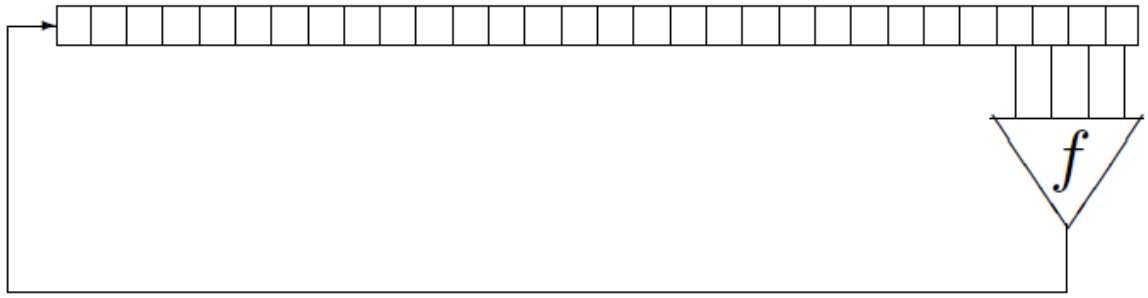
Cryptography Problem Set 1

3180103772 张溢弛

1. Nonlinear Feedback Shift Register

What must the structure of the function f be for the shift register to be invertible?



- NFSR is a structure that commly used in stream ciphers which can feedback the register itself the result of the feedback function ，we can name the feedback function as$f(x_0, x_1, \ldots, x_{n-1})$，function f is always a boolean function, each operaion in the NFSR can be recorded as

$$\begin{bmatrix} x_0 \\ x_1 \\ \cdots \\ x_{n-1} \end{bmatrix} \rightarrow \begin{bmatrix} x_1 \\ x_2 \\ \cdots \\ f(x_0, x_1, \ldots, x_{n-1}) \end{bmatrix}$$

- The function f in NFSR should have at least one non-linear term in the function expression, which will make the time complexity of the function f higher than O(n), which is linear complexity
- To be an invertible function, the structure of f should be$f(x_0, x_1, \ldots, x_{n-1}) = x_0 \oplus g(x_1, \ldots, x_{n-1})$，it is a general conclusion,which is relavant to whether the function f is singular. In such a structure, the singular of f must depend on the x0

2. Cellular Automata in SM4

Two cellular automata are used in SM4, one in the encryption process and one in the key schedule. Determine whether these cellular automata are invertible.You may either approach this problem theoretically or approach it experimentally by programming the automata and running them on the four-billion 32-bit words and testing for invertibility.

- Two cellular automata in SM4 are invertible
- SM4 is a 128-bit block cipher algorithm, the length of key is also 128-bit. The encryption and key management algorithm both use a **32-round** iteration with a round function, which is the form of the cellular automata. SM4 is a kind of Involutive Operator(对合运算), the round key of dectyption is a reverse of the round key of encryption
- SM4 algorithm is involutive，the encryptionSM and decryption SM^{-1} use the same algorithm with different order of the keys, including 32 iterations and 1 reverse，the iteration is in the form
  $X_{i+4} = F(X_{i+1}, X_{i+2}, X_{i+3}, rk_i) = X_i \oplus T(X_{i+1}, X_{i+2}, X_{i+3}, rk_i)$,the reverse is in the form
  $(Y_0, Y_1, Y_2, Y_3) = R(X_{32}, X_{33}, X_{34}, X_{35}) = X_{35}, X_{34}, X_{33}, X_{32}$,the algorithm of key management is
  $rk_i = K_{i+4} = K_i \oplus T'(K_{i+1} \oplus K_{i+2} \oplus K_{i+3} \oplus CK_i)$, and we have
  $C = L(B) = B \oplus (B <<< 2) \oplus (B <<< 10) \oplus (B <<< 18) \oplus (B <<< 24)$
- cellular Automata is an array of cells with each cell assigned a value，a cellular is defined by size，initial state，neighborhood and boundary conditions，the cell with update its value by $s_i^{t+1} = R(s_{i-r}^t, \ldots, s_i^t, \ldots, s_{i+t}^t)$, the function is called global transition function
- A cellular automata is invertible if and only if the global transition function is a one-to-one mapping, in fact we only need to prove the encryption and key management function is invertible.
- In the encryption, the transform of plain text is
  $(x_0, x_1, x_2, x_3) \rightarrow (x_1, x_2, x_3, x_4) \rightarrow (x_2, x_3, x_4, x_1) \rightarrow \ldots\ldots \rightarrow (x_{32}, x_{33}, x_{34}, x_{35}) \rightarrow (x_{35}, x_{34}, x_{33}, x_{32}) \rightarrow (y_0, y_1, y_2, y_3)$
  The final step is a reverse

- In the decryption, the transfrom of the cipher is $(x_{35}, x_{34}, x_{33}, x_{32}) \rightarrow (x_{34}, x_{33}, x_{32}, x_{31}) \rightarrow (x_{33}, x_{32}, x_{31}, x_{30}) \rightarrow \ldots\ldots \rightarrow (x_3, x_2, x_1, x_0) \rightarrow (x_0, x_1, x_2, x_3)$ The final step is a reverse
- We can get $SM^{-1}(SM(x_0, x_1, x_2, x_3)) = (x_0, x_1, x_2, x_3)$, so SM4 is invertible. Which means the cellular automata is invertible.

3. RSA

Suppose that you were to consider employing the RSA cryptosystem with the modulus 35. What is wrong with that modulus other than the fact that it is much too small?

- In RSA algorithm we should choose 2 primes p and q, which n=pq. This time n=25, so p=5 and q=7, $\phi(n) = (p-1)(q-1) = 4 * 6 = 24$
- But 24 has such a property：for any prime p larger than 3，$24|p^2 - 1$
- Prove：It is obviously that p can't be aliquot by 2 or 3，and$p^2 - 1 = (p-1)(p+1)$，p-1 and p+1 must have one can by aliquot bt 3，and one of them can be aliquot by 2 and another aliquot by 4，2*3*4=24,so we have $24|p^2 - 1$, which can be same as $p^2 = 1(mod 24)$，when we choose a d as public key, we could let e=d, it must be an effective private key, which will make the RSA cipher easily broken by others
- We can also **give a counter-example** $gcd(3, \phi(n)) = gcd(3, 24) = 3$ such e^{-1} doesn't exist

Examine the smallest possible RSA moduli: 6 = 2 *3; 10 = 2* 5, up through perhaps 143 = 11* 13; 323 = 17 * 19 or even 899 = 29 * 31. What is the smallest of these that exhibits the attractive properties of the RSA system, for example, keys should not be their own inverses.

- For small primes like p=2,q=3, we have n=6 and $\phi(6) = 2$, and $3^{-1} = 1(mod 2)$, such a RSA can't do encryption because the cipher text is the plain text itself
- For a larger pair p=5 and q=7, we have prove that such p and q are unsafe and wrong
- The next prime is 11 and we found that the smallest moduli can be p=5,q=11 and n=55, e=5, d=27. 11*13 and 17*19 can also be small modulis of RSA