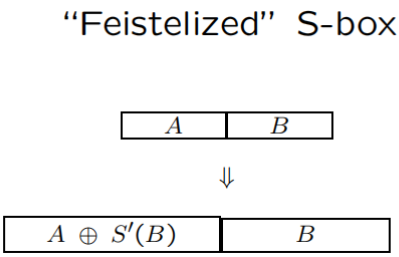
Homework 2

1 - “Feistelized” S-box

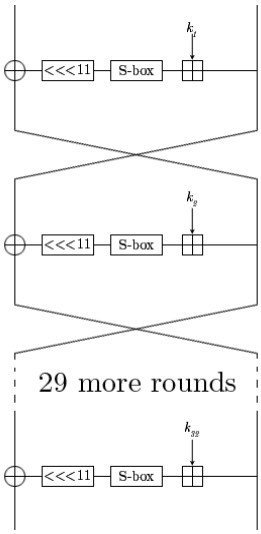
Feistel type systems: DES, Magma are only superficially different from straight through systems like AES.

Write Magma as a straight-through system using Feistelized S-boxes



Solution:

Magma



2 - Cellular Automata in SM4

Two cellular automata are used in SM4, one

$$L(B) = B \oplus B <<< 2 \oplus B <<< 10 \oplus B <<< 18 \oplus B <<< 24$$

in the encryption process and one

$$L'(K) = K \oplus K <<< 13 \oplus K <<< 23$$

in the key schedule.

Determine whether L’ is invertible.

Solution:

L′ is invertible. The encryption and decryption of SM4 has the same structure. The only difference between them is the sequence that the round keys are used: if k_r is the rth round key of SM4 encryption, it is the (33 – *r*)th round key of SM4 decryption.

To show that the function is invertible we have to prove that the function is both One to One and Onto.

Let's check for One to One.

Let $K = (k_0, k_1, k_2, k_3) \in (Z_2^8)^4, K' = (k'_0, k'_1, k'_2, k'_3) \in (Z_2^8)^4$, such that $L'(K) = L'(K')$

$=> K \oplus K <<< 13 \oplus K <<< 23 = K' \oplus K' <<< 13 \oplus K' <<< 23$

$=> K = K'$

Therefore, $L'(K)$ is One to One function.

Now, we have to check for Onto.

$L'(K) = K \oplus K <<< 13 \oplus K <<< 23$

$K \in Z_2^{32}, L'(K) \in Z_2^{32}$

Therefore, Range = Codomain => $L'(K)$ is Onto function.

Since function $L'(K)$ is both One to One and Onto, function $L'(K)$ is Invertible.

3 - Balance

A sequence of bits is balanced if it has the same number of 0s and 1s. A function is called balanced if the sequence of its outputs over all inputs is balanced.

Demonstrate that every column in the table of an invertible n-bit to n-bit function must be balanced.

Proof:

Since the n-bit to n-bit function is invertible, the function is one-to-one and onto. Then every element of the domain has a single image with codomain after mapping and the Range of the function is equal to the codomain. Therefore, every column in the table of the function has the same number of 0s and 1s. Every column in the table of an invertible n-bit to n-bit function is balanced.

4 - Balance

Show that the linear functions (other than 0) are balanced.

Proof:

Let the linear functions (other than 0) be $f(x) = kx + b$.

When $k = 0, b \neq 0, f(x) = b$, obviously the function y is balanced.

When $k \neq 0, b \neq 0$, let $x, y \in R$ such that $f(x) = f(y)$

$=> kx + b = ky + b$

$x = y$

Since $f(x) = f(y) => x = y, \forall x, y \in R$, so function is One to One.

Let $y = kx + b$

$=> x = (y - b)/k$

Since $x \in R, y \in R$, so range of f is given as R, also codomain of $f = R$. Therefore, Range = Codomain => f is Onto function. Hence function $f(x)$ is an invertible n-bit to n-bit function and every column in the table of $f(x)$ must be balanced. Then the sequence of its outputs over all inputs is balanced and the linear functions (other than 0) are balanced.

5 - RSA

Suppose that the RSA modulus is 126, 619 and the encrypting exponent

is 33. What is the decrypting exponent?

Solution:

$n = pq = 126 \times 619 = 77994$

126 is not a prime number

$\phi(n) = (p-1)(q-1) = 125 \times 618 = 77250$

$e = 33$

$\gcd(e, \phi(n)) = 3 \neq 1$

$d = e^{-1} (\mod \phi(n))$ cannot be calculated.