[CS304] Introduction to Cryptography and Network Security

Course Instructor: Dr. Dibyendu Roy — Winter 2022-2023
Scribed by: Chitranshi Srivastava (202051055) — Lecture 1 and 2 (Week #1)

1 Introduction

- **Cryptography**
  This is the part where we develop algrithms for security
- **Cryptanalysis**
  This is the part where we try break the security of designed algorithm to analyze its strength

Cryptology = Cryptography + Cryptanalysis
NIST(National Institute of Standards and Technology) - Standardizes crptographic algorithms(reviews both design and implementation)
Example:
ATM1 → pin1 + x = y1
ATM2 → pin2 +x = y2
Here x is secret. We can write y1 on our atm card and when we want to use it, we can simply substract x from y to get the actual pin.

- **Encryption :** Converting readable text into unreadable text
  E(P, K) = C
- **Decryption :** Converting unreadable text into meaningful, readable text
  D(C, K) = P

In above example, pin1 is the Plain text, x is the secret key and y1 is the Cipher text. Encryption and Decrption function is always public, only hidden thing is secret key.

2 Types of Cryptography :

1. Symmetric Key Cryptography : It has one secret key for both encryption and decryption functions
2. Public Key Cryptography : It has two different keys for encryption and decryption(public key and secret key). The keys are related but are different.

3 Security Services

Cryptography provides the following security services :

1. **Confidentiality**
   It stands for hiding information from undesired and unauthorized persons.

2. **Integrity**
   It means that the information cannot be altered and if it is altered then it would be properly notified(only specified and authorized alterations allowed)

3. **Authentication**
   It means that we are able to verify that the information is coming from desired source.

4. **Non-repudiation**
   It is a mechanism to prove that the sender has actually sent a particular message(actions can be traced uniquely)

Confidentiality can be achieved by encryption and decryption.

- Plain text → original message
- Encryption Algorithm → function
- Cipher text → un-readable form of plain text
- Decryption Algorithm → function

Encryption function (M, Encryption key) = Cipher text
(P x Encryption key → C)
Decryption function (C, Decryption key) = Plain text
(C x Decryption key → P)

4 Definitions

- **Function**
  f : A → B is a relation between the elements of A and B such that
  if a,b ∈ A and a=b, then f(a) = f(b)
- **one to one function :**
  f(a) = f(b) ⇒ a = b
- **onto function :**
  f : A→B , then ∀ b∈B ∃ a∈A such that f(a) = b
- **Bijective function :**
  f : A → B is bijective iff f is one to one and onto
- **Permutation :**
  Let π be a permutation on a set S, then π : S → S is a bijection from S to S
  $\pi : \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$
- **one-way function :**
  f : x → y is one-way if it is easy to compute f(x) (in polynomial time) but it is very difficult to find x if f(x) is given.
  Eg. Finding product of two prime numbers is easy if the numbers are given. But if we are given a large product and we have to find the prime numbers which give that product, it is difficult. f(x) = p*q, where p and q are prime. Hence, f(x) is one-way function.
- **Substitution box :**
  S : A → B , $|B| \leq |A|$.

5 Classical Ciphering Techniques

5.1 Caesar Cipher

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

agreed number = 3(for caesar cipher)

E(x,3) = (x+3)%26

D(c,3) = (c+26-3)%26

Example:

plain text → INTERNET

key = 3

Encryption : cipher text → LQWHUQHW

Decryption : plain text → INTERNET

5.2 Transposition Cipher

It is a type of cipher where the order of alphabets in plain text is rearranged to create the cipher text.

$M = m_1m_2m_3m_4....m_t$

Now we do a permutation on t elements.

Encryption : $C = m_{e(1)}m_{e(2)}m_{e(3)}m_{e(4)}....m_{e(t)} = c_1c_2c_3c_4....c_t$

Decryption : $M = c_{e^{-1}(1)}c_{e^{-1}(2)}c_{e^{-1}(3)}c_{e^{-1}(4)}...c_{e^{-1}(t)} = m_1m_2m_3m_4....m_t$

Example:

Plain Text: CAESAR

Secret Key (e): 641352

Cipher Text: RSCEAA

The secret key indicates that the character on the e_i position of plain text should be moved to the i^{th} position to generate cipher text.

Cipher Text: RSCEAA

Secret Key (e^{-1}): 364251

Plain Text: CAESAR

It is a symmetric cryptographic technique.

5.3 Substitution Cipher

In this method, cipher text is generated by substituting the letters of plain text by some other alphabets or symbols. The cipher text may include some new characters that are different from the plain text.

Encryption : $C = e_{m_1}e_{m_2}.....e_{m_t}$

where e is the secret key

5.4 Affine Cipher

It is a more generalized version of shift cipher(substitution cipher). The encryption key for an affine cipher is an ordered pair of integers from the set {0,...,n 1}, where n is the size of the character set being used(Here it is the alphabets so range is from 0 to 25).

A→0, B→1, C→2,..., Z→ 25

The secret key for affine cipher is :

$k = (a, b) \in Z_{26} \times Z_{26}$
Encryption: $e(x, k) = (a \cdot x + b)$ mod 26
Decryption: $d(c, k) = ((c - b) \cdot a^{-1})$ mod 26
Here, a^{-1} is multiplicative inverse of a modulo m.
We will be able to decrypt a message only if we are able to find a^{-1}.

5.4.1 Multiplicative Inverse

The multiplicative inverse of an integer x under modulo m is an integer x^{-1} such that:

$$x \cdot x^{-1} \equiv 1 \text{ mod m}$$

The multiplicative inverse of x under modulo m exists iff gcd(x, m) = 1. Let y be the multiplicative inverse of x modulo m. Hence,

$$x \cdot y \equiv 1 \text{ mod m}$$
$$\Rightarrow m \text{ divides } ((x \cdot y) - 1)$$
$$\Rightarrow \exists \text{ t}\in\text{Z such that } (x \cdot y) - 1 = t \cdot m$$
$$\Rightarrow 1 = t \cdot m + x \cdot y$$

The Bezout's Identity states that there always exists integers a and b such that:

$$gcd(x, y) = a \cdot x + b \cdot y$$

The integers a and b can be found using Extended Euclidean Algorithm.
Equation $1 = t \cdot m + x \cdot y$ can be written as:

$$gcd(x, m) = 1 = t \cdot m + x \cdot y$$

Therefore, t and y are the integers that can be found using Extended Euclidean Algorithm, of which y will be the multiplicative inverse of x under modulo m.

5.4.2 Euler's Totient Function

The number of numbers lesser than n such that they are relatively prime to n (or their gcd with n is 1) can be found using Euler's Totient Function. It is denoted by $\phi(n)$. The function is defined in table 1.

n	$\phi(n)$
n is prime	n - 1
$n = p \cdot q$, p and q are primes	$(p - 1) \cdot (q - 1)$

Table 1: Euler's Totient Function.

5.4.3 Number of Keys for Affine Cipher

As we have seen above, decryption of Affine encryption is possible only if multiplicative inverse of a mod 26 exists where $a \in Z_{26}$. Also, from Euler's Totient Function:

$$\phi(26) = (2 - 1) \cdot (13 - 1) = 12$$

since $26 = 2 \cdot 13$, and 2 and 13 are prime.
Therefore, possible values of a in key are 12 out of 26 and 26 possible values of b. Hence, there are a total of $12 \cdot 26 = 312$ keys possible for Affine Cipher.

5.5 Playfair Cipher

It is a multi-letter encryption technique in which pairs of letters are encrypted instead of single letters.
Encryption :
We take a 5 × 5 matrix. Each of the 25 alphabets must be unique and one letter of the alphabet (usually J) is omitted from the table as we need only 25 alphabets instead of 26. If the plaintext contains J, then it is replaced by I. Now let us see how to generate this key table using the secret key.
In a key table, the first characters (going left to right) in the table is the phrase, excluding the duplicate letters. The rest of the table will be filled with the remaining letters of the alphabet, in natural order.
If there is an odd number of letters, a X is added to the last letter.
Now let us generate the key table for the given example.
Example :
Secret Key : PLAYFAIR EXAMPLE

$$\begin{bmatrix} P & L & A & Y & F \\ I & R & E & X & M \\ B & C & D & G & H \\ K & N & O & Q & S \\ T & U & V & W & Z \end{bmatrix}$$

Process

- If both the letters are in the same column, take the letter below each one (going back to the top if at the bottom)
- If both letters are in the same row, take the letter to the right of each one (going back to the left if at the farthest right)
- If neither of the preceding two rules are true, form a rectangle with the two letters and take the letters on the horizontal opposite corner of the rectangle.

We use the above rules to get the cipher text.
Plain text : HIDE ⇒ HI DE
Cipher text : BM OD ⇒ BMOD
Plain text : SACHIN ⇒ SA CH IN
Cipher text : OF DB RK ⇒ OFDBRK