[CS304] Introduction to Cryptography and Network Security

Course Instructor: Dr. Dibyendu Roy
Scribed by: Archit Agarwal (202051213)

Winter 2022-2023
Lecture 1 and 2 (Week 1)

1 Introduction

- **Cryptography**
  The art or science of encompassing the principles and methods of transforming an intelligible message into one that is unintelligible and then re-transforming that message back into its original form is known as Cryptography. This is the part where we develop algorithms for security. It involves two important information, one is the encryption/decryption algorithms and the other is the security key.

- **Cryptanalysis**
  Cryptanalysis is the process of studying cryptographic systems to look for weaknesses or leaks of information. This is the part where we try to 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). For Example:

  $$\text{ATM1} \rightarrow \text{PIN1} + \text{x} = \text{y1}$$
  $$\text{ATM2} \rightarrow \text{PIN2} + \text{x} = \text{y2}$$

  In above example, PIN1 or PIN2 is the actual PIN (plain text), x is the secret key and y1 is the cipher text. Encryption and Decryption function are always public, the only hidden thing is secret key.
  Let us say the encryption technique used is adding a certain integer (the secret key x) to the actual pin to get cipher text y1. We can write y1 on our ATM Card and when we want to use it, we can simply subtract x from y to get the actual pin. We chose addition/subtraction for the sake of example. One can choose some complex algorithm to do the same.

- **Encryption:** Converting intelligent(readable) text into unintelligent(unreadable) text

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

- **Decryption:** Converting unintelligent(unreadable) text into intelligent(readable) text

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

  Here, P is the plain text, C is the cipher text, E and D are encryption and decryption algorithms respectively and K is the secret key (can be same or different).

2 Types of Cryptography

1. **Symmetric/Private Key Cryptography:** It has one secret key for both encryption and decryption functions. Since the key for both encryption and decryption is same, no one else should know about the key other than the sender and the receiver.

2. **Asymmetric/Public Key Cryptography:** It has two different keys for encryption and decryption(public key and secret key). The keys are related but are different. The public key is known to the world while the secret key is known to the user only. The sender encrypts the message using receiver's public key and the receiver is able to decrypt the message using his/her secret key.

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).

4 Function

A function f: A $\rightarrow$ B is a relation from the elements of set A to the elements of set B iff(if and only if) a,b $\in$ A and a = b, then f(a) = f(b). That is, no element in set A is mapped to multiple elements in set B.

- **One-to-One/Injective Function:** A function is an injection iff each element in the domain is mapped to a distinct element in the co-domain.

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

- **Onto/Surjective function:** A function is a surjection iff each element in its co-domain is mapped to some element in the domain.

$$f : A \rightarrow B, \text{ then } \forall\ b \in B\ \exists\ a \in A \text{ such that } f(a) = b$$

- **Bijective Function :** A function is a bijection iff it is both one-one(injection) and onto(surjection).

- **Permutation:** Let π be a permutation on a set S, then $\pi : S \to S$ is a bijection from S to S. It can be defined as an ordering of the elements of a set being mapped to a different ordering of the elements of the same set.

$$\pi : \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$$

- **One-Way Function:** A function is called a one-way function if given x ∈ X, it is easy to compute f(x) but given f(x), it is hard to find x.
  For example: Finding product of two very large primes p and q is easy, but given p · q, it is difficult to find two primes that have a product equal to p · q.

- **Substitution Box:** It is a mapping from set A to set B such that the $|B| \leq |A|$.

5 Classical Ciphering Techniques and Ciphers

5.1 Caesar Cipher

This cipher is named after Julius Caesar. It relies on shifting the letters of a message by an agreed number (the key) which is equal to 3.
The set of English alphabets corresponds to the integers from 0 to 25 i.e. A corresponds to 0, B to 1 and Z to 25.
Encryption: E(x, 3) = (x + 3) mod 26
Decryption: D(c, 3) = (c + 26 - 3) mod 26
Example:

Plain Text: INTERNET
Secret Key (e): 3
Cipher Text: LQWHUQHW

I corresponds to 8, and (8 + 3) mod 26 = 11, which corresponds to L. Each character will be encrypted in a similar way.
During decryption, L corresponds to 11, (11 + 26 - 3) mod 26 = 8, which corresponds to I.

5.2 Transposition Cipher

The transposition technique converts the plain text to cipher text by performing permutations on the plain text. Since, it is just a permutation of the plain text characters, other new characters are not introduced in the cipher text.

$M = m_1 m_2 ... m_t$ (plaintext)
e: permutation on t elements 1, 2...., t (secret key)

Encryption: $C = m_{e(1)} m_{e(2)} .... m_{e(t)} = c_1 c_2 .... c_t$
Decryption: $M = c_{e^{-1}(1)} c_{e^{-1}(2)} .... c_{e^{-1}(t)}$
Example:

Plain Text: CAESAR
Secret Key (e): 641352
Cipher Text: RSCEAA

The secret key mentions that the character at the position mentioned at i^{th} character of secret key should be moved to the i^{th} position to generate cipher text.

Cipher Text: RSCEAA
Secret Key (e^{-1}): 364251
Plain Text: CAESAR

The decryption can be done using the same key (the decryption key is generated from encryption key only), hence, it is a symmetric cryptographic technique.

5.3 Substitution Cipher

The Substitution Cipher converts plain text into cipher text by substituting the letters by other letters or symbols. Since, the letters are substituted, new characters or symbols may appear in the cipher text. The secret key involved is a substitution from set of alphabets to itself.

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

Examples of substitution cipher includes Caesar Cipher, Playfair Cipher, Affine Cipher, Hill Cipher etc.

5.4 Affine Cipher

Let **A** be the set of alphatets and Z_{26} be the set of integers from 0 to 25 (both inclusive). The secret key for the Affine Cipher is given below:

$$k = (a, b) \in Z_{26} \times Z_{26}$$

Encryption: $e(x, k) = (a \cdot x + b) \bmod 26$
Decryption: $d(c, k) = ((c - b) \cdot a^{-1}) \bmod 26$
where k = (a, b) is the key, x is plain text, c is cipher text and $a^{-1} \in Z_{26}$ is multiplicative inverse of a modulo 26. 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:

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

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

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

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.

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 greatest common divisor 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.

5.4.3 Number of Keys for Affine Cipher

As we have seen, 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

Playfair Cipher uses a 5 × 5 matrix formed using the secret key for encryption and decryption.
Encryption: The following rules are followed for encryption:

1. Create the 5 × 5 matrix using secret key.Rules for creating the matrix are mentioned below:
   - Characters I and J are considered as same.
   - Fill the key characters row-wise in the matrix. If a character has already appeared, skip it.
   - Fill the remaining alphabets in lexicographic order.
2. Break the message (plain text) into groups of 2 characters.
3. Add fillers if a group has same characters or if it has only one character.
   - If length of message is odd, add X at the end of message.

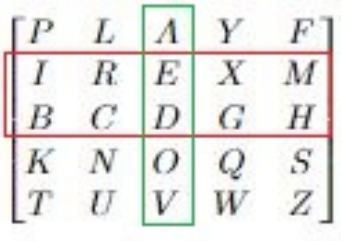

Figure 1: The matrix after highlighting the boxes for plain text HIDE.

4. For each group, find the characters in the matrix. Do the following according to the position of these characters:
   - If both characters are in the same row, use the next right character as cipher text. If the plain text character is the last element of that row, take the first character of that row as cipher text.
   - If both characters are in the same column, use the next down character as cipher text. If the plain text character is the last element of that column, take the first character of that column as cipher text.
   - If the characters are in different rows and columns, form a rectangle with these two characters at corners. Now, use the other row corner as the cipher text for both characters.

Example 1:

Secret Key: PLAYFAIR EXAMPLE
Plain Text: HIDE

The matrix formed using encryption rules will be:

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

Now, breaking the plain text into groups of 2 will give us:

Plain Text: HI DE

For the first group, the characters H and I form a rectangle shown by red colour at the top of the image. Hence, the corners will be swapped.

Plain Text: HI DE
Cipher Text: BM OD

For the second group, the characters D and E are in the same column. Hence, the next down character will be the cipher text. **Example 2:**

Secret Key: PLAYFAIR EXAMPLE
Plain Text: SACHIN

Now, breaking the plain text into groups of 2 will give us:

Plain Text: SA CH IN
Cipher Text: OF DB RK $\Rightarrow$ OFDBRK

The matrix after highlighting the boxes is given in Figure 2.

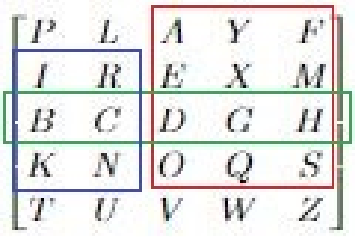

Figure 2: The matrix after highlighting the boxes for plain text SACHIN.

6 Mathematics Recall

6.1 Extended Euclidean Algorithm

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. Let us first compute GCD of x = 3 and y = 17 using Euclid's Division Algorithm.

$$17 = 3 \cdot 5 + 2 \text{ (Eq.1)}$$
$$3 = 2 \cdot 1 + 1 \text{ (Eq.2)}$$
$$2 = 1 \cdot 2 + 0 \text{ (Eq.3)}$$

Hence, GCD(3, 17) = 1. Now, going in reverse direction of this will lead us to the values of a and b.

$$1 = 1 \cdot 3 - 1 \cdot 2 \text{ (from Eq.2)}$$
$$1 = 1 \cdot 3 - 1 \cdot (1 \cdot 17 - 5 \cdot 3) \text{ (from Eq.1)}$$
$$1 = 6 \cdot 3 - 1 \cdot 17 \text{ (from Eq.1)}$$

Hence, a = 6 and b = -1.