[CS304] Introduction to Cryptography and Network Security

Course Instructor: Dr. Dibyendu Roy Winter 2023-2024

Scribed by: Manas Jitendrakumar Ingle (202151086) Lecture (Week 2)

1 Total Permutations[Complexities]

Let $\{A, B, C, \ldots, Z\}$ be the alphabet. The encryption function is defined as:
E_s(M) = S(m_1)S(m_2)....S(m_n) = C

total possibilities = 26!
The total number of permutations is 26!, which is approximately equal to 2^{80} possible permutations. The encryption function for a simple affine cipher is given by:

$$C = e_k(x) = (a \cdot x + b) \mod m$$

k = (a,b) where $0 \leq a, b \leq 25$

- Modulus m is the size of the alphabet.
- a and b are the key parameters of the cipher.
- a must be chosen such that a and m are coprime.

The total combinations of a and b are 12×26.

2 Hill Cipher

Secret key → $A = (a_{ij})_{n \times n}$ (invertible matrix)

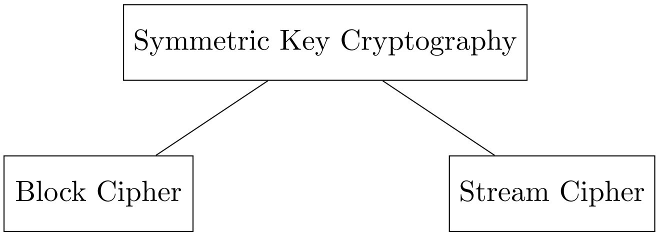
$M = m_1 \cdot m_2 \cdot m_3 \ldots m_n$ → Plaintext

Ciphertext → $C = A \cdot M$ (encryption algorithm)

$$C_j = \sum_{j=1}^{n} a_{ij} \cdot m_j$$

Decryption: $M = A^{-1} \cdot C$

3 Symmetric Key Cryptography



4 Block Cipher :

A block cipher is a cryptographic algorithm that processes a fixed-size block of plaintext as a whole and transforms it into an equally-sized block of ciphertext.
It is an Implementation of ECB(electronic code book) mode of operation

$M = m_0 \,\|m_1 \,\|m_2 \,\|....\|m_n$
$\mathrm{len}(M) = m \quad \mathrm{len}(m_i) = l \hookleftarrow \textit{blocksize}$

Encryption :

$C = E_{nc}(m_0,k) \,\|E_{nc}(m_1,k) \,\|.....\|E_{nc}(m_n,k)$

ciphertext $C = C_0 \,\|C_1 \,\|C_2 \,\|...C_n$

$E_{nc}(m,k) = C \quad E_{nc} = M$

Decryption :

$M = \mathrm{Dec}(C_0,k) \,\|Dec(C_1,k) \,\|......\|Dec(C_n,k)$

$M = m_0 \,\|m_1 \,\|m_2$ where $\mathrm{len}(m_0) = \mathrm{len}(m_1) = n$ and $\mathrm{len}(m_2) = l$

length = $2n+l$ where $l \leq n$

$C_0 = E_{nc}(m_0,k), \quad C_1 = E_{nc}(m_1,k), \quad C_2 = E_{nc}(m_2 \,\|0^{n-l},k)$

$C = C_0 \,\|C_1 \,\|C_2$ where $C_2 \rightarrow m_2 \,\|0....0 \hookleftarrow$ *padding to make length equal*

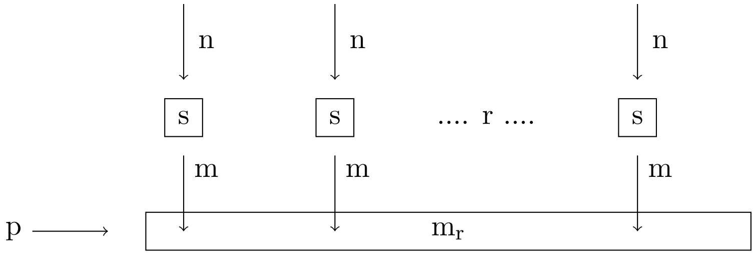
5 Product Cipher :

It combines two or more transformations in a manner intending that the resulting ciphers is more secure than it's individual components.

Example: Substitution Permutation Network (SPN)

Plaintext P : $\{0,1\}^{m\cdot r} \rightarrow \{0,1\}^{m\cdot r}$

Ciphertext S : $\{0,1\}^n \rightarrow \{0,1\}^m$



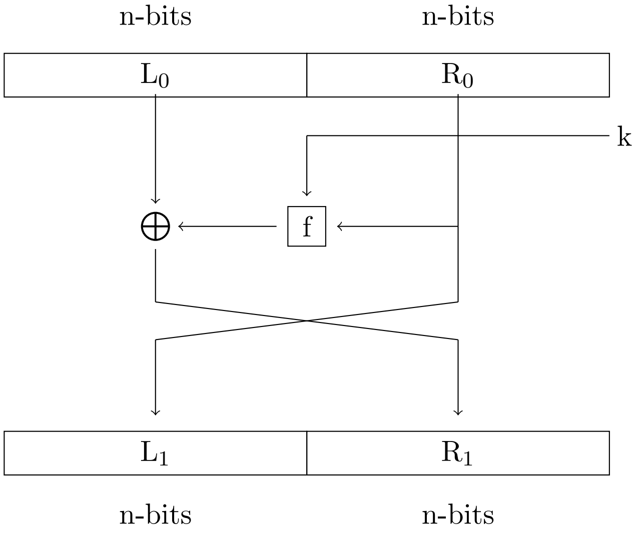
6 Fiestel Network

There are several steps in making a fiestel network.

- The data is divided into equal left and right part.
- In the next iteration the right part from the previous iteration becomes the left part of the next iteration
- For the right part
  - We have a function F that takes 2 parameters, a piece of data and a secret key k.
  - We apply the function on right part of the previous iteration and a secret key k
  - then we take the output and xor it with the left part of the previous part of the iteration. This becomes the right part of the next iteration.

Below image explains the above steps

Encryption :
f : $\{0,1\}^n \times \{0,1\}^k \rightarrow \{0,1\}^n$
$L_1 = R_0$
$R_1 = L_0 \oplus f(\mathrm{R}_0, \mathrm{k})$



This Image shows Demonstration of a single Round..Such Multiple(r) rounds can exist.

Decryption : $L_0 = R_1 \oplus f(\mathrm{L}_1,\mathrm{k})$

7 Iterated Block Cipher

It is a Block Cipher where involving the sequential repetition of an internal function called as round function where tha parameters include the number of rounds 'r', the block size 'n' and bit size 'x^k' of the input key 'k' from which 'r' subkeys 'k_i' (round keys) are derived.

Example: 2-round iterated block cipher encryption

Encryption: $\mathrm{F}(k_1,\mathrm{P}) \rightarrow \mathrm{C}_1 \rightarrow F(\mathrm{k}_2,C_1) = C$
$WhereP \rightarrow Plaintext \quad C \rightarrow Ciphertext$

rounds = 2
round keys = k_1, k_2

k $\rightarrow G(k) \rightarrow$k$_1$, k_2 Where G is Key Scheduling Algorithm

Decryption: C $\rightarrow \mathrm{F}^{-1}(C_1,k_2) \rightarrow \mathrm{C}_1 \rightarrow \mathrm{F}^{-1}(C_1,k_1)$ = plaintext P

8 Data Encryption Standard (DES):

- Designed by IBM it is based on Fiestel network. DES is an iterated block cipher with 16 rounds.
- It has a secret key of 64-bit and the plaintext block size of 64-bit as well.
- In the 64-bit key, there are 8 parity check bits. So, those 8 bits are decided by the remaining 56 bits. Which means that the ctual key is ascutally only 56-bit
- **Encryption :**

$$\begin{tikzcd} & \text{K 56/64-bit} \arrow[d] & \\ \text{P 64-bit} \arrow[r] & \boxed{\text{DES}} \arrow[r] & \text{C 64-bit} \end{tikzcd}$$

- **Decryption :**

$$\begin{tikzcd} & \text{K 56/64-bit} \arrow[d] & \\ \text{C 64-bit} \arrow[r] & \boxed{\text{DES}} \arrow[r] & \text{P 64-bit} \end{tikzcd}$$

- **Key scheduling algorithm for 64-bit key :**

  Keys K $\rightarrow$k$_1$, k_2, k_3...., k_{16}

  Where every K_i is of 48-bit

  input P (64-bit) IP(initial permutation) : $\{0{,}1\}^{64} \rightarrow \{0,1\}^{64}$