Feistel Cipher

Math 4175

§4.5. Horst Feistel (1915-1990), a brief bio

- Feistel was born in Berlin, Germany in 1915, and moved to the USA in 1934.
- Received his Bachelor degree in Physics at MIT and Masters at Harvard.
- Placed under house arrest during second world war.
- Received citizenship and US Air Force security clearance after the war.
- Joined IBM and developed Feistel cipher, Lucifer, and Data Encryption Standard (DES).

§4.5. Feistel Cipher (Horst Feistel, 1915-1990)

Next we want to learn the modern cipher called Data Encryption Standard (DES).

For this purpose, now we will discuss another type of iterated cipher, called Feistel Cipher.

A Feistel cipher is a special type of iterated cipher with r rounds.

The basic form of a Feistel cipher is as follows:

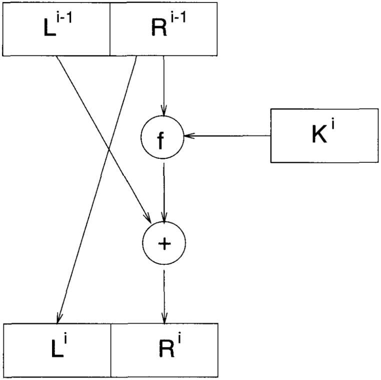
- Input: $w^0 = L^0 || R^0$ is a $2n$-bit string consisting of a left half, L^0 of length n, and a right half, R^0 also of length n.
- At each round i, $1 \leq i \leq r$,
  - Input: w^{i-1}
  - Output: w^i
- Each $w^i = L^i || R^i$ where L^i and R^i are n-bit strings.

§4.5. Feistel Cipher

- Key schedule produces $(K^1, K^2, \ldots, K^r)$ from a key K.
- The round function g has the following form: $g(L^{i-1}, R^{i-1}, K^i) = (L^i, R^i)$, where
$$\begin{aligned} L^i &= R^{i-1} \\ R^i &= L^{i-1} \oplus f(R^{i-1}, K^i) \end{aligned}$$
  Here $f(x, y)$ is any internal round function, where x is an n-bit string and y is a round key.
- The function f need not be injective, because the round function g is always invertible for a given key. Given the round key, the inverse of g is given by:
$$\begin{aligned} L^{i-1} &= R^i \oplus f(L^i, K^i) \\ R^{i-1} &= L^i \end{aligned}$$

§4.5. Feistel Cipher

One round of a Feistel cipher:



§4.5. Feistel Cipher

Example: "Baby Horst"

- Input: 8-bit string (4-bit halves)
- Number of rounds: 2
- The key K is a 8-bit, K^1 is the string given by the first four bits of K, and K^2 given by the last four bits of K.
- Let $f(x, y) = x \odot y$ be the bitwise multiplication of x and y.

Encrypt the plaintext AB (hexadecimal) using the key $K = 75$.

§4.5. Baby Horst Cipher

First round:

- Plain text AB: $\implies L^0 = A = 1010,\ R^0 = B = 1011.$
- $K^1 = 7 = 0111.$
- $L^1 = R^0 = B = 1011.$
- Now

$$\begin{aligned} R^1 &= L^0 \oplus f(R^0, K^1) \\ &= 1010 \oplus (1011 \odot 0111) \\ &= 1010 \oplus 0011 \\ &= 1001 \end{aligned}$$

Therefore $L^1 R^1 = 1011\,1001.$

§4.5. Baby Horst Cipher

Second round:

- Now $L^1 = 1011$, $R^1 = 1001$.
- $K^2 = 5 = 0101$.
- $L^2 = R^1 = 1001$.
- Then

$$\begin{aligned} R^2 &= L^1 \oplus f(R^1, K^2) \\ &= 1011 \oplus (1001 \odot 0101) \\ &= 1011 \oplus 0001 \\ &= 1010 \end{aligned}$$

Therefore cipher text: $L^2 R^2 = 1001\,1010 = 9A$.