[CS304] Introduction to Cryptography and Network Security

Course Instructor: Dr. Dibyendu Roy — Winter 2022-2023
Scribed by: Rathva Kaushikkumar Sanjaybhai (202051156) — Week : 1 (1st lecture#)

1 Cryptology:

1.1 Parts of Cryptology:

Definition 1 *Cryptography : We develop/design algorith to make system secure.*

Definition 2 *Cryptoanalysis : We try to penetrate the security of system.*

Definition 3 *Cryptology = Cryptography + Cryptoanalysis.*

Remark 1 *NIST(National Institute of Standards and Technology) is a Institution that Standardizes Cryptographic Algorithms.*

2 Encription and Decryption

2.1 Encription

Encription can be defined by $\underline{E(P,k) = C}$. Encription is process to convert/transform plain (readable[2]) text into cipher(unreadable [3]) text.

2.2 Decryption

Decryption can be defined by $\underline{D(C,k) = P}$. Decryption is process to convert/transform cipher text to plain text.

Where,
$P = Plaintext$
$C = Ciphertext$
$k = Secretkey$

2.3 Example:

ATM 1 → PIN 1 + X = Y1
ATM 2 → PIN 2 + X = Y2
ATM 3 → PIN 3 + X = Y3
.
.
.
ATM 10 → PIN 10 + X = Y10

Remark 2 *Here,X → Secret*

[2] it's meaning is known by reading it and can be used directly where it's intended.
[3] it's meaning can't known by reading it and can't used as intended directly.

3 Cryptography :

3.1 Symetric key cryptograpy

Both Encryption and Decryption keys are the same in this type of cryptography.
Encryption : $E(P, k) = C$¡
Decrytion : $D(C, k) = P$

Where ,
$P = plaintext,$

3.2 Public key cryptograpy

Encryption and Decryption keys are diffrent but both are related.

There are two keys :

1. Public key : which can be seen by anyone.
2. Secret key : This key is kept secret and known reciever.This key is related to public key.

4 Cryptography provides following security services :-

4.1 Confidentiality(Secrecy) :

It means that the massage is only known or understood by desired people.

4.1.1 Plain text :

original massage.

4.1.2 Encription Algorithms :

function

4.1.3 Decryption Algorithm :

function

4.1.4 Cipher text :

un-readable form of plain text.

4.1.5 Encription key :

key

4.1.6 Decryption key :

key

4.2 Integrity

Integrity means Text on both Sender and the Receiver end is same.

4.3 Authentication

Authentication is a process to identify desired person.

4.4 Non-repudiation

A mechanism to prove that sender sent the message.

5 CAESAR cipher :

This cipher is named after Julius caesar.It works by shifting letters of mases by an agreed number. Here we are taking agreed number =3.

If we give/map all alphabet a number staring from 0.
A → 0, B → 1, C → 2, . . ., Z → 25

while Encrypting shift right all the letters by 3.

plain text → INTERNET
agreed number = 3 → secret key
Cipher text → LQWHUQHW

while Decrypting shift left all the letters by 3.

Plain text → INTERNET