[CS304] Introduction to Cryptography and Network Security

Course Instructor: Dr. Dibyendu Roy
Scribed by: Ambati Hari Charan (202151019)

Winter 2023-2024
Lecture (Week 1)

Cryptography

It involves the use of mathematical algorithms to encode information in such a way that only authorized individuals can decipher and understand it.

Encryption

$$\text{Plain Text} \xrightarrow{\text{Encryption Algorithm + Key}} \text{Cipher Text}$$

Decryption

$$\text{Cipher Text} \xrightarrow{\text{Decryption Algorithm + Key}} \text{Plain Text}$$

Cryptoanalysis

It is the study of analyzing and breaking secure communication systems, attempting to find weaknesses in cryptographic algorithms or implementations to gain unauthorized access to encrypted information.

Cryptology

Combining cryptography and cryptoanalysis, it is the study of the techniques used in securing communication and information, as well as the methods of breaking the security of these systems.

Types Of Cryptography:

1. **Symmetric Cryptography**: Also known as private-key cryptography, it uses the same key for both the encryption of plaintext and the decryption of ciphertext.
2. **Asymmetric Cryptography**: In asymmetric cryptography, unlike symmetric cryptography, it contains two keys: a public key and a secret key, both generated by the receiver. The sender uses the public key of the receiver and

Security Services:

- **Confidentiality**: Ensures that unauthorized individuals cannot access or understand sensitive information; it involves the protection of the data.
- **Integrity**: Ensures that data remains unchanged and unaltered during transmission or storage.

- **Authentication**: Verifies the identity of the parties involved in communication; it ensures that the sender and the receiver of the message are who they claim to be.
- **Non-Repudiation**: Prevents individuals from denying their involvement in communication or transactions.

One Way Function

it is easy to go from the input to the output, but difficult to go from the output back to the input. A function $f : X \to Y$ is considered a one-way function if:

1. It is easy to compute $f(x)$ for any x in X.
2. It is computationally difficult to find x' in X such that $f(x') = y$, where y is a given element in the codomain Y.

Substitution Box

It performs a substitution of a fixed-size block of input bits with another block of output bits. The substitution is typically based on a fixed table or a mathematical algorithm. The S-box function $S : A \to B$, where $|A| \geq |B|$.

Example:

$$S : \{1, 2, 3, 4\} \to \{1, 2, 3\}$$
$$S(1) = 3, \quad S(2) = 1, \quad S(3) = 4, \quad S(4) = 2$$

TYPES OF CIPHERS

1. **Substitution Cipher:**
   In a substitution cipher, each letter in the plaintext is replaced by another letter or symbol based on a predetermined substitution key

   Example:

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

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

   Plaintext: YAGAMI

   Encryption:

Original:	Y	A	G	A	M	I
Encrypted:	W	Y	E	Y	K	G

   Decryption:

Encrypted:	W	Y	E	Y	K	G
Decrypted:	Y	A	G	A	M	I

2. **Transportation Cipher:**

   - A transposition cipher is a method of encryption where the positions of characters in the plaintext are rearranged based on a specific permutation.
   - The rearranged characters form the ciphertext, and the process can be reversed during decryption using the inverse of the permutation to recover the original plaintext.

   Plaintext: "YAGAMI"

   Key (Permutation Order): "312546"

   Encryption:

$$\begin{array}{cccccc} 1 & 2 & 3 & 4 & 5 & 6 \\ \hline Y & A & G & A & M & I \end{array} \rightarrow \text{Encrypted message: "AGYMAI"}$$

   Decryption:

$$\begin{array}{cccccc} 1 & 2 & 3 & 4 & 5 & 6 \\ \hline A & G & Y & M & A & I \end{array} \rightarrow \text{Decrypted message: "YAGAMI"}$$

3. **Caesar Cipher**:

   - **A** substitution cipher where each letter in the plaintext is shifted a certain number of places down or up the alphabet.
   - **T**he shift value is the key used for both encryption and decryption.
   - **Encryption Formula:**
$$E(x) = (x + k) \mod 26$$
   - **Decryption Formula:**
$$D(x) = (x - k) \mod 26$$

   Example: Encrypting "Yagami" with a shift of 3

Encrypting:

$$\begin{aligned} Y &\rightarrow (24 + 3) \mod 26 = 1 \rightarrow A \\ A &\rightarrow (0 + 3) \mod 26 = 3 \rightarrow D \\ G &\rightarrow (6 + 3) \mod 26 = 9 \rightarrow J \\ A &\rightarrow (0 + 3) \mod 26 = 3 \rightarrow D \\ M &\rightarrow (12 + 3) \mod 26 = 15 \rightarrow P \\ I &\rightarrow (8 + 3) \mod 26 = 11 \rightarrow L \end{aligned}$$

Encrypted result: DJDPLA

4. **Affine Cipher**:

   Encryption Formula:
$$E(x) = (ax + b) \mod m$$

   where:

- x: Position of the letter in the alphabet (A=0, B=1, ..., Z=25),
- a, b: Key values chosen such that a and m are coprime.

Decryption Formula:

$$D(x) = a^{-1}(x - b) \mod m$$

where:

- a^{-1}: Modular multiplicative inverse of a modulo m.

Example: Encrypting and Decrypting "Yagami" with $a = 5, b = 8$:

$$\begin{aligned}
\text{Original alphabet:} \quad & ABCDEFGHIJKLMNOPQRSTUVWXYZ \\
\text{Encrypting "Yagami":} & \\
Y \to (5 \cdot 24 + 8) \mod 26 &= 20 \to T \\
a \to (5 \cdot 0 + 8) \mod 26 &= 8 \to I \\
g \to (5 \cdot 6 + 8) \mod 26 &= 10 \to K \\
a \to (5 \cdot 0 + 8) \mod 26 &= 8 \to I \\
m \to (5 \cdot 12 + 8) \mod 26 &= 10 \to K \\
i \to (5 \cdot 8 + 8) \mod 26 &= 12 \to M \\
\text{Encrypted result:} \quad & \text{TIKIKM} \\
\text{Decrypting "TIKIKM":} & \\
T \to 21(20 - 8) \mod 26 &= 24 \to Y \\
I \to 21(8 - 8) \mod 26 &= 0 \to A \\
K \to 21(10 - 8) \mod 26 &= 6 \to G \\
I \to 21(8 - 8) \mod 26 &= 0 \to A \\
K \to 21(10 - 8) \mod 26 &= 12 \to M \\
M \to 21(12 - 8) \mod 26 &= 8 \to I \\
\text{Decrypted result:} \quad & \text{YAGAMI}
\end{aligned}$$

5. **PlayFair Cipher**: **Key Table Construction:**

   - A key is chosen (e.g., a keyword), and a key table is constructed by placing the unique letters of the key in a matrix.
   - The remaining letters of the alphabet are then filled in, avoiding duplicates.

   Encryption:

   - The message is divided into pairs of letters (digraphs).
   - For each digraph:
     - If the letters are in the same row, they are replaced with the letters to their immediate right, wrapping around to the beginning if necessary.
     - If the letters are in the same column, they are replaced with the letters immediately below, wrapping around to the top if necessary.

– If the letters form a rectangle, each letter is replaced with the letter in the same row but in the other corner of the rectangle.

Decryption:

- The process is reversed for decryption, with letters replaced by those in the opposite direction.

Example: "YAGAMI"

Key Table:

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

Encryption

```
Y | A
--|--
G | A
--|--
M | I
```

Encrypting pairs:

- "YA" becomes "VD"
- "GA" becomes "LC"
- "MI" becomes "KG"

Encrypted Result: "VD LC KG"