University of Michigan–Ann Arbor

Department of Electrical Engineering and Computer Science

EECS 475 **Introduction to Cryptography**, Winter 2023

Lecture 12: Modes of operation: CTR, OFB, ECB. Pseudorandom permutations (PRP), CBC.

February 15, 2023

Lecturer: Mahdi Cheraghchi

Scribe: Yi-Wen Tseng

1 Counter Mode (CTR)

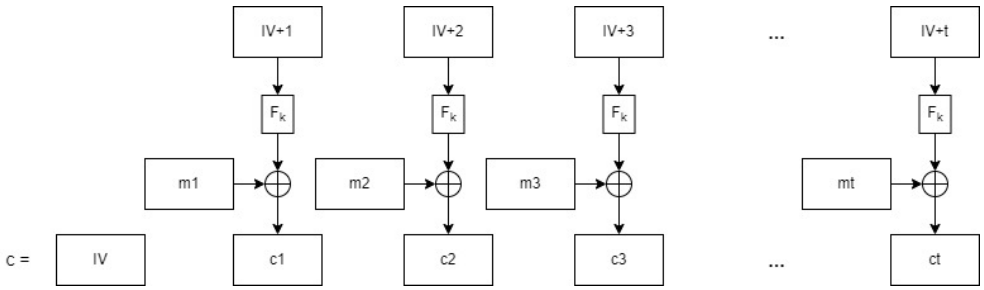

Figure 1: CTR Mode Encryption

By using CTR, we can now encrypt messages of various lengths: message space M:$\{0,1\}^*$. Additionally, if F is PRF (pseudorandom function), then CTR is CPA secure.

Proof: Every Input to F across the entire CPA game is distinct, with a very negligible probability to be the same. Therefore, all output of F will *look like* truly random and independent.

Advantages of using CTR:

- Simple and satisfy CPA secure
- Fast and efficient because it can be computed in parallel
- No need for padding (we can just trim the output of F to fit the last message block size)

2 Output Feedback Mode (OFB)

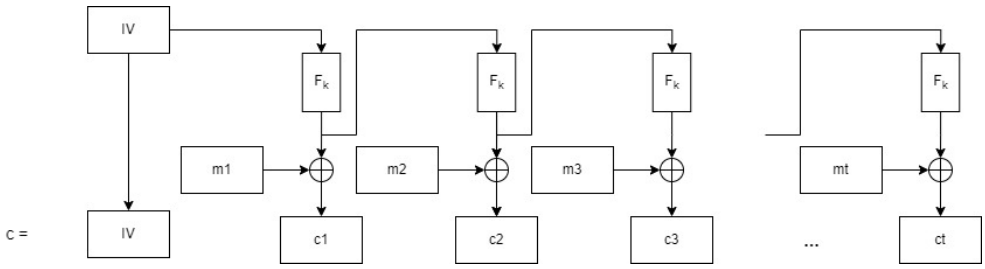

Figure 2: OFB Mode Encryption

- OFB is random by the chain, which is independent of message, not by counter.
- OFB is also CPA secure because it essentially does not have repeated input to F (happen with negligible probability).
- OFB can increase security.
  - Because IV is not random, if IV is attacked, every block in CTR can in danger. In contrast, in OFB, because IV is executed with F before XOR with message block, OFB can still be secure even if IV is guessed.
- OFB cannot be computed in parallel

3 Electronic Codebook Mode (ECB)

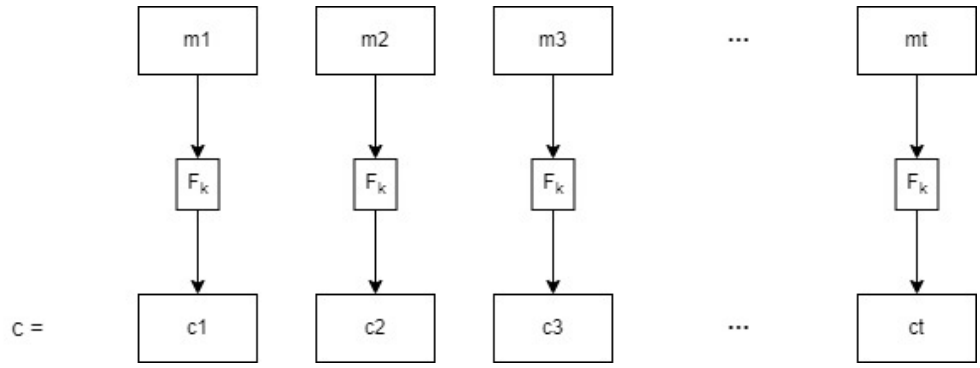

Figure 3: ECB Mode Encryption

This encryption mode is not secure.

- Same message block is encrypted to the same ciphertext block
  - This implies that ECB is not CPA secure because it is stateless and deterministic.

- If F is PRF, we are not able to decrypt the ciphertext because it is not guaranteed that the inverse function of F exists.
- If F is PRP, we are able to decrypt the ciphertext but it is still not CPA secure because the same message still shares the same ciphertext.

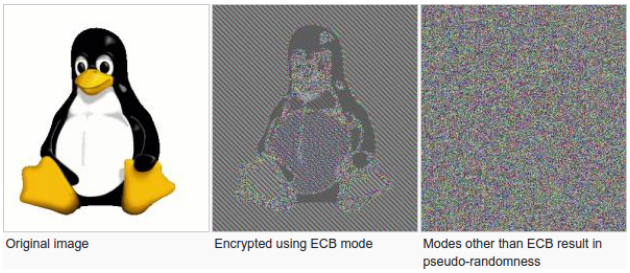

Figure 4: ECB Encryption Example

4 Pseudorandom Permutation (PRP)

4.1 Block cipher

Definition: A keyed function F: K x $\{0,1\}^n \rightarrow \{0,1\}^n$, where F_k is bijection, and F_k and F_k^{-1} can be computed efficiently given the key k

Note: Block cipher is an invertible version of a PRF

4.2 PRP

Definition: F_k is called a pseudorandom permutation (PRP) if F_k, given random key k in key space K, is indistinguishable from a random bijection (permutation on $\{0,1\}^n$) for alll ppt A:

$$\left| \Pr_{k \leftarrow K} \left[\mathcal{A}^{F_k(.)} = 1 \right] - \Pr_{P \leftarrow P_n} \left[\mathcal{A}^{P(.)} = 1 \right] \right| = negl(n)$$

where P_n is a set of all bijection on $\{0,1\}^n$

Note: If we can give A access to $F_k^{-1}(.)/P^{-1}(.)$ as well, then F_k is a strong PRP.

Theorem: If F is a PRP, F is also a PRF.

Proof Idea: Given oracle access, a random permutation is identical to a random function as long as distinct input queries to the random function don't return the same value (because if $c_1 = c_2$, function F is not invertible), which implies "birthday collision" on outputs. However, collision happens with negligible probability: $\frac{poly(n)}{2^n}$. Thus, under the efficient setting, if F is a PRP, it is also a PRF.

5 Cipher Block Chaining (CBC)

5.1 Encryption

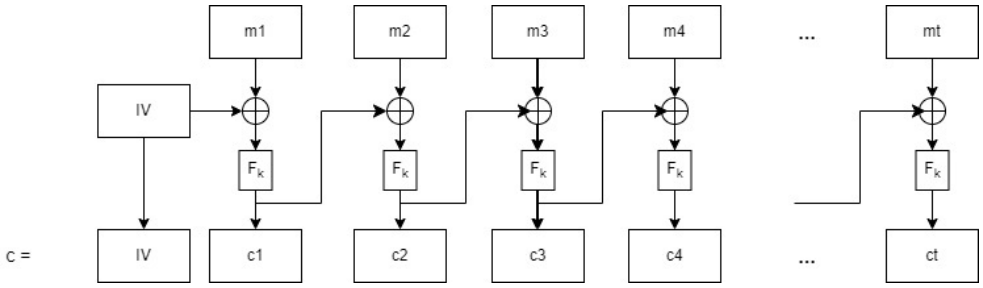

Figure 5: CBC Mode Encryption

$$\begin{cases} c_0 = IV \\ c_i = F_k(m_i \oplus c_{i-1}) \end{cases} \tag{1}$$

5.2 Decryption

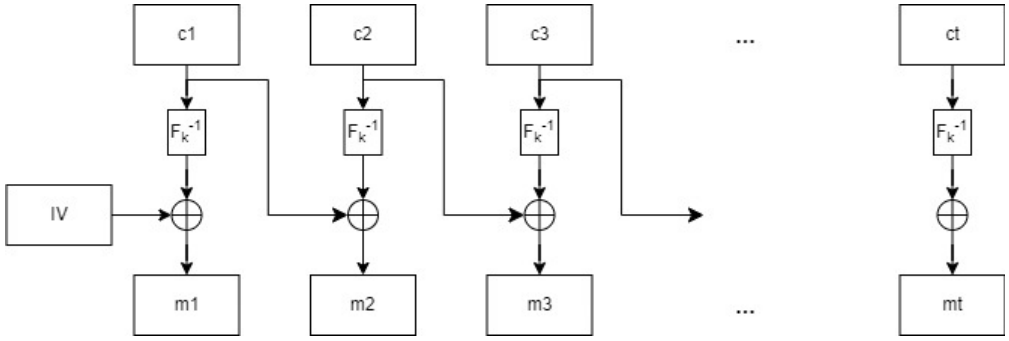

Figure 6: CBC Mode Decryption

$$m_i = c_{i-1} \oplus F_k^{-1}(c_i) \tag{2}$$

- **Theorem:** If F is a PRP (which is also PRF), then CBC is CPA-secure.

  Proof Idea: All ciphertexts look like random independent strings as long as no input to $F_k(.)$ is ever repeated. Based on the birthday paradox, repetitions happen with only negligible ($\frac{poly(n)}{2^n}$) probability by the choice of IV and (pseudo)-random outputs of prior blocks.

- **Cons**

  1. Longer execution time:

- Because we cannot trim the output of F to fit the last message block, CBC requires padding the last message block which will increase the execution time.

2. Encryption is sequential
   - Cannot compute ciphertext without computing all prior blocks

   Note: Decryption can be done in parallel.

3. Can be broken in "streaming" contexts that fall slightly outside the CPA attack model
   - **Padding Oracle Attack**: if attacker can get errors (padding error or encryption error) from CBC mode, the attacker can decrypt the entire message.