Cryptography

Cunsheng DING

HKUST, Hong Kong

COMP3631

Lecture 06: A Design Paradigm of One-Key Block Ciphers

The Outline of This Lecture

1. The objective of this lecture.
2. Shannon's idea of confusion and diffusion.
3. A design paradigm of one-key block ciphers.
4. An example cipher following the design paradigm.

Part 1: The Objective of This Lecture

The Objective of This Lecture

In Lecture 4, we did the following:

1. We defined one-key block ciphers $(\mathcal{M}, \mathcal{C}, \mathcal{K}, E_k, D_k)$ and made three security requirements.
2. We discussed simple substitution ciphers, and realized that they are not secure.
3. We learnt the one-time pad cipher, which is **secure** in the information-theoretic sense, but **impractical**.

In Lecture 5, we discussed linear and nonlinear functions.

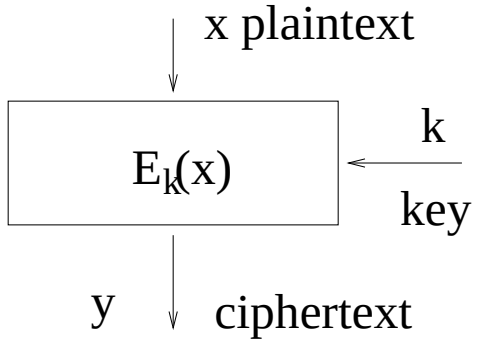
The objective of this lecture: To introduce a design paradigm of **secure** and **practical** one-key block ciphers.

Part 2: Shannon's Idea of Diffusion and Confusion

For the Construction of One-Key Block Ciphers

Diffusion Measure

Message (respectively, key) bit diffusion measure: The minimum number of bits in the ciphertext block $y = (y_1, \ldots, y_n)$ affected by changing one bit in the plaintext block $x = (x_1, \ldots, x_n)$ (respectively, secret key $k = (k_1, \ldots, k_t)$) `divided by` n.



1. The higher this diffusion measure, the better the diffusion.
2. The encryption and decryption function should have good diffusion.
3. Both linear and nonlinear functions are employed to provide diffusion.

Example of Bad Diffusion

Example: Suppose that $x = (x_1, x_2, \ldots, x_8)$, $y = (y_1, y_2, \ldots, y_8)$ and $k = (k_1, k_2, \ldots, k_8)$ all have 8 bits. Let $y = E_k(x)$ be defined by

$$y_1 = x_1 + k_1, \quad y_2 = x_2 + k_2, \quad y_3 = x_3 + k_3, \quad y_4 = x_4 + k_4,$$
$$y_5 = x_5 + k_5, \quad y_6 = x_6 + k_6, \quad y_7 = x_7 + k_7, \quad y_8 = x_8 + k_8,$$

where all the additions + are the integer addition modulo 2.

Message bit diffusion: 1/8.

Key bit diffusion: 1/8.

Comments: The function $y = E_k(x)$ has very bad diffusion, because each plaintext bit or key bit affects only one bit in the output block y.

Example of Good Diffusion

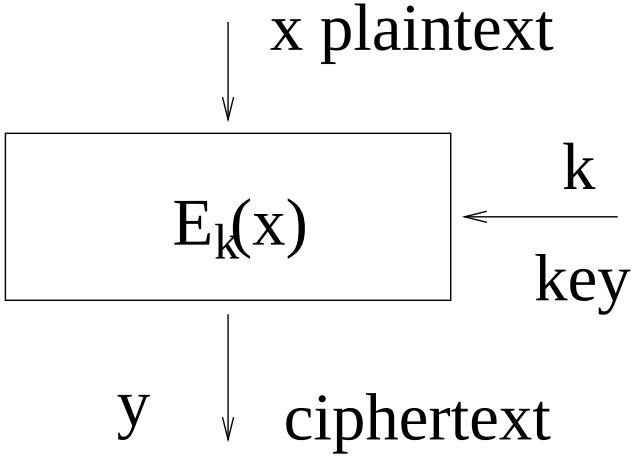
Example: Suppose that $x = (x_1, x_2, \ldots, x_8)$, $y = (y_1, y_2, \ldots, y_8)$ and $k = (k_1, k_2, \ldots, k_8)$ all have 8 bits. Let $y = E_k(x)$

$$
\begin{aligned}
y_1 &= x_1 + x_2 + x_3 + x_4 + x_5 + k_1 + k_2 + k_3 + k_4 + k_5, \\
y_2 &= x_2 + x_3 + x_4 + x_5 + x_6 + k_2 + k_3 + k_4 + k_5 + k_6, \\
y_3 &= x_3 + x_4 + x_5 + x_6 + x_7 + k_3 + k_4 + k_5 + k_6 + k_7, \\
y_4 &= x_4 + x_5 + x_6 + x_7 + x_8 + k_4 + k_5 + k_6 + k_7 + k_8, \\
y_5 &= x_5 + x_6 + x_7 + x_8 + x_1 + k_5 + k_6 + k_7 + k_8 + k_1, \\
y_6 &= x_6 + x_7 + x_8 + x_1 + x_2 + k_6 + k_7 + k_8 + k_1 + k_2, \\
y_7 &= x_7 + x_8 + x_1 + x_2 + x_3 + k_7 + k_8 + k_1 + k_2, + k_3 \\
y_8 &= x_8 + x_1 + x_2 + x_3 + x_4 + k_8 + k_1 + k_2 + k_3 + k_4.
\end{aligned}
$$

Comments: It has very good diffusion, as each plaintext bit or key bit affects 5 bits in the output block $y = (y_1, y_2, \cdots, y_8)$.

Confusion Measure

Confusion measure: The "complexity" of the relations between the ciphertext block bits and the plaintext block bits and the key bits.



Remark: The confusion measure above is not rigorous, as we do not have a measure of the complexity of relations.

Remark: Nonlinear functions are **mainly** used to provide confusion. They could provide also diffusion.

Bad Confusion

Let $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$ be the plaintext block and ciphertext block, respectively. Let $k = (k_1, \ldots, k_t)$ be the secret key such that $y = E_k(x)$.

Bad confusion: It means that the relations among the plaintext block bits, ciphertext block bits and the key bits are so **simple** that it is **feasible** to recover k by solving the following system of equations

$$y = E_k(x)$$

for a number of given pairs (x, y).

Warning: If the encryption and decryption function of a one-key cipher have bad confusion, then the cipher is not secure w.r.t. known-plaintext attacks (excluding the One-Time-Pad cipher, which is impractical).

Example of Functions with Bad Confusion

Example: Suppose that $x = (x_1, x_2, \ldots, x_8)$, $y = (y_1, y_2, \ldots, y_8)$ and $k = (k_1, k_2, \ldots, k_8)$ all have 8 bits. Let $y = E_k(x)$

$$\begin{aligned}
y_1 &= x_1 + x_2 + x_3 + x_4 + x_5 + k_1 + k_2 + k_3 + k_4 + k_5, \\
y_2 &= x_2 + x_3 + x_4 + x_5 + x_6 + k_2 + k_3 + k_4 + k_5 + k_6, \\
y_3 &= x_3 + x_4 + x_5 + x_6 + x_7 + k_3 + k_4 + k_5 + k_6 + k_7, \\
y_4 &= x_4 + x_5 + x_6 + x_7 + x_8 + k_4 + k_5 + k_6 + k_7 + k_8, \\
y_5 &= x_5 + x_6 + x_7 + x_8 + x_1 + k_5 + k_6 + k_7 + k_8 + k_1, \\
y_6 &= x_6 + x_7 + x_8 + x_1 + x_2 + k_6 + k_7 + k_8 + k_1 + k_2, \\
y_7 &= x_7 + x_8 + x_1 + x_2 + x_3 + k_7 + k_8 + k_1 + k_2, + k_3 \\
y_8 &= x_8 + x_1 + x_2 + x_3 + x_4 + k_8 + k_1 + k_2 + k_3 + k_4.
\end{aligned}$$

Comments: $y = E_k(x)$ has very bad confusion, as the relation between the input bits and output bits is linear. It is easy to recover k given a pair (x, y).

Good Confusion

Let $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$ be the plaintext block and ciphertext block, respectively. Let $k = (k_1, \ldots, k_t)$ be the secret key such that $y = E_k(x)$.

Good confusion: It means that the relations among the plaintext block bits, ciphertext block bits and the key bits are so **complex** that it is **infeasible** to recover k by solving the following system of equations

$$y = E_k(x)$$

for a number of given pairs (x, y).

Good confusion requirement: The encryption and decryption function of a **secure** and **practical** one-key block cipher should have good confusion.

Part 3: An Important Design Paradigm

The Iterative Design Paradigm (I)

In order to design E_k and D_k such that

1. they have good diffusion and confusion with respect to the secret key bits and plaintext bits, and
2. they are fast in software and hardware implementation,

we could design a simple one-to-one function f_h (called, **round function**) and define

$$E_k(m) = f_{k_\ell}(f_{k_{\ell-1}}(\cdots f_{k_2}(f_{k_1}(m))\cdots))$$

where the **round keys** $k_1, k_2, \cdots, k_\ell$ are computed from the secret key k according to an algorithm (called the **key schedule/expansion algorithm**), and ℓ is the number of rounds of iteration.

Questions: How to design f_h and the key schedule algorithm? How large should ℓ be?

Part 4: An Example Cipher Following the Design Paradigm

Remark: In this part, $+$, $-$ and $\times$ denote the modulo-p addition, modulo-p subtraction and modulo-p multiplication in $\mathbf{Z}_p$, respectively, when the operands are from $\mathbf{Z}_p$. Otherwise they denote the school integer operations for integers. This will not cause confusions.

For example, $x + y$ means the modulo-p addition if the operands x and y are from $\mathbf{Z}_p$, and it means the integer addition if the operands x and y are integers.

An Example Cipher Following the Iterative Approach (1)

Some preparations before defining the one-key block cipher:

Proposition: Let p be a prime with $\gcd(3, p-1) = 1$. Then x^3 is a permutation on $\mathbf{Z}_p$. Its inverse function is x^u, where u is the multiplicative inverse of 3 modulo $p-1$.

Proof: Since u is the multiplicative inverse of 3 modulo $p-1$, there is a positive integer j such that $3u = j(p-1)+1$. For any $x \in \mathbf{Z}_p \setminus \{0\}$, it follows from "Fermat's Theorem" (see Lecture 10) that

$$x^{3u} = x^{j(p-1)+1} = (x^{(p-1)})^j x = x.$$

Hence, x^3 and x^u are the inverses of each other. Suppose that $x_1^3 = x_2^3$. Then $(x_1^3)^u = (x_2^3)^u$. Consequently, $x_1 = x_2$. Hence, x^3 is injective. As a result, x^3 must be bijective, as $\mathbf{Z}_p$ has finitely many elements.

An Example Cipher Following the Iterative Approach (2)

Some preparations before defining the one-key block cipher:

Proposition: Let p be a prime with $\gcd(3, p-1) = 1$. Then $f_h(x) = (x+h)^3 + h$ is a permutation of $\mathbf{Z}_p$ for each $h \in \mathbf{Z}_p$. Its inverse function $f_h^{-1}(x) = (x-h)^u - h$, where u is the multiplicative inverse of 3 modulo $p-1$.

Proof: If $f_h(x_1) = f_h(x_2)$, then $(x_1+h)^3 + h = (x_2+h)^3 + h$. Consequently, $(x_1+h)^3 = (x_2+h)^3$. Since x^3 is a permutation of $\mathbf{Z}_p$, $x_1 + h = x_2 + h$. Hence $x_1 = x_2$. It is straightforward to verify that

$$f_h^{-1}(f_h(x)) = x.$$

This completes the proof.

An Example Cipher Following the Iterative Approach (3)

The System Parameters of a One-Key Block Cipher

Let p be a large prime with $\gcd(3, p-1) = 1$ and α be an integer with $2 \leq \alpha \leq p-3$.

Remark: The large prime p and α are put in the public domain.

An Example Cipher Following the Iterative Approach (4)

The Description of the One-Key Block Cipher

Let ℓ be a fixed positive integer. Let $\mathcal{M} = \mathcal{C} = \mathcal{K} = \mathbf{Z}_p$. Define the round function by $f_h(x) = (x+h)^3 + h$ from $\mathbf{Z}_p$ to $\mathbf{Z}_p$, where $h \in \mathbf{Z}_p$.

For a secret key $k \in \mathbf{Z}_p$, define round keys $k_i = \alpha^{k+i} \in \mathbf{Z}_p$ for each $i \geq 1$.

Define

$$E_k(m) = f_{k_\ell}(f_{k_{\ell-1}}(\cdots f_{k_2}(f_{k_1}(m))\cdots)),$$
$$D_k(c) = f_{k_1}^{-1}(f_{k_2}^{-1}(\cdots f_{k_{\ell-1}}^{-1}(f_{k_\ell}^{-1}(c))\cdots))$$

where $f_h^{-1}(x) = (x-h)^u - h$ and u is the multiplicative inverse of 3 modulo $p-1$.

Question: How many rounds of iteration should this cipher have?

Remark: It may take many years to answer this hard question.

Summary of This Lecture

- We introduced Shannon's idea of confusion and diffusion, and learnt that a **secure and practical** one-key block cipher should have good confusion and good diffusion.
- We introduced a design paradigm for one-key block ciphers, and studied an example cipher following the design paradigm.

In the next two lectures, we will introduce two more one-key block ciphers designed by following this iterative design paradigm.