**AES vs DES**

| **AES** | **DES** |
| --- | --- |
| AES stands for Advanced Encryption Standard | DES stands for Data Encryption Standard |
| Key length can be of 128-bits, 192-bits and 256-bits. | Key length is 56 bits in DES. |
| Number of rounds depends on key length : 10(128-bits), 12(192-bits) or 14(256-bits) | DES involves 16 rounds of identical operations |
| The structure is based on substitution-permutation network. | The structure is based in feistal network. |
| AES is more secure than the DES cipher and is the de facto world standard. | DES can be broken easily as it has known vulnerabilities. |
| AES can encrypt 128 bits of plaintext. | DES can encrypt 64 bits of plaintext. |

**b) FireWall Limitation**

1. Firewalls cannot protect against what has been authorized
2. It cannot stop social engineering attacks or an unauthorized user intentionally using their access for unwanted purposes
3. Firewalls cannot fix poor administrative practices or poorly designed security policies
4. It cannot stop attacks if the traffic does not pass through them
5. They are only as effective as the rules they are configured to enforce.

**c) DDOS**

A distributed denial-of-service (DDoS) attack is a malicious attempt to disrupt normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic. DDoS attacks achieve effectiveness by utilizing multiple compromised computer systems as sources of attack traffic. Exploited machines can include computers and other networked resources such as IoT devices ……. …………………………………..Yr simple ha ye normal traffic ko panga dhalta r computer aur IOT devices k sath cher char krta bsss

**d) three key objectives of computer security**

+CONFIDENTIALITY

+INTEGRITY +

AVAILABILITY

These three are the fundamental characteristics of data that must be protected.

Confidentiality means that only authorized persons can access information.

Integrity ensures that the information is correct.

Availability ensures that the data is readily available when an authorized persons wants to access it.

**Bss aeni g gl ay …… Darro ni bss dil bara kro acha hi ho ga ppr InshAllah**

**e) Computer security chalanges**

1. Computer virus

### **2. Rogue security software**

### **3. Trojan horse**

### **4. Adware and spyware**

### **5. Logic Bomb**

### **6. Spyware**

### Section C

### Q3 (b)

Diffie-Hellman is a way of generating a shared secret between two people in such a way that the secret can't be seen by observing the communication. That's an important distinction: **You're not sharing information during the key exchange, you're creating a key together.**

This is particularly useful because you can use this technique to create an encryption key with someone, and then start encrypting your traffic with that key. And even if the traffic is recorded and later analyzed, there's absolutely no way to figure out what the key was, even though the exchanges that created it may have been visible.

EXAMPLE:

The algorithm in itself is very simple. Let's assume that Alice wants to establish a shared secret with Bob.

1. Alice and Bob agree on a prime number, p, and a base, g, in advance. For our example, let's assume that p=23 and g=5.
2. Alice chooses a secret integer a whose value is 6 and computes A = g^a mod p. In this example, A has the value of 8.
3. Bob chooses a secret integer b whose value is 15 and computes B = g^b mod p. In this example, B has the value of 19.
4. Alice sends A to Bob and Bob sends B to Alice.
5. To obtain the shared secret, Alice computes s = B^a mod p. In this example, Alice obtains the value of s=2
6. To obtain the shared secret, Bob computes s = A^b mod p. In this example, Bob obtains the value of s=2.

The algorithm is secure because the values of a and b, which are required to derive s are not transmitted across the wire at all.

**Diff types of fiorewall and explain packet filtering**

1. Packet filtering firewall
2. Circuit-level gateway
3. Stateful inspection firewall
4. Application-level gateway (aka proxy firewall)
5. Next-generation firewall (NGFW)

### Packet filtering firewall

Packet filtering firewalls operate inline at junction points where devices such as routers and switches do their work. However, these firewalls don't route packets, but rather they compare each packet received to a set of established criteria -- such as the allowed IP addresses, packet type, port number and other aspects of the packet protocol headers. Packets that are flagged as troublesome are, generally speaking, unceremoniously dropped -- that is, they are not forwarded and, thus, cease to exist.

**arbitrated digital signature techniques**

Implementing an arbitrated digital signature invites a third party into the process called a "trusted arbiter." The role of the trusted arbiter is usually twofold: first this independent third party verifies the integrity of the signed message or data. Second, the trusted arbiter dates, or time-stamps, the document, verifying receipt and the passing on of the signed document to its intended final destination.

**Distiguish b/w active and apassive attack**

The major difference between active and passive attacks is that in active attacks the attacker intercepts the connection and modifies the information. Whereas, in a passive attack, the attacker intercepts the transit information with the intention of reading and analyzing the information not for altering it.

| **Active Attack** | **Active Attacks Passive Attack** |
| --- | --- |
| Attacker needs to have physical control or the media or network. | Attacker merely needs to observe the communication in the media or network. |
| It can he easily detected. | It cannot be easily detected. |
| It affects the system. | It does not affect the system. |
| It involves a modification of data. | It involves the monitoring of data. |
| Types of active attack are Masquerade, session replay, denial of service, distributed denial of service. | Types of passive attack are Release of a message, traffic analysis. |
| It does not check for loopholes or vulnerabilities. | It scans the ports and network in search of loopholes and vulnerabilities. |
| It is difficult to prevent the network from an active attack. | A passive attack can be prevented. |

**Public key cryptography**

Public key encryption, or public key cryptography, is a method of encrypting data with two different keys and making one of the keys, the public key, available for anyone to use. The other key is known as the private key. Data encrypted with the public key can only be decrypted with the private key, and data encrypted with the private key can only be decrypted with the public key. Public key encryption is also known as asymmetric encryption. It is widely used, especially for [TLS/SSL](https://www.cloudflare.com/learning/ssl/transport-layer-security-tls/), which makes [HTTPS](https://www.cloudflare.com/learning/ssl/what-is-https/)possible.

## **What is a cryptographic key?**

In cryptography, a key is a piece of information used for scrambling data so that it appears random; often it's a large number, or string of numbers and letters. When unencrypted data, also called plaintext, is put into an encryption algorithm using the key, the plaintext comes out the other side as random-looking data. However, anyone with the right key for decrypting the data can put it back into plaintext form.

For example, suppose we take a plaintext message, "hello," and encrypt it with a key\*; let's say the key is "2jd8932kd8." Encrypted with this key, our simple "hello" now reads "X5xJCSycg14=", which seems like random garbage data. However, by decrypting it with that same key, we get "hello" back.

Plaintext + key = ciphertext:

hello + 2jd8932kd8 = X5xJCSycg14=

Ciphertext + key = plaintext:

X5xJCSycg14= + 2jd8932kd8 = hello

(This is an example of symmetric encryption, in which only one key is used.)

\*Using Blowfish algorithm, CBC mode, Base64 encoding.

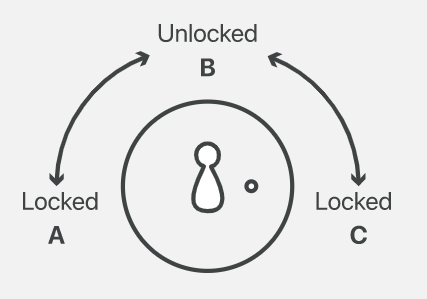
## **How does public key encryption work?**

Public key cryptography can seem complex for the uninitiated; fortunately a writer named [Panayotis Vryonis](https://medium.com/@vrypan/explaining-public-key-cryptography-to-non-geeks-f0994b3c2d5" \t "_blank) came up with an analogy that roughly goes as follows.

Imagine a trunk with a lock that two people, Bob and Alice, use to ship documents back and forth. A typical lock has only two states: locked and unlocked. Anyone with a copy of the key can unlock the trunk if it's locked, and vice versa. When Bob locks the trunk and sends it to Alice, he knows that Alice can use her copy of the key to unlock the trunk. This is essentially how what's known as symmetric cryptography works: one secret key is used for both encrypting and decrypting, and both sides of a conversation use the same key.

Now imagine, instead, that Bob makes a trunk with a special kind of lock. This lock has three states instead of two:

* A. Locked, key turned all the way to the left
* B. Unlocked, in the middle.
* C. Locked, key turned all the way to the right.



Instead of one key, two keys go with this lock:

* Key No. 1 can only turn to the left
* Key No. 2 can only turn to the right

**how block cipher works for data encryption and decryption**

A block [cipher](https://searchsecurity.techtarget.com/definition/cipher) is a method of encrypting [text](https://whatis.techtarget.com/definition/text) (to produce [ciphertext](https://whatis.techtarget.com/definition/ciphertext)) in which a cryptographic key and [algorithm](https://whatis.techtarget.com/definition/algorithm) are applied to a block of data (for example, 64 contiguous bits) at once as a group rather than to one bit at a time. The main alternative method, used much less frequently, is called the [stream cipher](https://searchsecurity.techtarget.com/definition/stream-cipher).

So that identical blocks of text do not get encrypted the same way in a message (which might make it easier to decipher the ciphertext), it is common to apply the ciphertext from the previous encrypted block to the next block in a sequence. So that identical messages encrypted on the same day do not produce identical ciphertext, an *initialization vector* derived from a *random number generator* is combined with the text in the first block and the key. This ensures that all subsequent blocks result in ciphertext that doesn't match that of the first encrypting.