[CS304] Introduction to Cryptography and Network Security

Course Instructor: Dr. Dibyendu Roy — Winter 2022-2023
Scribed by: Akshay (202051018) — Lecture (Week 1)

1 Introduction

Cryptography: The part where we develop algorithms to get security (Designing the algorithm).

Cryptanalysis: We try to break the security of the designed algorithm.

$$\text{Cryptology} = \text{Cryptography} + \text{Cryptanalysis}$$

NIST is an organisation which standardizes cryptographic algorithms.

An Easiest Example:
Suppose I want to keep the pins of my ATM cards. One super easy way is to write the pin on the card itself but this type of implementation is highly insecure. If somebody steals my card then he/she will easily get the pin. To keep the pin secure what I can do is choose a specific number (key) add it to each pin number and write the resultant number (cipher) on the corresponding ATM card.

$$\begin{gathered}\text{ATM 1} \rightarrow \text{PIN 1} + \text{X} = \text{Y1}\\ \text{ATM 2} \rightarrow \text{PIN 2} + \text{X} = \text{Y2}\\ .\\ .\\ .\\ \text{ATM n} \rightarrow \text{PIN n} + \text{X} = \text{Yn}\end{gathered}$$

Now, to retrieve my pin I will just subtract X from the number written on the card. Keeping the X secret no none will be able to steal my pin even if he/she knows that I performed addition.
Nomenclature:

$$\begin{gathered}\text{PIN : Plain text (P)}\\ \text{X : Secret key (K)}\\ \text{Y : Cipher text (C)}\end{gathered}$$

Encryption: It is a function which takes plain text and key as argument and returns cipher text.

$$\text{E(P,K)} = \text{C}$$

Decryption: It is a function which takes cipher text and key as argument and returns meaningful plain text.

$$\text{D(C,K)} = \text{P}$$

2 Classification of Cryptography Algorithms

2.1 Symmetric Key Cryptography

Under this encryption and decryption keys are kept **same** and **secret**.

2.2 Asymmetric Key Cryptography

- Encryption and decryption keys are kept different but not random. They are related somehow.
- Some keys are kept public while others are kept secret.

3 Cryptography provides following security services:

1. Confidentiality (secrecy): Hiding the message from undesirable person. To achieve confidentiality encryption and decryption algorithms are used.
2. Integrity: Refers to the assurance that a message has not been tampered with or altered during transmission.
3. Authentication: Process of verifying the identity of a person or device. This is typically done through the use of a username and password, or by using a digital certificate.
4. Non-repudiation: A mechanism to prove that the sender really sent this message.

4 CAESAR Cipher

This cipher is named after Julius Caesar. It refers on shifting the letters of a message by an agreed number.

$$\text{agreed number} = 3$$

We map the English alphabets with integers. A to 0, B to 1, ... Z to 25.
if 'x' is a plain text:
E(x,3) = $(x+3)\%26$
D(c,3) = (c - 3 + 26)%26 [26 is added to avoid negative output]

5 Revisiting Maths

5.1 Function

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

5.2 One to One Function

f(a) = f(b) $\implies$ a = b

5.3 Onto Function

f : A $\rightarrow$ B then $\forall$ b $\in$ B $\exists$ a $\in$ A such that f(a) = b.

5.4 Bijective Function

f : A $\rightarrow$ is bijective function iff f is one to one and onto.

5.5 Permutation

Let π be a permutation on a set S then π : S → S is a bijection from S to S.
E.g:
$\pi : \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$

5.6 One way Function

f : X → Y is called a one way f given x ∈ X it is easy to compute f(x) but given it is hard to find x.
E.g.
Given that p and q are large prime numbers, computing N = p*q is easy.
Given N, finding p and q (large prime numbers) s.t. N = p*q is hard.

5.7 Substitution Box

S : A → B with $|B| \leq |A|$
E.g.:
S : $1, 2, 3, 4 \rightarrow 1, 2, 3$
S(1) = 1, S(2) = 3, S(3) = 2, S(4) = 1

6 Transposition Cipher

$$M = m_1 m_2 m_3 .....m_t \text{ (plain text)}$$

e : **permutation** on t elements → Secret key

6.1 Encryption

Cipher text, $C = m_{e(1)} m_{e(2)} .....m_{e(t)} = c_1 c_2 .....c_t$
If e(1) = 5 then m_5 is placed at position 1.

6.2 Decryption

$M = c_{e^{-1}(1)} c_{e^{-1}(2)} ......c_{e^{-1}(t)}$

E.g.:
Plaintext : CAESAR = $m_1 m_2 .....m_6$

Secret key, e : $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 4 & 1 & 3 & 5 & 2 \end{pmatrix}_{encryption}$

Cipher text : RSCEAA = $c_1 c_2 c_3 ....c_6$

$d = e^{-1} : \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 4 & 2 & 5 & 1 \end{pmatrix}_{decryption}$

7 Substitution Cipher

$M = m_1m_2.....m_t$
$S = \{A, B, C, ...Z\},\ m_i \in S$
e : Substitution from S to S, e → Secret key.
Encryption: $C = e(m_1)e(m_2).....e(m_t)$

E.g.:
e(A) = Z, e(B) = D, .. e(C) = A
plain text : ABC
cipher text : ZDA

8 Affine Cipher

A is mapped to 0, B to 1, ... , Z to 25.
S : set of alphabets
$S \longrightarrow \mathbb{Z}_{26}$
K = secret key = (a, b) $\in \mathbb{Z}_{26} \times \mathbb{Z}_{26}$

Encryption : e(x, K) = (a*x + b)$mod26$ = C

Decryption : d(C, K) = $((c - b) * a^{-1})mod26$

$\boxed{\text{Inverse of a number 'a' under modulo 26 exists only when gcd(a, 26) = 1}}$

8.1 Proving that modular inverse of x only exists when gcd(x, m)=1

If y is the inverse of x under moudulo m then:
xy = 1 mod m
$\Longrightarrow$ m divides (xy-1)
$\Longrightarrow$ xy - 1 = t*m
$\Longrightarrow$ 1 = x*y + m*t
Now, using Extended Euclidean Algorithm we can say that gcd(x, m) = 1
[$gcd(a, b) = a * x + b * y$]

8.2 Basic Euclidean Algorithm to find gcd(a, b)

- while one of the number does not become 0
  - subtract the multiple of smaller number from the bigger number. Resultant will the remainder. We can do so by taking bigger number modulo smaller number
  - Replace bigger number with this remainder

Reasoning:
a = gx (say) ; b= gy (say) , where g is gcd of a and b then gcd(x,y) = 1 because after taking out the highest common factor from two numbers (which is g here) , nothing common lefts in them.
now if $b < a$, a-b = g(x-y) $\Longrightarrow$ gcd(a-b,b) = g = gcd(a,b)
If we keep on doing this then both number a, b will become equal to gcd (g) at some point.

When we are subtracting b from a till $a > b$ ultimately we are removing multiple of b from a and leaving the remainder. For $a > b$, let's say a = n*b + r, where n is the number of times b is present in a and r is the rest part. So, instead of removing b one by one from a till $a > b$, we can optimize this process by directly reaching r via the modulus operator.

8.3 For how many numbers does inverse exist under modulo m?

Answer is **Euler Totient Function ($\phi(m)$)**
$\phi(m)$ = Number of positive integers less than 'm' that are relatively prime to m
(i.e., gcd(integer, m) = 1).

$\phi(m)$	**Criteria of 'm'**	**Formula**
	'm' is prime	$\phi(m) = m - 1$
	m=p*q p and q are primes	$\phi(m) = (p - 1) * (q - 1)$
	m=a*b Either a or b is composite. Both a and b are composite	$\phi(m) = m * (1 - \frac{1}{p_1})(1 - \frac{1}{p_2})$..... where $p_1, p_2, ...$ are distinct primes.

26 = 13*2

Thus we have 12 meaningful choices for 'a' in the Affine cipher. Still 26 choices for 'b'

$\therefore$

Total valid keys possible = 12*26 = 312

9 Playfair Cipher

Plain text : HIDE
Secret Key : PLAYFAIR EXAMPLE

Key Schedule :

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

- Create a 5x5 table
- First write the secret key, drop any duplicate letters
- Fill the rest of the table with the remaining letters of the alphabet.
- I and J are put in the same space since we have 26 letters

We pick two letters at a time from our plain text and apply following rules :

1. If both letters are the same (or only one letter is left), add X after the first letter

2. If the letters appear on the same row of your table, replace them with the letters to their immediate right respectively (wrapping around to the left side of the row if a letter in the original pair was on the right side of the row.

3. If the letters appear on the same column of your table, replace them with the letters immediately below respectively (wrapping around to the top side of the column if a letter in the original pair was on the bottom side of the column.

4. If the letters are not on the same row or column, replace them with the letters on the same row respectively but at the other pair of corners of the rectangle defined by the original pair. The order is important - the first letter of the encrypted is the one that lies on the same row as the first letter of the plain-text pair.

Plain text :	HI	DE
Cipher text :	BM	OD