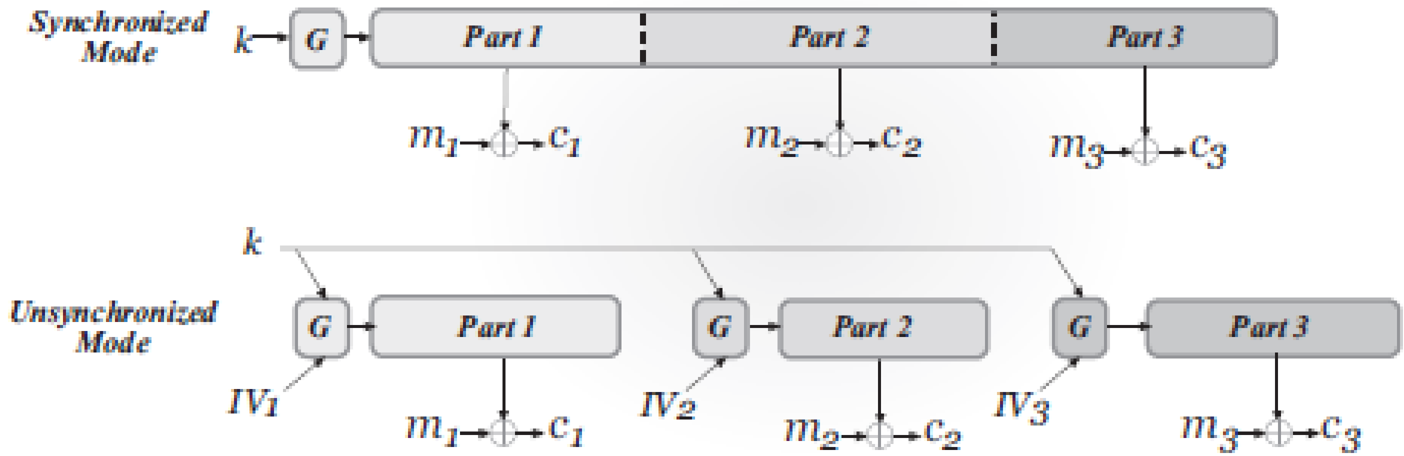

FIGURE 3.4: Synchronized mode vs. unsynchronized mode.

If sender and receiver are willing to maintain state, can encrypt multiple messages.

Modes of Operation—Block Cipher

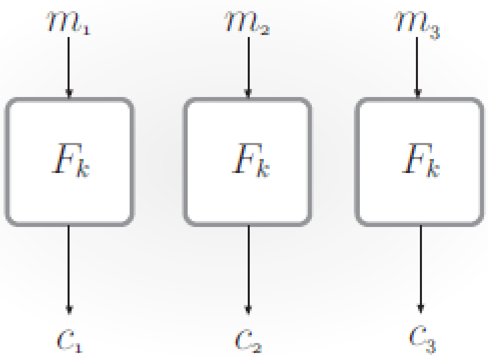

FIGURE 3.5: Electronic Code Book (ECB) mode.

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.

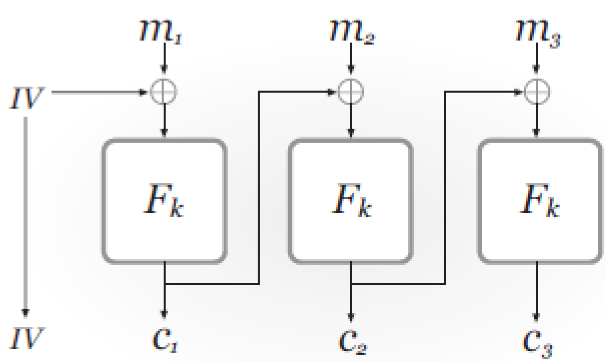

FIGURE 3.7: Cipher Block Chaining (CBC) mode.

Modes of Operation—Block Cipher

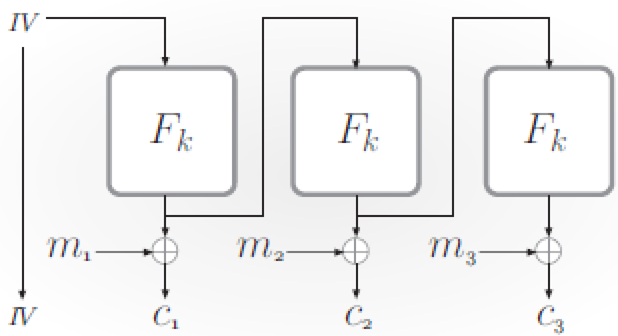

FIGURE 3.9: Output Feedback (OFB) mode.

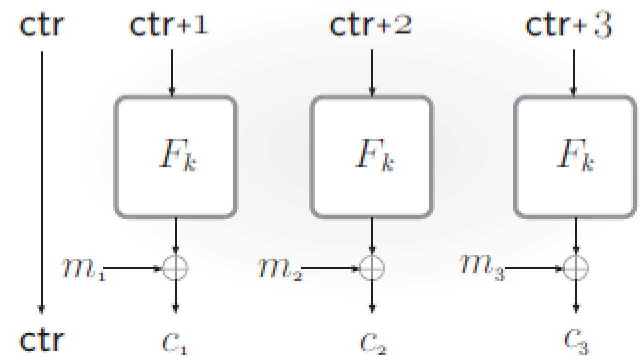

FIGURE 3.10: Counter (CTR) mode.

Message Integrity

- Secrecy vs. Integrity

- Encryption vs. Message Authentication

Message Authentication Codes

Definition: A message authentication code (MAC) consists of three probabilistic polynomial-time algorithms $(Gen, Mac, Vrfy)$ such that:

1. The key-generation algorithm Gen takes as input the security parameter 1^n and outputs a key k with $|k| \geq n$.
2. The tag-generation algorithm Mac takes as input a key k and a message $m \in \{0,1\}^*$, and outputs a tag t.
   $t \leftarrow Mac_k(m)$.
3. The deterministic verification algorithm $Vrfy$ takes as input a key k, a message m, and a tag t. It outputs a bit b with $b = 1$ meaning valid and $b = 0$ meaning invalid.
   $b := Vrfy_k(m, t)$.

It is required that for every n, every key k output by $Gen(1^n)$, and every $m \in \{0,1\}^*$, it holds that $Vrfy_k\big(m, Mac_k(m)\big) = 1$.