# Network Information Security

# **Assignment 1**

# Roll No. **2109805**

Name: Jagrut Gala
Class: SYBSc CS
Roll No: 2109805
Subject: Network Information Security

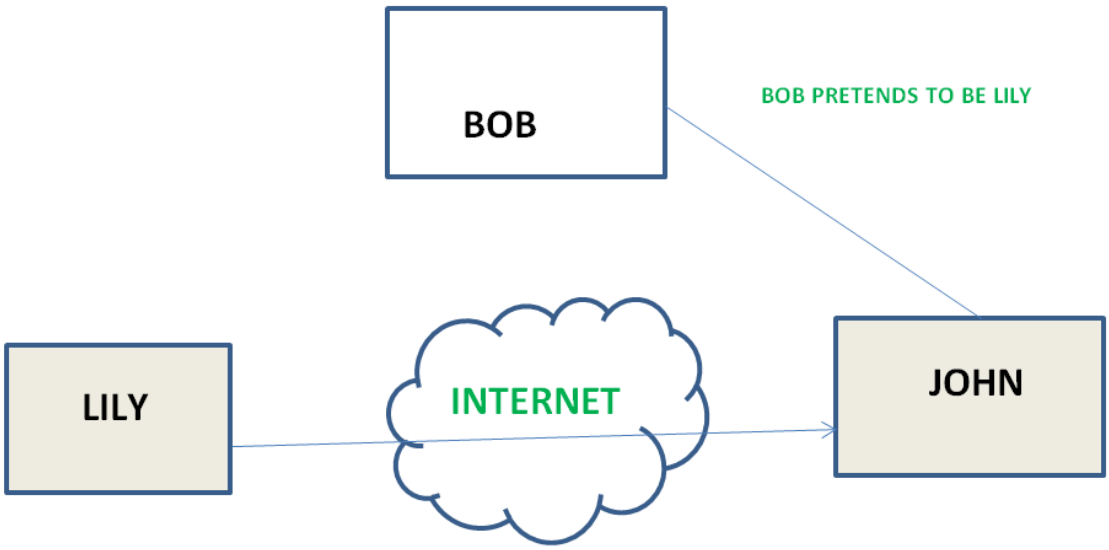
**Q1) Explain active attacks with the help of an example.**

**Ans:**

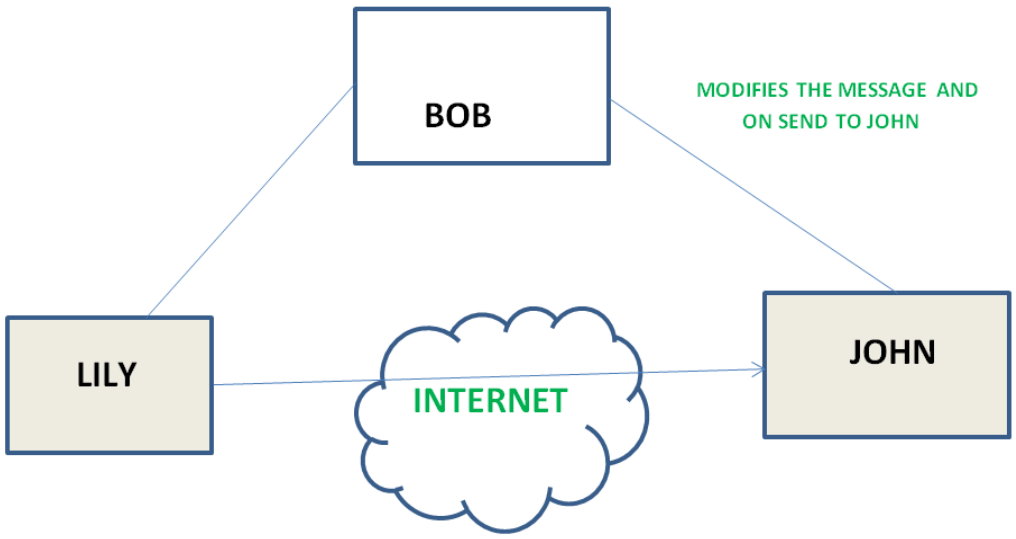
The active attacks are based on the modification of the original. Message in some particular manner or on the creation of a false message. These attacks cannot be prevented easily. However, efforts can be taken to detect them and recover from them.

These attacks can be in the form of:

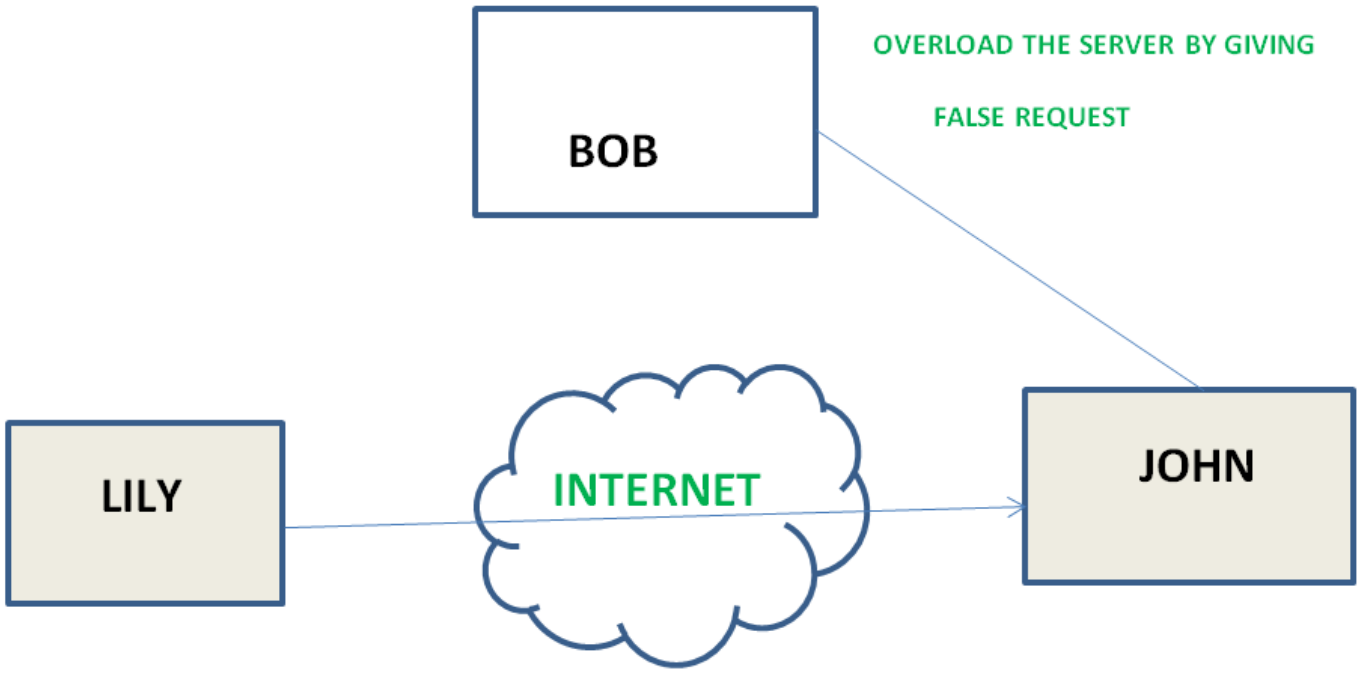
- Masquerade: A masquerade attack is an attack that uses a fake identity, such as a network identity, to gain unauthorized access to personal computer information through legitimate access identification. If an authorization. The process is not fully protected, it can become extremely vulnerable to a masquerade attack. For Example, Bob performs a masquerade attack on Jhon by spoofing Lily's identity and gaining access to personal conversations between Lily and Jhon.




- Relay: A replay attack is also known as a playback attack. It is a form of network attack in which valid data transmission is maliciously or fraudulently repeated or delayed. This is carried out either by the originator or by an adversary who intercepts the data and retransmits it. For example, a thief could capture the radio signal from your vehicle's key fob and relay it to an accomplice who could use it to open your car door.
- Modification: A modification attack means that some portion of a message is altered or that message is delayed or reordered to produce an unauthorized effect. For example, a message meaning "Allow JOHN to read confidential file X" is modified as "Allow Smith to read confidential file X".




- Denial of Service: A denial of service prevents normal use of communication facilities. This attack may have a specific target. For example, an entity may suppress all messages directed to a particular destination. Another form of service denial is the disruption of an entire network either by disabling the network or by overloading it with messages to degrade performance. For example, Lily wants to send a request to Jhon and is expecting a response soon but Jhon is bombarded with overwhelming amounts of requests by Bob that it cannot respond to Lily's request.



**Q2) Why do we need network security? Explain the advantages of network security.**
**Ans:**

Network security is any system, device, or action designed to protect the safety and reliability of a network and its data.

Like a fence around private land or a lock on a door, network security manages access to a network by stopping a variety of threats from entering and spreading through a system.

Cybersecurity aims to protect Internet-connected systems and networks from initial attacks like a hacker or a virus.

Network security is focused on protecting files, documents, and information from those types of attacks. Most commonly, network security starts with authentication in the form of a username and password, but it can also employ other tools like firewalls, anti-virus programs, and virtual private networks (VPNs) to protect the network's information.

The Advantages of Network Security are:

- Builds trust: Security for large systems translates to security for everyone. Network security boosts client and consumer confidence, and it protects your business from the reputational and legal fallout of a security breach.
- Mitigates risk: The right network security solution will help your business stay compliant with business and government regulations, and it will minimize the business and financial impact of a breach if it does occur.
- Protects proprietary information: Your clients and customers rely on you to protect their sensitive information. Your business relies on that same protection, too. Network security ensures the protection of information and data shared across the network.
- Enables a more modern workplace: From allowing employees to work securely from any location using VPN to encouraging collaboration with secure network access, network security provides options to enable the future of work. Effective network security also provides many levels of security to scale with your growing business

**Q3) Explain Hill cipher with the help of an example.**

**Ans:**

The Hill cipher is a polygraphic substitution cipher built on concepts from Linear Algebra. The Hill cipher makes use of modulo arithmetic, matrix multiplication, and matrix inverses; hence, it is a more mathematical cipher than others. The Hill cipher is also a block cipher, so, theoretically, it can work on arbitrary-sized blocks. For example, we encrypt the text 'CODE' and later decrypt it.

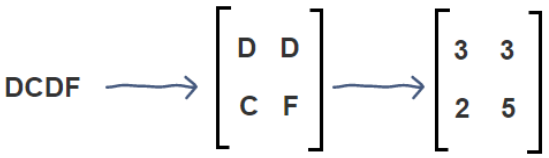
Here we will use a straightforward substitution scheme where the letter A is mapped to 0, B is mapped to 1, etc. to stick to a 2x2 key matrix. The complexity of the Hill cipher increases with the size of the key matrix.

Encryption

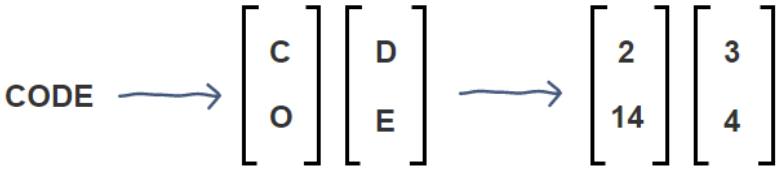
- Encrypting with the Hill cipher is built on the following operation:

$$E(K, P) = (K*P) \bmod 26$$

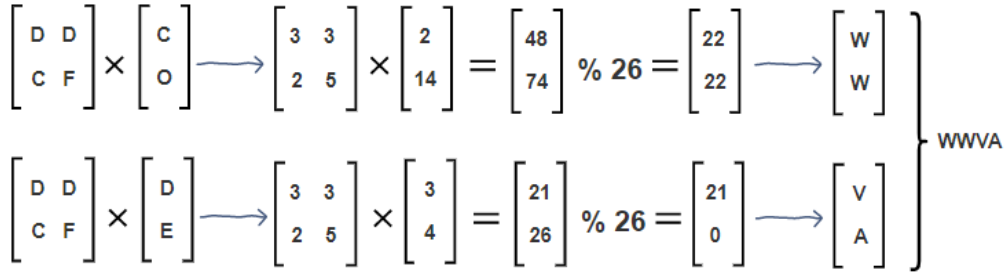
- Where K is our key matrix and P is the plaintext in vector form. Matrix multiplying these two terms produces the encrypted ciphertext. Let's do so step by step:
- Pick a keyword to encrypt your plaintext message. Let's work with the random keyword "DCDF". Convert this keyword to matrix form using your substitution scheme to convert it to a numerical 2x2 key matrix.




- Next, we will convert our plaintext message to vector form. Since our key matrix is 2x2, the vector needs to be 2x1 for matrix multiplication to be possible. In our case, our message is four letters long so we can split it into blocks of two and then substitute to get our plaintext vectors.



- Now, we can matrix multiply the key matrix with each 2x1 plaintext vector, take the moduli of the resulting 2x1 vectors by 26, and concatenate the results to get “WWVA”, the final ciphertext.

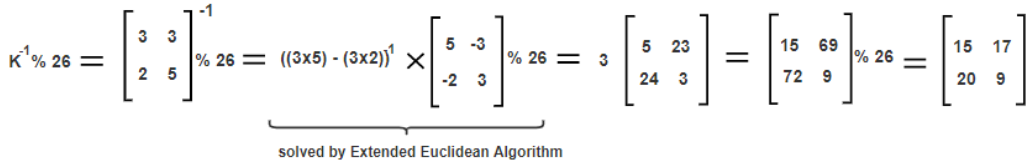



Decryption

- Decrypting with the Hill cipher is built on the following operation:

$$D(K, C) = (K^{-1} * C) \bmod 26$$

- Where K is our key matrix and C is the ciphertext in vector form. Matrix multiplying the inverse of the key matrix with the ciphertext produces the decrypted plaintext. Let's do this step by step with our ciphertext, "WWVA":
  - First, we calculate the inverse of the key matrix. In doing so, we must keep the result between 0-25 using modulo 26. For this reason, the Extended Euclidean algorithm is used to find the modular multiplicative inverse of the key matrix determinant.




- Next, we will multiply 2x1 blocks of the ciphertext with the inverse of the key matrix to get our original plaintext message, “CODE,” back.

$$\begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix} \times \begin{bmatrix} 22 \\ 22 \end{bmatrix} = \begin{bmatrix} 704 \\ 638 \end{bmatrix} \% 26 = \begin{bmatrix} 2 \\ 14 \end{bmatrix} \longrightarrow \begin{bmatrix} C \\ O \end{bmatrix}$$

$$\begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix} \times \begin{bmatrix} 21 \\ 0 \end{bmatrix} = \begin{bmatrix} 315 \\ 420 \end{bmatrix} \% 26 = \begin{bmatrix} 3 \\ 4 \end{bmatrix} \longrightarrow \begin{bmatrix} D \\ E \end{bmatrix}$$

} CODE

**Q4) Differentiate between symmetric and asymmetric key cryptography.**
**Ans:**

| Symmetric Key Encryption | Asymmetric Key Encryption |
|---|---|
| It only requires a single key for both encryption and decryption. | It requires two keys one to encrypt and the other one to decrypt. |
| The size of ciphertext is the same or smaller than the original plain text. | The size of ciphertext is the same or larger than the original plain text. |
| The encryption process is very fast. | The encryption process is slow. |
| It is used when a large amount of data is required to transfer. | It is used to transfer small amounts of data. |
| It only provides confidentiality. | It provides confidentiality, authenticity, and non-repudiation. |
| Examples: 3DES, AES, DES, and RC4 | Examples: Diffie-Hellman, ECC, El Gamal, DSA, and RSA |
| In symmetric key encryption, resource utilization is low as compared to asymmetric key encryption. | In asymmetric key encryption, resource utilization is high. |

**Q5) Explain polyalphabetic cipher with the help of an example.**

**Ans:**

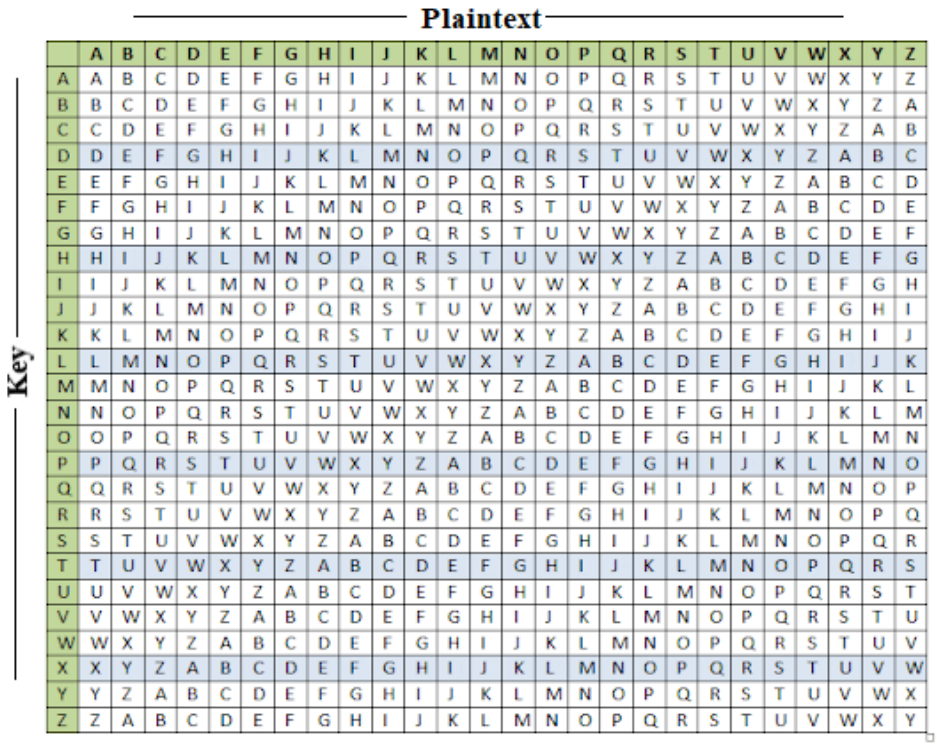
A polyalphabetic cipher is any cipher based on substitution, using multiple substitution alphabets. The Vigenère cipher is a very common example of a polyalphabetic cipher, though it is a simplified special case.

The relationship between a character in the plain text and the characters in the ciphertext is one-to-many. Each alphabetic character of plain text can be mapped onto 'm' alphabetic characters of a ciphertext.

A stream cipher is a polyalphabetic cipher if the value of the key does depend on the position of the plain text character in the plain text stream. It includes autokey, Playfair, Vigenere, Hill, one-time pad, rotor, and Enigma cipher. Polyalphabetic ciphers are much stronger than Monoalphabetic ciphers.

Example:

When the vigenère table is given:




| Plain | S | O | M | A | I | Y | A |
|---|---|---|---|---|---|---|---|
| Key | B | E | S | T | B | E | T |
| Cipher | T | S | E | T | J | C | S |