NS Practical questions

1. In DES input, key length \_\_\_ bits and plaintext length \_\_\_\_ bits.

**(a) 56 bit key length, 64 bit plaintext**

(b) 56 bit key length, 120 bit plaintext

(c) 64 bit key length, 120 bit plaintext

(d) 64 bit key length, 64 bit plaintext

1. DES stands for \_\_\_\_\_\_\_\_\_ and AES stands for \_\_\_\_\_\_\_\_\_\_

(a) Data Encryption software, Advanced Encryption Software

**(b) Data Encryption Standard, Advanced Encryption Standard**

(c) Data Encryption System, Advanced Encryption System

(d) None

1. DES has an initial and final permutation block and \_\_\_\_ rounds

(a) 14

**(b) 16**

(c) 8

(d) 12

1. In DES the length of each round key?

(a) 16 bit

(b) 32 bit

(c) 54 bit

**(d) 48 bit**

1. Explain the DES algorithm? draw the block diagram
2. Explain the logic of DES algorithm.
3. **Explain RSA algorithm**

* Select two large prime numbers, p and **q**.
* Multiply these numbers to find **n = p x q,** where **n** is called the modulus for encryption and decryption.
* Choose a number **e** less than **n**, such that n is relatively prime to **(p - 1) x (q -1).** It means that **e** and **(p - 1) x (q - 1)** have no common factor except 1. Choose "e" such that 1<e < φ (n), e is prime to φ (n),  
  **gcd (e,d(n)) =1**
* If **n = p x q,** then the public key is <e, n>. A plaintext message **m** is encrypted using public key <e, n>. To find ciphertext from the plain text following formula is used to get ciphertext C.  
  **C=me mod n**  
  Here**, m** must be less than **n**. A larger message (>n) is treated as a concatenation of messages, each of which is encrypted separately.
* To determine the private key, we use the following formula to calculate the d such that:  
  **De mod {(p - 1) x (q - 1)} = 1**  
  **Or**  
  **De mod φ (n) = 1**
* The private key is <d, n>. A ciphertext message **c** is decrypted using private key <d, n>. To calculate plain text **m** from the ciphertext c following formula is used to get plain text m.  
  **m = cd mod n**

1. How many keys are using in RSA algorithm?
2. Explain the working of keys in RSA algorithm
3. Explain Caesar Cipher technique with example.
4. Explain Caesar Cipher program.
5. **Give the difference between symmetric Encryption and Asymmetric Encryption.**

**Mention the difference between symmetric and asymmetric encryption**.

|  |  |  |
| --- | --- | --- |
| Differentiator | Symmetric Encryption | Asymmetric Encryption |
| Encryption Key | Only one key to encrypt and decrypt a message | Two different keys (public and private keys) to encrypt and decrypt the message |
| Speed of Execution | Encryption is faster and simple | Encryption is slower and complicated |
| Algorithms | RC4, AES, DES, and 3DES | RSA, Diffie-Hellman, and ECC |
| Usage | For the transmission of large chunks of data | For smaller transmission to establish a secure connection prior to the actual data transfer |

1. **What are different type of cryptography**

**Types of Cryptography**

Cryptography can be broken down into three different types:

* Secret Key Cryptography
* Public Key Cryptography
* Hash Functions

1. **What are the benefits of a firewall?**

Ans. The benefits of firewalls are:

* Monitors network traffic
* Enhances Privacy
* Stops Spyware
* Prevents hacking
* Inhibits virus attacks

1. **What does VPN stand for?**

Ans. VPN stands for the Virtual Private Network. It creates a secure network connection over a public network like the internet.

1. **What is the use of a VPN?**

Ans. A VPN or virtual private network is an encrypted connection over the Internet from a device to a network. It provides online privacy and anonymity by creating a private network from a public internet connection. It prevents unauthorized people from spying on the traffic and allows the user to conduct work remotely.

### What is cryptography?-----------[Cryptography](https://intellipaat.com/blog/what-is-cryptography/" \t "_blank) aids to secure information from third parties who are called adversaries. It allows only the sender and the recipient to access the data securely.

1. **What is a firewall? Mention its uses.**

A firewall is a [network security](https://intellipaat.com/blog/what-is-network-security/) device/system, which blocks malicious traffic such as hackers, worms, malware, and viruses to maintain [data privacy](https://intellipaat.com/blog/what-is-data-privacy/).

Uses:

It monitors the incoming and outgoing network traffic. It permits or allows only data packets that agree to the set of security rules.

It acts as a barrier between the internal network and the incoming traffic from external sources like the Internet.

### Define network security?

**Ans:**A group of technologies known as network security guards against a wide range of potential dangers from entering or spreading within a network, preserving the usefulness and integrity of a company's infrastructure.

### In terms of network security, what is a firewall?

**Ans:**An example of a network security tool is a firewall, which monitors incoming and outgoing network traffic and decides which traffic to allow or block in accordance with a set of security rules. Firewalls have been the primary line of defense for network security for more than 25 years.

### What is the purpose of network security?

**Ans:**Having a secure network is essential for both private and professional networks. Most homes with high-speed internet have one or possibly more wireless routers, which, if they are not sufficiently protected, might be targets of attacks. A robust network security system can reduce the risk of sabotage, data loss, and theft.

### Where is the use of network security?

**Ans:**Network security includes a range of computer networks, both private and public, that are utilized in daily tasks, including carrying out transactions and facilitating interactions between enterprises, governmental organizations, and people. Networks can be private, like that inside of a business, or they might be public.

**22.What are different types on attack in network security?**

Ans: **Active attacks and Passive Attack**

**Active attacks** are a type of cybersecurity attack in which an attacker attempts to alter, destroy, or disrupt the normal operation of a system or            network. Active attacks involve the attacker taking direct action against the target system or network, and can be more dangerous than passive         attacks, which involve simply monitoring or eavesdropping on a system or network.

**Types of active attacks are as follows:**

**Masquerade**

**Modification of messages**

**Repudiation**

**Replay**

**Denial of Service**

**Passive attacks:** A Passive attack attempts to learn or make use of information from the system but does not affect system resources. Passive Attacks are in the nature of eavesdropping on or monitoring transmission. The goal of the opponent is to obtain information that is being transmitted. Passive attacks involve an attacker passively monitoring or collecting data without altering or destroying it. Examples of passive attacks include eavesdropping, where an attacker listens in on network traffic to collect sensitive information, and sniffing, where an attacker captures and analyzes data packets to steal sensitive information.

**Types of Passive attacks are as follows:**

The release of message content

Traffic analysis

**23.What is Ciphertext?**

Ciphertext is encrypted text transformed from plaintext using an encryption algorithm. Ciphertext can't be read until it has been converted into plaintext (decrypted) with a key.

**23.What is plaintext?**

In cryptography, plaintext is usually ordinary readable text before it is encrypted into ciphertext, or readable text after it is decrypted.

**24. What is Denial of Service attack?**

**Denial of Service –**

Denial of Service (DoS) is a type of cybersecurity attack that is designed to make a system or network unavailable to its intended users by overwhelming it with traffic or requests. In a DoS attack, an attacker floods a target system or network with traffic or requests in order to consume its resources, such as bandwidth, CPU cycles, or memory, and prevent legitimate users from accessing it.

**25.Explain Masquerade?**

**Masquerade –**

Masquerade is a type of cybersecurity attack in which an attacker pretends to be someone else in order to gain access to systems or data. This can involve impersonating a legitimate user or system to trick other users or systems into providing sensitive information or granting access to restricted areas.

**26.Explain Network security principle?**

**Confidentiality**

Confidentiality measures are designed to prevent unauthorized disclosure of information. The purpose of the confidentiality principle is to keep personal information private and to ensure that it is visible and accessible only to those individuals who own it or need it to perform their organizational functions.

**Integrity**

Consistency includes protection against unauthorized changes (additions, deletions, alterations, etc.) to data. The principle of integrity ensures that data is accurate and reliable and is not modified incorrectly, whether accidentally or maliciously.

**Availability**

Availability is the protection of a system’s ability to make software systems and data fully available when a user needs it (or at a specified time). The purpose of [availability is to make the technology infrastructure](https://www.imperva.com/learn/availability/high-availability/), the applications and the data available when they are needed for an organizational process or for an organization’s customers.

**Other important terms include**:

**Identification:** The act of a user professing an identity to the system, such as login ID

**Authentication:** Verification that the user’s claimed identity is valid, such as through the use of a password.

**Accountability:** Determination of the actions and behavior of a single individual within a system and holding the individual responsible for his/her actions.

**Authorization:** The privileges allocated to an individual or process that enable access to a computer resource.