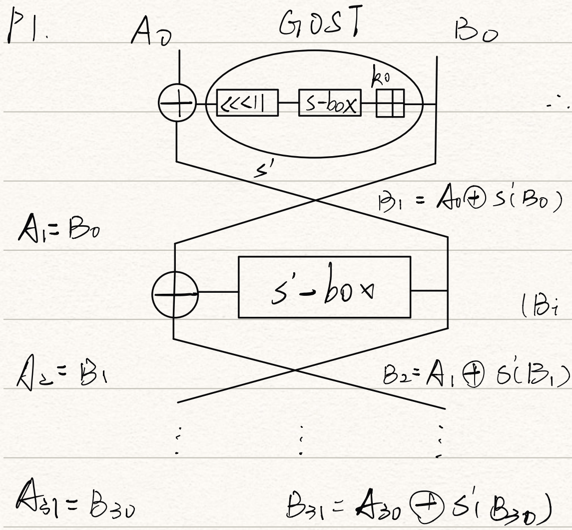
P1.



$A_{i+1} = B_i$, $B_{i+1} = A_i \oplus S'(B_i)$, $i=0,1,\dots,31$

$\therefore (A_{i+1}, B_{i+1}) = (B_i \ll 32) + (A_i \oplus S'(B_i))$, $i=0,1,\dots,31$

So if Magma is a straight through system. we should compute $(B_i \ll 32) + (A_i \oplus S'(B_i))$ in each step.

A_0 is the high 32 bits of the original plaintext and B_0 is the low 32 bits of the original plaintext.

$S'(B_i) = S((B_i + k_i) \bmod 2^{32}) \lll 11$

Think about: I think it is because that DES has additional initial permutation and final permutation.

P2. L' is invertible.

We can transform L' to a matrix form

$$\begin{pmatrix} a_{0,0} & \cdots & a_{0,31} \\ \vdots & \ddots & \vdots \\ a_{31,0} & \cdots & a_{31,31} \end{pmatrix} \begin{pmatrix} k_0 \\ \vdots \\ k_{31} \end{pmatrix}, \quad a_{ij} = \begin{cases} 1, & (32+i-j) \bmod 32 \in \{0, 13, 23\} \\ 0, & \text{otherwise} \end{cases}$$

Obviously. the matrix is non-singular.

So L' is invertible.

P3. Because the function is invertible, it's truth table is one-to-one permutation. For each number of $0, 1, \dots, 2^n-1$, it occurs just once. that is, for each column, the number of 0s and 1s are both the number of permutation of the other $(n-1)$ bits.

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

P4 Linear function $f(x) = \sum_{i=0}^{n-1} k_i x_i$ can be written as xor of $x_0, \dots, x_k$

Proof:

① When $n=1$, then $f_1(x) = x$

there are only 2 conditions: $f_1(x) = 1$ and $f_1(x) = 0$, so $f_1(x)$ is balanced.

② Assume that $f_k(x) = \sum_{i=0}^{n-1} k_i x_i$ is balanced

then $f_{k+1}(x) = f_k(x) \oplus x_{k+1}$.

Since $x_{k+1} \in \{0,1\}$, $X \oplus 0 = X$, $X \oplus 1 = \bar{X}$

$f_{k+1}(x) = f_k(x)$ or $f_{k+1}(x) = f_k(x)$

Since $f_k(x)$ has the same number of 0s and 1s, $f_{k+1}(x)$ also has the same number of 0s and 1s. So $f_{k+1}(x)$ is balanced.

Therefore, the linear functions (other than 0) are balanced.

P5 $n = 126619$, $e = 33$

$n = 127 \times 997$, $p = 127$, $q = 997$

$\varphi(n) = (p-1)(q-1) = 125496$

Because 125496 and 33 are not mutually prime, we cannot get decrypting exponent.

$ed - 1 = \varphi(n) k$, $33d - 1 = 125496k$.

we cannot get integer solution of d, k