[CS304] Introduction to Cryptography and Network Security

Course Instructor: Dr. Dibyendu Roy — Winter 2022-2023
Scribed by: Pallikonda Sai Teja — Lecture (Week 02)
Student ID : 202011052

1 Hill Cipher

$\mathrm{A} = (\mathrm{a_{ij}})_{\mathrm{nxn}} \quad \Rightarrow$ Invertable matrix $\quad \mathrm{a_{ij}} \in Z_{26}$
$A \Rightarrow$ Secret Key
$\mathrm{M} = (\mathrm{m_1 m_2 .... m_n})$

1.1 Encryption

$$\mathrm{C = A.M = (c_1c_2....c_n)(mod26)}$$

1.2 Decryption

$$\mathrm{M} = A^{-1}.\mathrm{C(mod26)}$$

S = {A,B,..,Z} ⇒ {A,B,..,Z}
P ⇒ C = S(P) C ⇒ Known, S ⇒ Secret key
S = 26^{26} nearly equal to 2^{122}

2 Kerchoff's Rule

Design has to be public

3 Shannon's notion of perfect secrecy

E ⇒ Encryption Algorithm — E(M) = C ⇒ Going via public channel
M ⇒ Message
C ⇒ Ciphertext
E will be providing perfect secrecy iff the ciphertext does not reveal any information regarding the plain text/message.

Pr[M = m,C = c] = Pr[M = m]
Pr[message with ciphertext] = Pr[meassage]
OTP ⇒ One Time Pad

4 Symmetric Key Cipher

1. Block Cipher

2. Stream Cipher

4.1 Block Cipher

M = $m_0||m_1||...||m_l$
The plain text is divided into blocks and each block is encrypted and decrypted using the same key.

4.2 Stream Cipher

M = $m_0m_1...m_l$
In stream cipher bitwise encryption will be done.
Stream cipher is used to encrypt the long messages.

5 Product cipher

5.1 Substitution Permutation Network SPN

It is a product cipher based on Substitution box and Permutation box.
In each round successively a substitution function and a permutation function on the lm bit input to that found are applied.

Example S : $\{0,1\}^n \Rightarrow \{0,1\}^m$, P : {0,1,..,mr-1} ⇒ {0,1,..,mr-1}
length(input) = n*r

5.2 Feistel Networrk

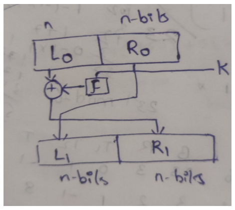
1. In Feistel network, the plain text is of size 2n bits will be there.

2. A Feistel network uses a round function, it will take two inputs – a data block and a subkey – and returns one output of the same size as the data block.

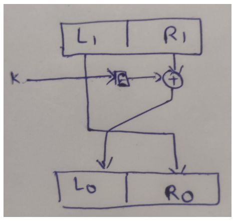
3. Round function(f) may not be invertible but still you can decrypt.

4. The function associated to the feistel cipher in one round is invertible, no matter what is the property of one function 'f'.

f : $\{0,1\}^n$ x $\{0,1\}^l \rightarrow \{0,1\}^n$
2n → Length of plain text
l → Bits in key
Encryption :



$L_1 = R_0$
$R_1 = L_0 \oplus f(R_0,k)$
Decryption :

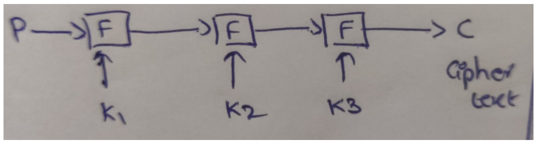


$R_0 = L_1$
$L_0 = R_1 \oplus f(L_1,k)$

6 Iterated Block Cipher

1. An iterated block cipher is block cipher involving the sequential repetition of an internal function(called as round function).
2. 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.
3. Iterated Block Cipher, the number of keys used will be more and encryption will be done based on number of rounds.
4. In this key scheduling function will be there that will generate the round keys.

Example
F ⇒ Round Function
P ⇒ Plaintext block
K ⇒ Secret Key



$G(k) \Rightarrow k_1,k_2,k_3 \Rightarrow$ Round Keys
G(k) ⇒ Key Scheduling function

7 One Time Padding

- One time padding provides the perfect secrecy under some conditions:
  1. Condition-1: We cannot reuse the key to encrypt two messages.
  2. Condition-2: Length of key is greater than length of plain text.

3. Condition-3: The key k is uniformly selected from the key space.

P $\Rightarrow$ Plain Text
K $\Rightarrow$ Secret Key

Encryption(P,k) $= P \oplus k = C$
Decryption(C,k) $= C \oplus k = P$