

1 Lecture Plan

- Complete the proof of the CPA-security of the encryption scheme presented in the last lecture.
- Define pseudorandom permutations
- Describe block cipher modes
- Describe the construction of DES

2 Recap

CPA-Secure Encryption from Pseudorandom Functions

- Let F be a pseudorandom function. Define a private-key encryption scheme for messages of length n as follows:
 - **Gen**: On input 1^n , choose k uniformly from $\{0, 1\}^n$.
 - **Enc**: Given $k \in \{0, 1\}^n$ and 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**: Given $k \in \{0, 1\}^n$ and ciphertext $c = \langle r, s \rangle$, output the plaintext message

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

Theorem (Theorem 3.31 of KL). *If F is a pseudorandom function, then the above construction is a CPA-secure private-key encryption scheme for messages of length n .*

Proof. Done in class. □

- What is a drawback of this construction?

3 Pseudorandom Permutations

- In practice, constructions of pseudorandom permutations are used instead of pseudorandom functions.

- Let Perm_n be the set of all permutations (bijections) on $\{0, 1\}^n$. An $f \in \text{Perm}_n$ can be seen as a lookup table where any two distinct rows must be different.
- $|\text{Perm}_n| = (2^n)!$
- A function $F : \{0, 1\}^{l_{\text{key}}(n)} \times \{0, 1\}^{l_{\text{in}}(n)} \rightarrow \{0, 1\}^{l_{\text{in}}(n)}$ is called a *keyed permutation* if for all $k \in \{0, 1\}^{l_{\text{key}}(n)}$, F_k is a permutation.
- $l_{\text{in}}(n)$ is called the *block length* of F .
- F is *length-preserving* if $l_{\text{key}}(n) = l_{\text{in}}(n) = n$.
- F is said to be *efficient* if both $F_k(x)$ and $F_k^{-1}(y)$ have polynomial-time algorithms for all k, x, y .
- A *pseudorandom permutation* is a permutation which cannot be efficiently distinguished from a random permutation, i.e. a permutation uniformly chosen from Perm_n .
- When the blocklength is sufficiently long, a random permutation is indistinguishable from a random function (by birthday problem analysis).
- In practice, constructions of pseudorandom permutations are called *block ciphers*.

4 Block Cipher Modes of Operation

4.1 Electronic Code Book (ECB) Mode

- **Insecure and should not be used.**
- Let $m = m_1, m_2, \dots, m_l$ where $m_i \in \{0, 1\}^n$.
- Let F be a block cipher with block length n .
- $c := \langle F_k(m_1), F_k(m_2), \dots, F_k(m_l) \rangle$
- ECB is deterministic and cannot be CPA-secure.

4.2 Cipher Block Chaining (CBC) Mode

- Let $m = m_1, m_2, \dots, m_l$ where $m_i \in \{0, 1\}^n$.
- Let F be a length-preserving block cipher with block length n .
- A uniform *initialization vector* (IV) of length n is first chosen.
- $c_0 = IV$. For $i = 1, \dots, l$, $c_i := F_k(c_{i-1} \oplus m_i)$.
- For $i = 1, 2, \dots, l$, $m_i := F_k^{-1}(c_i) \oplus c_{i-1}$.
- This mode has a ciphertext which is larger than the plaintext by n bits.
- Decryption is much faster than encryption.
- If F is a pseudorandom permutation, then the CBC-mode encryption is CPA-secure.

4.3 Counter (CTR) Mode

- Let $m = m_1, m_2, \dots, m_l$ where $m_i \in \{0, 1\}^n$.
- Let F be a length-preserving block cipher with block length n .
- A uniform value \mathbf{ctr} of length n is first chosen.
- $c_0 = \mathbf{ctr}$. For $i = 1, \dots, l$, $c_i := F_k(\mathbf{ctr} + i) \oplus m_i$.
- For $i = 1, 2, \dots, l$, $m_i := F_k(\mathbf{ctr} + i) \oplus c_{i-1}$.
- This mode has a ciphertext which is larger than the plaintext by n bits.
- Both encryption and decryption can be parallelized.
- The generated stream can be truncated to exactly the plaintext length.
- F does not need to be a permutation.
- If F is a pseudorandom function, then the CTR-mode encryption is CPA-secure.

5 Data Encryption Standard (DES)

- DES was proposed by IBM in 1974 in response to a call for proposals from the US National Bureau of Standards (now NIST)
- Adopted as a US federal standard from 1979 to 2005
- In 2000, AES selected as successor to DES.
- DES considered insecure now but still interesting for historical reasons.

5.1 Construction

- Based on the *Feistel transform*
- Let $f : \{0, 1\}^n \rightarrow \{0, 1\}^n$ be any function. The Feistel transform of f is the function $FSTL_f : \{0, 1\}^{2n} \rightarrow \{0, 1\}^{2n}$ is defined by

$$FSTL_f(L, R) = (R, f(R) \oplus L)$$

- Even if f is not a bijection, $FSTL_f$ is a bijection.
- The inverse is given by

$$FSTL_f^{-1}(X, Y) = (Y \oplus f(X), X)$$

- DES has a key length of 56 bits and a block length of $n = 64$ bits. It consists of 16 *rounds* of a Feistel transform.
- The 56-bit key K is expanded to a sequence of 16 subkeys K_1, K_2, \dots, K_{16} each of length 48 bits.

- Decryption use the same structure as encryption except for the fact that the subkeys are applied in reverse order.
- See pages 41–44 of Bellare-Rogaway notes for full description.

6 References and Additional Reading

- Section 3.5, 3.6 from Katz/Lindell
- Chapter 3 of *Introduction to Modern Cryptography* by Mihir Bellare, Phillip Rogaway, 2005.
<http://web.cs.ucdavis.edu/~rogaway/classes/227/spring05/book/main.pdf>