2022201041

CPA SECURE

CPA (Chosen Plaintext Attack) security is a standard for measuring the security of encryption schemes. A cryptographic scheme is said to be CPA-secure if it is computationally infeasible to distinguish between ciphertexts obtained from encrypting a random message and ciphertexts obtained from encrypting any other message, even if the attacker can choose the plaintexts to be encrypted.

CPA security is considered a strong security notion because it models the most realistic threat scenario: an attacker can choose any plaintexts that they want to encrypt and obtain the corresponding ciphertexts. CPA security is important for many applications, including electronic commerce, online banking, and secure communications.

In summary, CPA security provides strong protection against an attacker who has access to the encryption algorithm and can choose any plaintexts to be encrypted. It ensures that even if the attacker can see the encrypted message, they cannot learn any information about the original plaintext.

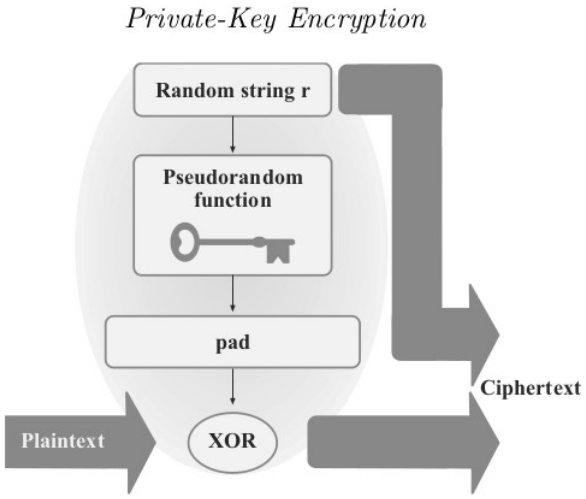
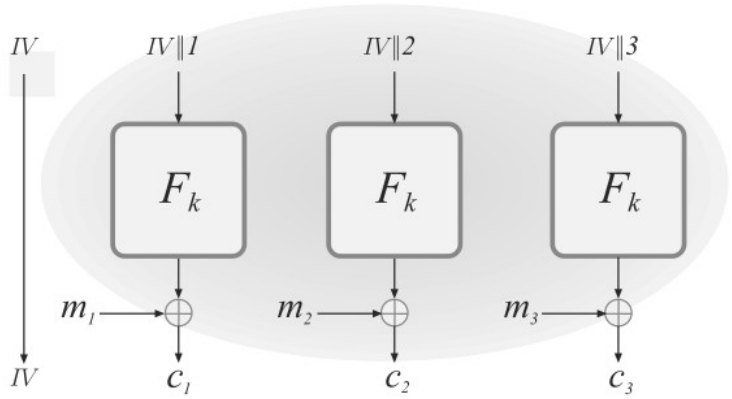


FIGURE 3.3: Encryption with a pseudorandom function.

Private-Key Encryption



CONSTRUCTION 3.28

Let F be a pseudorandom function. Define a fixed-length, private-key encryption scheme for messages of length n as follows:

- Gen: on input 1^n, choose uniform $k \in \{0,1\}^n$ and output it.
- Enc: on input a key $k \in \{0,1\}^n$ and a message $m \in \{0,1\}^n$, choose uniform $r \in \{0,1\}^n$ and output the ciphertext

$$c := \langle r, F_k(r) \oplus m \rangle.$$

- Dec: on input a key $k \in \{0,1\}^n$ and a ciphertext $c = \langle r, s \rangle$, output the message

$$m := F_k(r) \oplus s.$$

There are three modes of operation as discussed in class, namely, Cipher block Chaining (CBC), Output Feedback Mode (OFB), and Randomized Counter Mode.

To obtain a CPA-secure encryption scheme using PRF, Let F be a PRF. First, one needs

to define a private-key encryption scheme for messages of length n.

The encryption scheme is a collection of three algorithms, namely, key generation algorithm (Gen), encryption algorithm (Enc) and decryption algorithm (Dec). The Gen

gives key to both the sender and receiver, the Enc with key, plain text and local randomness gives the ciphertext as the output, and Dec takes the ciphertext and key to

output the message.

For the CPA-secure encryption :

1. Gen : on input 1n, choose k <- {0,1}n uniformly at random and output it as the key

2. Enc : on input a key where k is belonging to {0,1}n and a message ‘m’ belonging

to {0,1}n, choose r <- {0,1}n uniformly at random and output the ciphertext

c := <r, Fk(r) ⊕ m>

3. Dec : on input a key ‘k’ belonging to {0,1} n and a ciphertext c = <r,s>, output the

plaintext message

m := Fk(r) ⊕ s

By following the above mentioned instructions, a C