[CS309] Introduction to Cryptography and Network Security

Course Instructor: Dr. Dibyendu Roy
Scribed by: Kunj Thakkar (202251142)

Autumn 2024-2025
Lecture (Week 1&2)

1 Introduction

- Cryptography is a component of CryptoLogy.
- Cryptology = Cryptography + Cryptoanalysis
  - Where, Cryptography is Design algorithm for security purposes and CryptoAnalysis is analysis of the algorithm
- While designing algorithm, certain amount of analysis has to be done to measure its security
- In daily life, cryptographic algos are used in applications like Whatsapp, Youtube, etc.

1.1 Features of Cryptography

Confidentiality - Hide info in such a way that only desired person is able to read/access that information
Encryption - Algorithm to hide the information in a different way that it is not readable by human until he/she has key to decrypt it.
Decryption - Algorithm to extract hidden information gained by encrypting the plain text with the decryption key.

$$Enc(M, K) = C \quad Dec(C, K) = M$$

Where, M is message to encrypt, K is key used for encryption and decryption C is cipher text

There should exist decryption function for every encryption function

2 Caesar Cipher

- Named after *Julius Caesar*
- It relies on shifting the letters of a message by agreed number

Lets agreed number is N, then

$$E(x, N) = (x + N)\%26$$

$$D(c, N) = (c + 26 - N)\%26$$

Example

PlainText = INTERNET
N = 3
Then, CipherText = LQWHUQHW

3 Important Definitions

Definition 1 (Function) *A function $f : A \to B$ is a relation between the elements of A and B with the property that if $a \in A$ and $b \in B$, then $f(a) = b$ if and only if $(a, b) \in f$.*

Definition 2 (One-to-One Function) *A function $f : A \to B$ is one-to-one if for all $a_1, a_2 \in A$, $f(a_1) = f(a_2)$ implies $a_1 = a_2$.*

Definition 3 (Onto Function) *A function $f : A \to B$ is onto if for every $b \in B$, there exists an $a \in A$ such that $f(a) = b$.*

Definition 4 (Bijective Function) *A function $f : A \to A$ is bijective if f is one-to-one and onto.*

Definition 5 (Permutation) *Let S be a set. A permutation on S is a bijection from S to S.*

$$\pi : \{1, 2, 3, 4\} \longrightarrow \{1, 2, 3, 4\}$$

then possible function maping can be

$$1 \longrightarrow 2,\ 2 \longrightarrow 3,\ 3 \longrightarrow 1,\ 4 \longrightarrow 4$$

Definition 6 (One-Way Function) *A function $f : X \to Y$ is called a one-way function if:*
** Given $x \in X$, it is easy to compute $f(x)$. * Given $f(x) \in Y$, it is hard to find $x \in X$ such that $f(x) = y$.*

Example
p is large prime number
q is large prime number
then computing $N = p * q$ is easy but given N finding two larger prime numbers p and q is tough

Definition 7 (Substitution Box (S-box)) *An S-box is a function $S : A \to B$ with $|B| \leq |A|$. It is typically a mapping between sets of binary strings.*

4 Transposition Cipher

$$M = m_1 m_2 m_3 m_4 m_5 m_6 ....m_t \longrightarrow \text{Plain text}$$

$$e : \text{permutation on t elements} \longrightarrow \text{Secret Key}$$

Encryption

$$C = m_{e(1)} m_{e(2)} .....m_{e(t)} = C_1 C_2 .....C_t$$

if e(1) = 5 then,

$$m_1 \longrightarrow m_5$$

Decryption

$$C = C_{e^{-1}(1)} C_{e^{-1}e(2)} .....C_{e^{-1}e(t)} = m_1 m_2 .....m_t$$

Example

plainText = CAESAR = $m_1 m_2 ... m_6$
SecretKey e:

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 4 & 1 & 3 & 5 & 2 \end{bmatrix}$$

CipherText = RSCEAA = $C_1 C_2 .... C_6$
d = e^{-1}:

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 4 & 2 & 5 & 1 \end{bmatrix}$$

5 Substitution Cipher

M = $m_1 m_2 .... m_t$
A = {A, B, C, ... Z} $m_1 \epsilon A$
e: Substitution from A to A

Encryption

$$C = e(m_1) e(m_2) e(m_3) .... e(m_t)$$

Example

$$e(A) = z \quad e(B) = D \quad e(C) = A$$

$$\text{ABC} \longrightarrow \text{plain text}$$

$$\text{ZDA} \longrightarrow \text{cipher text}$$

6 Affine Cipher

$$\begin{array}{ccccc} A & & BC & & \cdots Z \\ \downarrow & & \downarrow\downarrow & & \downarrow \\ 0 & & 12 & & 25 \end{array}$$

$A \rightarrow$ set of alphabets

$$Z_n = \{xmodn\} = x\%n$$

$A \longrightarrow Z_{26}$ x: Plain Text $x \epsilon Z_{26}$
k : Secret Key $= (a, b) \epsilon Z_{26} x Z_{26}$

Encryption

$$e(x, k) = (ax + b)\%26$$

Decryption

$$d(c, k) = ((c - b)a^{-1})\%26$$