[CS304] Introduction to Cryptography and Network Security

Course Instructor: Dr. Dibyendu Roy
Scribed by: Aniruddh Modi (202151022)

Winter 2023-2024
Lecture 1 2 (Week 1)

1 Lecture 1

1.1 Introduction to the course

- Cryptology is the study of creating and solving the codes while Cryptography is the art of just creating them.
- Cryptanalysis is the process of finding weakness in the cryptographic algorithms and deciphering the cipher text without knowing the encryption key.
- NIST standardizes cryptographic algorithms
- An encrypter function E takes in input a *plain text* and an encryption key and outputs the *cipher text*.
$$E(P, K) = C$$
- A decrypter function D taken in input a *cypher text* and the encryption key and outputs the original *plain text*.
$$D(C, K) = P$$
- A one way function is a function for which, encryption is a very fast process but decrypting the encrypted value without the key will require the user to traverse the whole range space of the function.

1.2 Symmetric Key and Public Private Key

Public Private Key	**Symmetric Key**
It has a pair of key (one public key and other private).	It has a single key which is private.
Public key is for encryption and private key is for decryption.	Single key can both encrypt and decrypt.
$E(P, K_{\text{public}}) = C$	$E(P, K) = C$
$D(C, K_{\text{private}}) = P$	$D(C, K) = P$

1.3 Features of Cryptography

- **Confidentiality :** It means information is not disclosed to unauthorized individuals, entities and processes.
- **Integrity :** It means the data is accurate and complete. No one can edit or tamper with the data in any unauthorized way.
- **Authentication :** It means that we can verify the user, that is, we can know that the information reaching to us is from a trusted source.
- **Non repudiation :** It means no one can deny receiving or sending a message or a transaction.

1.4 Ceaser Cipher

1.4.1 Encryption Algorithm

Suppose we have a plaintext P. First, we will map each character to a number (A to 0, B to 1, etc.). To encrypt the text, we will take an encryption key K, and for each character C_p in P, we will add K to its mapping and take modulo 26:

$$E(C_p, K) = (C_p + K) \mod 26$$

1.4.2 Decryption Algorithm

To decrypt the ciphertext C, we will subtract the key K from each character's mapping and take modulo 26:

$$D(C, K) = (26 + C - K) \mod 26$$

2 Lecture 2

2.1 Permutation Cipher

A permutation $\pi : S \to S$ is a bijective function from set S to itself. For example, the permutation matrix

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

maps 1 to 2, 2 to 3, and 3 to 1.

The inverse permutation function π^{-1} for the above example would be

$$\pi^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

2.1.1 Encryption Algorithm

In the permutation cipher, we can represent it as a permutation function π. The encryption function involves rearranging the characters in the plaintext P according to the permutation matrix:

$$E(P, \pi) = \pi(P)$$

2.1.2 Decryption Algorithm

To decrypt the ciphertext C, we need the inverse permutation matrix π^{-1}. The decryption function involves multiplying the ciphertext C by the inverse permutation matrix:

$$D(C, \pi^{-1}) = \pi^{-1}(C)$$

The inverse permutation matrix undoes the rearrangement applied during encryption, reconstructing the original plaintext.

2.2 Substitution Cipher

In a Substitution Cipher, each character in the plaintext is replaced with another character, according to a predefined substitution rule or key. Unlike the Caesar Cipher, where characters are shifted by a fixed amount, substitution ciphers involve a more arbitrary mapping of characters.

2.2.1 Encryption Algorithm

In substitution cipher, we take a substitution key, which is a bijective mapping from a plaintext character to a cypher character. Mathematically, the encryption function can be denoted as:

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

Here, P is the plaintext, C is the ciphertext, and the substitution key defines the character mappings.

2.2.2 Decryption Algorithm

Decryption in a substitution cipher involves reversing the process. Given the ciphertext C and the substitution key, one can replace each ciphertext character with its corresponding plaintext character:

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

2.3 Affine Cipher

2.3.1 Encryption Algorithm

Just like the ceaser cipher, create a mapping for each character. Let (a, b) be our encryption key. Then, the encryption function E is given as :

$$E(x, K) = (a.x + b) \mod 26$$

2.3.2 Decryption Algorithm

To decrypt a cipher text C, we perform the following operation :

$$E(x, K) = a^{-1}(x - b) \mod 26$$

where a^{-1} is modular arithmetic inverse of a under 26. For this, a and 26 must be co-prime.

2.4 Playfair Cipher

We will take a 5×5 matrix and a phrase as an encryption key. Then we will start filling the matrix left to right while following the following rules :

- If a letter in the phrase has already occurred in the matrix, skip it.
- If all the letters in the phrase are exhausted and there are still blank entries left in the matrix, start filling from A to Z.
- While filling A to Z, skip already seen characters.
- Treat I and J as the same.

For example, if we have cipher text as $PLAYFAIREXAMPLE$, then the matrix is

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

2.4.1 Encryption Algorithm

Firsty, break the plaintext into pair of letters. If both the letters are same, or only one letter is left, add a X between them / at the end and continue. To encrypt a pair of plaintext letters in the Playfair Cipher, follow these steps:

1. If the letters are in the same row, replace them with the letters to their immediate right, wrapping around if necessary.
2. If the letters are in the same column, replace them with the letters directly below, wrapping around if necessary.
3. If the letters are not in the same row or column, form a rectangle with the two letters and replace them with the other two corners of the rectangle.

2.4.2 Decryption Algorithm

To decrypt a pair of ciphertext letters in the Playfair Cipher, follow these steps:

1. If the letters are in the same row, replace them with the letters to their immediate left, wrapping around if necessary.
2. If the letters are in the same column, replace them with the letters directly above, wrapping around if necessary.
3. If the letters are not in the same row or column, form a rectangle with the two letters and replace them with the other two corners of the rectangle.