[CS304] Introduction to Cryptography and Network Security

Course Instructor: Dr. Dibyendu Roy — Winter 2022-2023
Scribed by: Akshay (202051018) — Lecture (Week 2)

1 PlayFair Cipher contd..

We pick two letters at a time from our plain text and apply following rules :

1. If both letters are the same (or only one letter is left), add X after the first letter
   (a) Playfair cipher has no rule when the same letters are X. So, it avoid the infinite loop of adding X, we mutually decide any other letter apart from X to b/w two Xs.
   Note: Playfair cipher didn't mention. We can do this modification to use playfair cipher for plaintexts having XX pair(s).
2. If the letters appear on the same row of your table, replace them with the letters to their immediate right respectively (wrapping around to the left side of the row if a letter in the original pair was on the right side of the row.
3. If the letters appear on the same column of your table, replace them with the letters immediately below respectively (wrapping around to the top side of the column if a letter in the original pair was on the bottom side of the column.
4. If the letters are not on the same row or column, replace them with the letters on the same row respectively but at the other pair of corners of the rectangle defined by the original pair. The order is important - the first letter of the encrypted is the one that lies on the same row as the first letter of the plain-text pair.

For decryption we can apply these rules in opposite manner.

2 Hill Cipher

As usual map the alphabets with integers from 0 to 25.
Secret Key: $A = (a_{ij})_{n\times n}$ (invertible matrix)
$a_{ij} \in \mathbb{Z}_{26}$
Plaintext: $M = m_1 m_2 .....m_n$
n = dimension of key and n alphabets are encrypted at a time.

2.1 Encryption

E(M,A) = A*M = $[c_1\ c_2....c_n]^T$ = C
where M is plaintext vector, A is secret key (matrix) and C is cipher vector.

2.2 Decryption

D(C,A) = $A^{-1}C = M$

Note: All the arithmetic operation are done under modulo 26

2.3 Cryptanalysis

It follows S-box, $S : \{A, B, ...Z\} \rightarrow \{A, B, C....Z\}$

$$\text{C} = \text{S(P)}, \ \text{C is known}$$

Total possible S-boxes: $26^{26} \approx 2^{122}$
Brute force attack / exhaustive search

Kerchoff's rule: Design has to be public.

---

3 Shannon's Notion of Perfect Secrecy

If your crypto system is not giving any extra advantage in guessing (probability) the message from cipher text then you system is secure.
E : Encryption algo M : Message
C : Cipher text E(M) = C (going via public channel)
E will be providing perfect secrecy iff the ciphertext does not reveal any information regarding the plaintext/message.

$$Pr[M = m|C = c] = Pr[M = m]$$
$$Pr[message|ciphertext] = Pr[message]$$

4 Symmetric Key Ciphers (classification)

4.1 Block Ciphers

Given any message, it will be divided into multiple blocks of fixed size.
$M = M_0||M_1||.....M_n$ (divided into n+1 blocks)
Encryption is done block-wise.

$$C = Enc(M_0, K)||Enc(M_1, K)||.....||Enc(M_n, K) = C_0||C_1||.....C_n$$

4.2 Stream Ciphers

In this we do the encryption bit-wise.
$M = m_0m_1.....m_l$, where $m_i \in \{0, 1\}$

$$C = (m_0 \oplus Z_0, m_1 \oplus Z_1, ..., m_l \oplus Z_l)$$

To get the message back we have to xor again with same Z :

$$M = (c_0 \oplus Z_0, c_1 \oplus Z_1, ..., c_l \oplus Z_l)$$

$F(K) \rightarrow Z_i \in \{0, 1\}$ (some function to get Zs from secret key K)

5 Product Ciphers

A product cipher combines two or more transformations (functions) in a manner intending that the resulting cipher is more secure than the individual transformation.

5.1 Substitution Permutation Network (SPN)

It is a product cipher based in substitution box and permutation box.

$S : \{0,1\}^n \to \{0,1\}^m$
$P : \{0, ..., m_{r-1}\} \to \{0, \ ...., \ m_{r-1}\}$

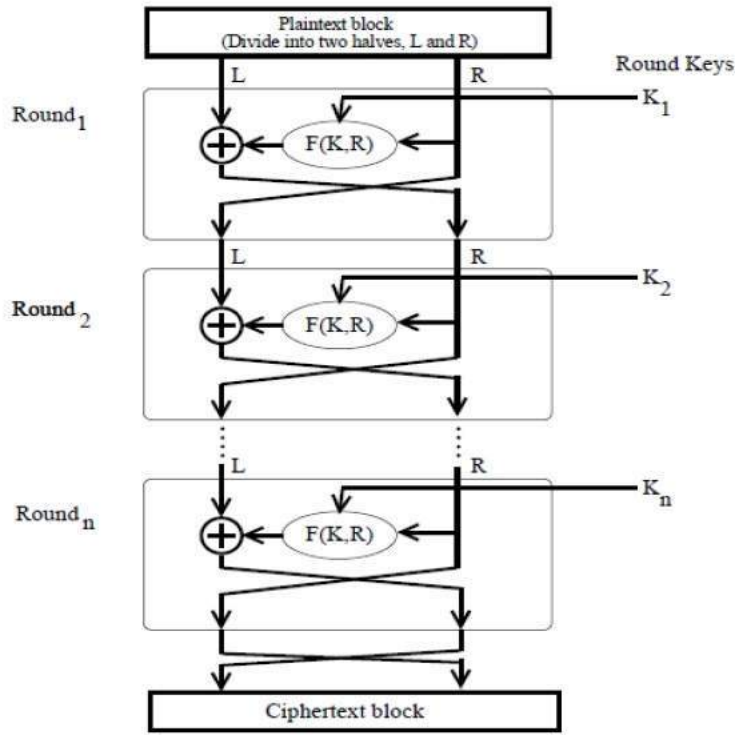
In a SPN based ciphers we have S-box and P-box along with some other functionalities/transformations. In simplest one, we first apply S-box and then P-box to encrypt.

5.2 Fiestal Network

It is also an other type of methodology to design my enc/dec algos.
P $\to$ plaintext of size 2n - bits.

$$P = L_0 || R_0$$

L_0 is left half and R_0 is right half of plaintext.
K : secret key len(K) = l-bits



$F : \{0,1\}^l \times \{0,1\}^n \to \{0,1\}^n$

For i^{th} round:
$L_i = R_{i-1}$
$R_i = L_{i-1} \oplus f(K, R_{i-1})$

6

Data Encryption Standard (DES) is based on Fiestal Network (FN).

Advanced Encryption Standard (AES) is based on SPN.

7 Iterated Block Cipher

An iterated block cipher is block cipher involving the sequential repetition of an internal function (called as Round function). The parameters include the number of rounds r, the block size n, and the round keys K_i of length l generated from the original secret key K.

8 OTP (One Time Padding)

OTP provides perfect secrecy under some conditions.

Encryption: P : plaintext, K: secret key
Enc(P,K) = P$\oplus$K = C
Decryption: Dec(C,K) = C $\oplus$ K = P

Aim: Pr[message | ciphertext] = Pr[message]

Conditions:

- The secret key K cannot be used to encrypt two messages.
- length(K) $\geq$ length(P)
- K is uniformly selected from the key space.