Design Issues of Block Ciphers

The objectives of this part is to show certain design issues of block ciphers.

Block Ciphers and Stream Ciphers

A one-key cipher is a 5-tuple $(\mathcal{M}, \mathcal{C}, \mathcal{K}, E_k, D_k)$, where

- $\mathcal{M}$, $\mathcal{C}$, $\mathcal{K}$ are respectively the plaintext space, ciphertext space, and key space;

- Any $k \in \mathcal{K}$ could be the encryption and decryption key; and

- E_k and D_k are encryption and decryption transformations with $D_k(E_k(m)) = m$ for each $m \in \mathcal{M}$.

Classification: For any message m, if the corresponding ciphertext $c := E_k(m)$ is time-invariant, the one-key cipher is called a block cipher. Otherwise, it is called a stream cipher.

An Example of Block Ciphers

- $\mathcal{M} = \mathcal{C} = \{0, 1\}^*$.
- $\mathcal{K} = \{0, 1\}^{256}$.
- A message is divided into blocks m_i, each with 256 bits. Encryption is then done block by block:

$$E_k(m_i) = m_i \oplus k.$$

- Each ciphertext block c_i (i.e., $E_k(m_i)$) is decrypted:

$$D_k(c_i) = c_i \oplus k.$$

Question: Why this is a block cipher?

Question: Is this block cipher secure? Why?

Remark: Examples of stream ciphers will be seen later.

Design Issues of One-key Block Ciphers

A one-key $(\mathcal{M}, \mathcal{C}, \mathcal{K}, E_k, D_k)$:

- You have to design all the five building blocks.
- The security of your cipher should depend only on the confidentiality of the key k. (We assume that the encryption algorithm E_k and decryption algorithm D_k are known to the enemy.)
- It should be secure in the computational sense.
- It should be fast in hardware and software.

Question: How do you design a one-key cipher meeting these requirements?

$\boxed{\textbf{Linear Functions}}$

Notation: Let $\mathbf{F}_2$ denote the set $\{0, 1\}$ and let

$$\mathbf{F}_2^n = \{(x_1, x_2, \cdots, x_n) | x_i \in \mathbf{F}_2\}.$$

We always associate $\mathbf{F}_2^n$ with the bitwise exclusive-or operation, also denoted $+$.

Linear functions: Let f be a function from $\mathbf{F}_2^n$ to $\mathbf{F}_2^m$, where n and m are positive integers. f is called **linear** if

$$f(x + y) = f(x) + f(y)$$

for all $x, y \in \mathbf{F}_2^n$.

Example: Let $f(x) = x_1 + x_2 + \cdots + x_n$, where

$$x = (x_1, \cdots, x_n) \in \mathbf{F}_2^n.$$

Then f is a linear function from $\mathbf{F}_2^n$ to $\mathbf{F}_2$. Note that $+$ denotes the modulo-2 addition.

$\boxed{\textbf{Linear Functions}}$

Linear function by circular shift: Let i be any positive integer. Define a function RS_i from $\mathbf{F}_2^n$ to $\mathbf{F}_2^n$ by

$$\begin{aligned} & RS_i((x_0, x_1, \cdots, x_{n-1})) \\ = \; & (x_{(0-i) \bmod n}, x_{(1-i) \bmod n}, \cdots, x_{(n-1-i) \bmod n}) \end{aligned}$$

for any $x = (x_0, x_1, \cdots, x_{n-1}) \in \mathbf{F}_n$.

Example:

$$RS_1((x_0, x_1, \cdots, x_{n-1})) = (x_{n-1}, x_0, x_1, \cdots, x_{n-2})$$

Lemma: RS_i is linear with respect to the bitwise exclusive-or.

Proof: Trivial.

$\boxed{\text{Nonlinear Functions}}$

Definition: Any function that is not linear is called a nonlinear function.

Example: The following function from $\mathbf{F}_2^4$ to $\mathbf{F}_2$ is nonlinear:

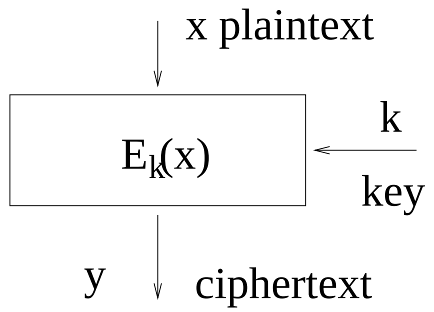
$$f(x_1, x_2, x_3, x_4) = x_1 + x_2 + x_3 + x_4 + x_1x_2x_3x_4$$

is nonlinear.

Remark: The degree of the Boolean function indicates the degree of nonlinearity.

Shannon's First Design Idea: Diffusion

Diffusion: Each plaintext block bit or key bit affects many bits of the ciphertext block.



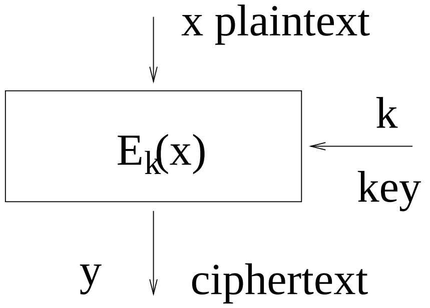
Example: Suppose that x, y and k all have 8 bits. If

$$\begin{aligned}
y_1 &= f_1(x_1, x_2, k_1, k_2)\\
y_2 &= f_2(x_2, x_3, k_2, k_3)\\
y_3 &= f_3(x_3, x_4, k_3, k_4)\\
y_4 &= f_4(x_4, x_5, k_4, k_5)\\
y_5 &= f_5(x_5, x_6, k_5, k_6)\\
y_6 &= f_6(x_6, x_7, k_6, k_7)\\
y_7 &= f_7(x_7, x_8, k_7, k_8)\\
y_8 &= f_8(x_8, x_1, k_8, k_1)
\end{aligned}$$

where the f_i are some functions, then it has very bad diffusion, because each plaintext bit or key bit affects only two bits in the output block y.

Shannon’s First Design Idea: Diffusion

Diffusion: Each plaintext block bit or key bit affects many bits of the ciphertext block.



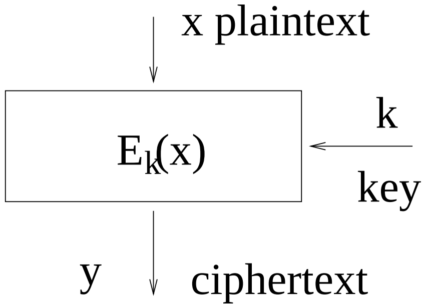
Example: Suppose that x, y and k all have 8 bits. If

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

then it has very good diffusion, because each plaintext bit or key bit affects half of the bits in the output block y.

Shannon's Second Design Idea: Confusion

Confusion: Each bit of the ciphertext block has highly nonlinear relations with the plaintext block bits and the key bits.



Example: Suppose that x, y and k all have 8 bits. If

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

then it has bad confusion, as they are linear relations.

Remark: Nonlinear functions are responsible for confusion.

An Important Design Paradigm

Iteration: 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 message block bits, and

2. they are fast in software and hardware,

we could design a simple function f_k and define

$$E_k(m) = f_{k_{16}}(f_{k_{15}}(\cdots f_{k_2}(f_{k_1}(m))\cdots))$$

where $k_1, k_2, \cdots$ and k_{16} are binary string computed from the secret key k according to an algorithm.

The Finite Field GF(2^8)

Primitive polynomial: $p(x) = x^8 + x^4 + x^3 + x + 1 \in \text{GF}(2)[x]$, which is irreducible and has "other" properties.

1. Every element of GF(2^8) is a polynomial:

   $$a(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_7 x^7 \in \text{GF}(2)[x].$$

2. For any two elements,

   $$\begin{aligned} a(x) &= a_0 + a_1 x + a_2 x^2 + \cdots + a_7 x^7 \\ b(x) &= b_0 + b_1 x + b_2 x^2 + \cdots + b_7 x^7, \end{aligned}$$

   the addition and multiplication are defined to be

   $$a(x) + b(x) = \sum_{i=0}^{7} (a_i + b_i) x^i \in \text{GF}(2)[x]$$

   and

   $$a(x) \times b(x) = a(x) b(x) \bmod p(x).$$

x^-1 has optimal nonlinerity.