3. a)

Bob is the recipient of Alice's message. The secret key belongs to both Alice and Bob. Message decryption with a shared secret key, Alice XOR her message. Message encryption is a process that involves encrypting a message before sending it Bob used his (same) secret key to XOR the message.

Example:

This is effective for 3 purposes:

• The XOR has reformed.

• Any XORed binary number is also 0.

• Any binary value, even 0 itself, is XORed.

The following are some of the benefits of using the secret keystroke:

1. XOR implementation is quite quick.

2. Everything is in order.

Disadvantages:

1. The key should be always kept secret.

2. Key exchanges with people should be done in private.

3. A key must be shared by each communication center.

Public Key Cryptography:

The key to public key encryption is two components: a private and a public component. Alice initially had to receive his public key to send a message to Bob. Bob has released his public key to anybody on his webpage since he likes to communicate with her (even if it's coded communications). Alice gets her public key, uses the message to encrypt and transmits it to Bob. Bob was able to encrypt a message using a secret code part of his key.

Advantages:

1. Only one component need be kept secret.

2. You do not have to update your public and private keys.

3. Only N public/private key pairs are required for N individuals to interact.

4. The first key does not need to be exchanged.

5. It has the capability of being used as a digital signature.

* Alice wants to send the message to the internet forum to check that anyone who sees the file has sent the message (and not by anybody else posing as him). With her secret key, Alice takes her message and encrypts it. Alice should encrypt the message encrypted on that forum using its public key.

Disadvantages:

1. Reduce the amount of calculation required to the bare minimum.

2. The length of the buttons should be increased (at least 1024 pieces these days).

3. No public key scheme has been proven to be secure.

4. It has never been subjected to comprehensive testing.

3. b)

A kind of asymmetric encryption is the RSA algorithm. The word "asymmetrical" relates to its usage of the public key and the private key. two different keys are used. All are given the public key, while a private key, as the name implies, is kept hidden.

Example of Asymmetric cryptography:

* A client (such as a browser) provides a server its public key along with data requests.
* The server encrypts the data and sends it encrypted using the client's public key.
* This data is retrieved and deleted by the client.
* Because this is inconsistency, no one other than the browser, even if the third party possesses the browser public key, may publish the details.

The concept! The RSA idea is predicated on the notion that obtaining the whole value is difficult. A public key is made up of two numbers, one of which is multiplied by two primary numbers. The secret key is likewise based on two key integers that are identical. As a result, if a high number is entered, the secret key is jeopardized. As a result, the encryption power is proportional to the key size, and increasing the key size by two or three times improves the encryption power substantially. The length of an RSA key can be 1024 or 2048 bits, but experts predict the 1024-bit keys will be cracked shortly. However, it appears to be an insurmountable task thus far.

RSA Implementation:

When utilizing the RSA technique, consider the three variables n, p and q. For 1024 bits RSA, p and q should have about 512 bits, but p and q must be less! p and q should have the same length. Select the first p and q numbers. To do this, select a random number set and check how large it is. More Rabin-Miller testing experience is needed (possible tests).e is usually chosen to be

Example:

4)

Assaults, scripts, and common ground for crypt attacks using Meet-in-the-Middle (MITM) are used to crack encryption programs using various encryption algorithms. The first reason the MITM attack cannot be employed Double DES and the attacker cannot force the Triple DES Key (168 bits).

The encryption of data regularly utilizing multiple keys is an intriguing approach when trying to improve security for blocks. Since a comprehensive search for all key combinations (light power) can take up to attempts if k-bit n times are encrypted, the most enrichment programs can be duplicated or tuple, depending on how many times the data are crucified.

MITM is a common attack that undermines the safety advantage of utilizing multiples encryption by maintaining and exploiting values during encryption and conversion to reduce encryption keys. As a result, it is considered normal time trading in the Meeting in the Middle (MITM) attack.

MITM Attack aims to find keys for various task formats (or block cyphers). The primary image is the one between the final tasks (in chip text) and the domain (plaintext), as the main image of the final tasks is like the other. For example, dual DES may be hacked using encryption functions or encrypting data with two 56-bit buttons.

Multitimensional MITM (MD-MITM) combines many MITM assaults at the same time, as mentioned above, with the meeting taking place in several places during the task.