[CS304] Introduction to Cryptography and Network Security

Course Instructor: Dr. Dibyendu Roy Winter 2022-2023
Scribed by : Pallikonda Sai Teja Lecture (Week 01)
Student ID:202011052

1 Introduction

- Cryptography:The part where we develop algorithms to get security / Designing the algorithm.
- Cryptanalysis: It is to break the security of a designed algorithm.

Cryptology = Cryptography + Cryptanalysis.
NIST standardizes cryptographic algorithms

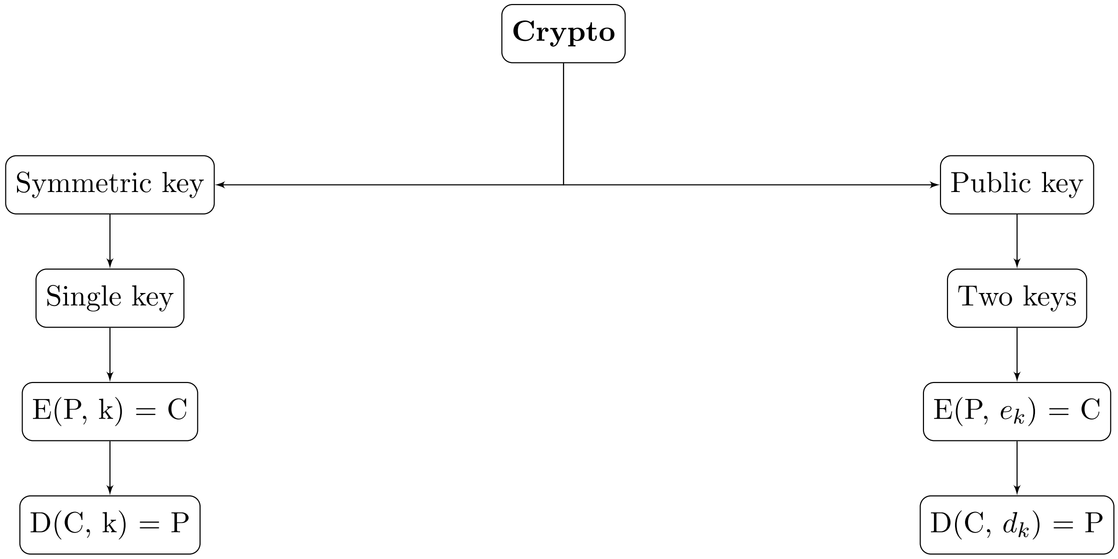
2 Encryption and Decryption

⇒ Encryption:The process of converting plaintext into Ciphertext .

$$E(P, k) = C$$

Plain Text + Secret Key = Cipher Text.
⇒ Decryption:The process of converting Ciphertext into plaintext.

$$D(C, k) = P$$



3 Security Services in Cryptograpy

1. Confidentiality:Ensuring that no one can read the message except the intended receiver .
2. Integrity: Assuring the receiver that the received message has not been altered in any way from the original.
3. Authentication: verification of one's identity.
4. Non-repudiation: A mechanism to prove that the sender really sent this meassage.

⇒ Confidentiality :
i) plaintext $\rightarrow originalmessage$
$ii) Encryption Algorithm \rightarrow function$
$iii) Ciphertext \rightarrow unreadableformofplaintext$
$iV) Decryptionalgorithm \rightarrow functioin$

⇒ Encryption function

$$\text{E(M, } e_k\text{) = C}$$
$$f : P \times e_k \rightarrow C$$

⇒ Decryption function

$$\text{D(C, } d_k\text{) = M}$$
$$f : C \times d_k \rightarrow P$$

4 Cryptographic Algorithms

4.1 Functions

$f : A \rightarrow B$ is a relation between the elements of A and B with the property that if $a, b \epsilon A$ and $a = b$, then $f(a) = f(b)$

- One-to-one: $f(a) = f(b) \Rightarrow a = b$
- Onto: $f : A \rightarrow B$ then ∀ b ϵ B, ∃ a ϵ A such theat $f(a) = b$.
- Bijective: $f : A \rightarrow B$ is bijective iff f is one-to-one and onto.
- Permutation: Let π be a permutation on a set S then $\pi : S \rightarrow S$ is a bijective function from S to S.
- One way: $f : X \rightarrow Y$ is called a one-way function if given $x \epsilon X$, it is easy(within polynomial time) to compute $f(x)$ but converse is not true.

  E.g.: Prime factors of a product of two primes.

4.2 Classical ciphers

4.2.1 Ceaser Cipher

⇒ Named after Julius Caeser ⇒ Shifting the letters of a message by k places.

agreed value of k = 3.

E.g.: D → G (Right shift by 3).

$$E(x,3) = (x+3)\%26 = C$$
$$D(C,3) = (x+26-3)\%26$$

E.g.: INTERNET → LQWHUQHW

Substitution Box

$$\Rightarrow S : A \to B \text{ with } |B| \leq |A|$$

⇒ E.g.: $S : 1,2,3,4 \to 1,2,3.$

4.2.2 TranspositionCipher

$\Rightarrow M = m_1 m_2 m_3 ... m_t$
$\Rightarrow e$: permutation on t elements → secret key

⇒ Encryption:

$C = m_{e(1)} m_{e(2)} m_{e(3)} m_{e(4)} \dots m_{e(t)}$

⇒ Decryption:

$C = m_{e(1)} m_{e^{-1}(2)} m_{e^{-1}(3)} m_{e^{-1}(4)} \dots m_{e^{-1}(t)}$

E.g.: CAESER

C	A	E	S	E	R
R	S	C	E	A	A

Secret Key					
1	2	3	4	5	6
6	4	1	3	5	2

4.2.3 Substitution Cipher

E.g. $e(A) = Z, e(B) = D, e(C) = A$

Plain text:	A	B	C
Cipher text:	Z	D	A

4.2.4 Affine Cipher

A	B	C	...	Z
0	1	2	...	25

$A \rightarrow \mathbb{Z}_{26}$
$k =$ secret key $= (a,b)\epsilon\mathbb{Z}_{26} \times \mathbb{Z}_{26}$ and $gcd(a,26) = 1$
$\Rightarrow$ Encryption:
$e(m,k) = (am+b)mod26 = c$

$\Rightarrow$ Decryption:
$d(c,k) = ((c-b)a^{-1})mod26$
$a * a^{-1} = 1mod26$

Proof of why it is possible to find Multi. Inverse iff $gcd(x,m) = 1$

$\Rightarrow$ $0 \neq x\epsilon\mathbb{Z}_m$

$\Rightarrow$ $gcd(x,m) = 1$

$\Rightarrow$ $x *_m y = 1$

$\Rightarrow$ $xy = 1modm$

$\Rightarrow$ $m\|(xy-1)$

$\Rightarrow$ $xy - 1 = t \cdot m$

$\Rightarrow$ $1 = t_1 m + xy$ for some t_1

$\Rightarrow$ It is proven that $gcd(x,m)$ can be written in the form of $ax + by$ (linear combination)

$\therefore gcd(x,m) = t_1 m + xy$

$\Rightarrow$ To find (t_1, y), we have to follow the extended euclidean algorithm

4.2.5 Playfair Cipher

E.g.: Secret key = PLAYFAIR EXAMPLE

P	L	A	Y	F
I	R	E	X	M
B	C	D	G	H
K	N	O	Q	S
T	U	V	W	Z

Plaintext: HIDE	
HI	DE
↓	↓
BM	OD
Ciphertext: BMOD	

$\Rightarrow$ For odd length, we add an X to the end. ODD → $\underline{\text{OD}}$ $\underline{\text{DX}}$