CSE

Cryptography and Network Security

1. Define security.
Ans:

Security:
Network security consists of the provisions and policies adopted by a network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Network Security involves the authorization of access to data in a network, which is controlled by the network administrator.

The Issues are:

- Privacy issue
- Integrity issue
- Authentication issue
- Non-repudiation issue

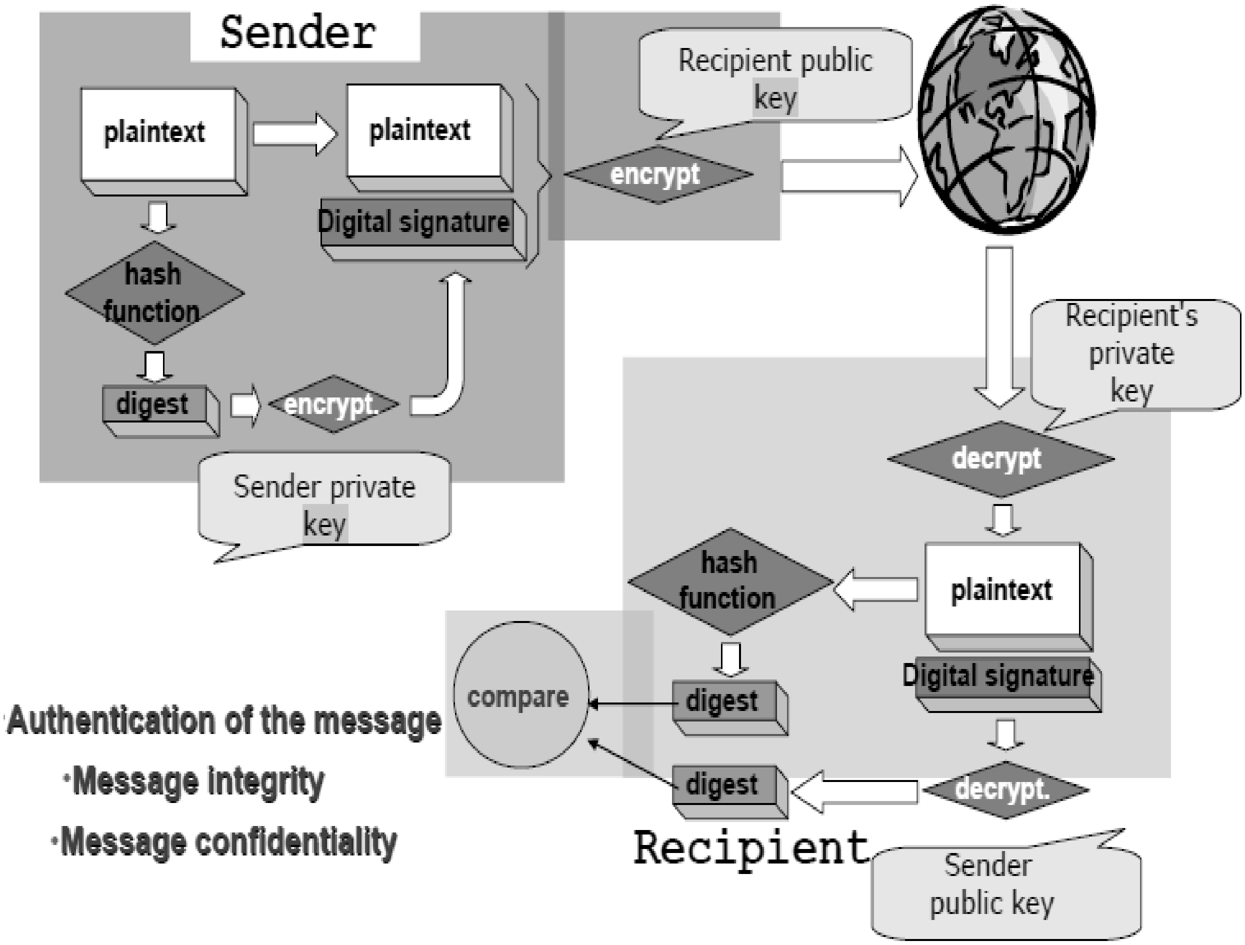
2. What is a Digital Signature? 2
Or
Write down the digital signature process of public key cryptography to ensure security over internet. 4
Ans:

Digital Signature:
A digital code (generated and authenticated by public key encryption) which is attached to an electronically transmitted message or document to verify its contents and the sender's identity.

- ✓ Developed to be used in public key cryptography.
- ✓ Solves problems of authentication and integrity.
- ✓ A digital signature ensures that plaintext was authored by someone.

Digital signature process:

- ➢ Sender uses private key to encrypt message digest, creating digital signature, Authenticating sender.
- ➢ Sender uses receiver public key to encrypt message.
- ➢ Receiver uses sender's public key to decipher digital signature, reveal message Digest.
- ➢ Receiver uses own private key to decipher original message.
- ➢ Receiver applies hash function to original message.



3. Explain with figure how cryptography works. 4

Ans:

Cryptography:

- ❖ Cryptography is the mathematical "scrambling" of data so that only someone with the necessary key can "unscramble" it.
- ❖ Cryptography allows secure transmission of private information over insecure channels.
- ❖ Cryptography also allows secure storage of sensitive data on any computer.

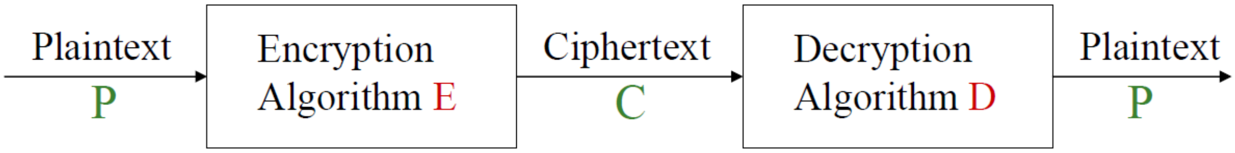


Figure: Cryptosystem

In cryptography, *encryption* is the process of transforming information (referred to as *plaintext*) using an algorithm (called *cipher*) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a *key*. The result of the process is encrypted information (in cryptography, referred to as *ciphertext*). In many contexts, the word encryption also implicitly refers to the reverse process, *decryption*, to make the encrypted information readable again (i.e. to make it unencrypted).

There are several ways to build a cipher.

Building a cipher - Substitution:
Replacing each byte with another.

Example (Cesar cipher): Replace a letter with the one following it by ***n*** positions. E.g.: The word “SECURE” becomes “VHFXUH”. Here, the key is 3, if the cipher is known bruteforcing it takes 25 attempts at most, 13 on average.

Building a cipher – Transposition or Diffusion:
Characters in a matrix, written by rows, read by columns. The “key” is the dimensions (in this case `K=[3,5]`). Not to be trivial, the product must be smaller than the message.

C	I	A	O	
A		T	U	T
T	I			

Here, CIAO A TUTTI (row-wise) and CATI IAT OU T (column-wise)

Public Key Cryptography:

- Higher degree of security
- Uses two keys:
    - Public key- freely distributed
    - Private Key- Kept secret by owner.
- If public key used to encrypt message only corresponding private key can decrypt it.

Example: RSA

Describe 3 steps (Key generation, encryption and decryption) of RSA encryption technique with an example of p=11 & q=13.

P= 11 and q=13

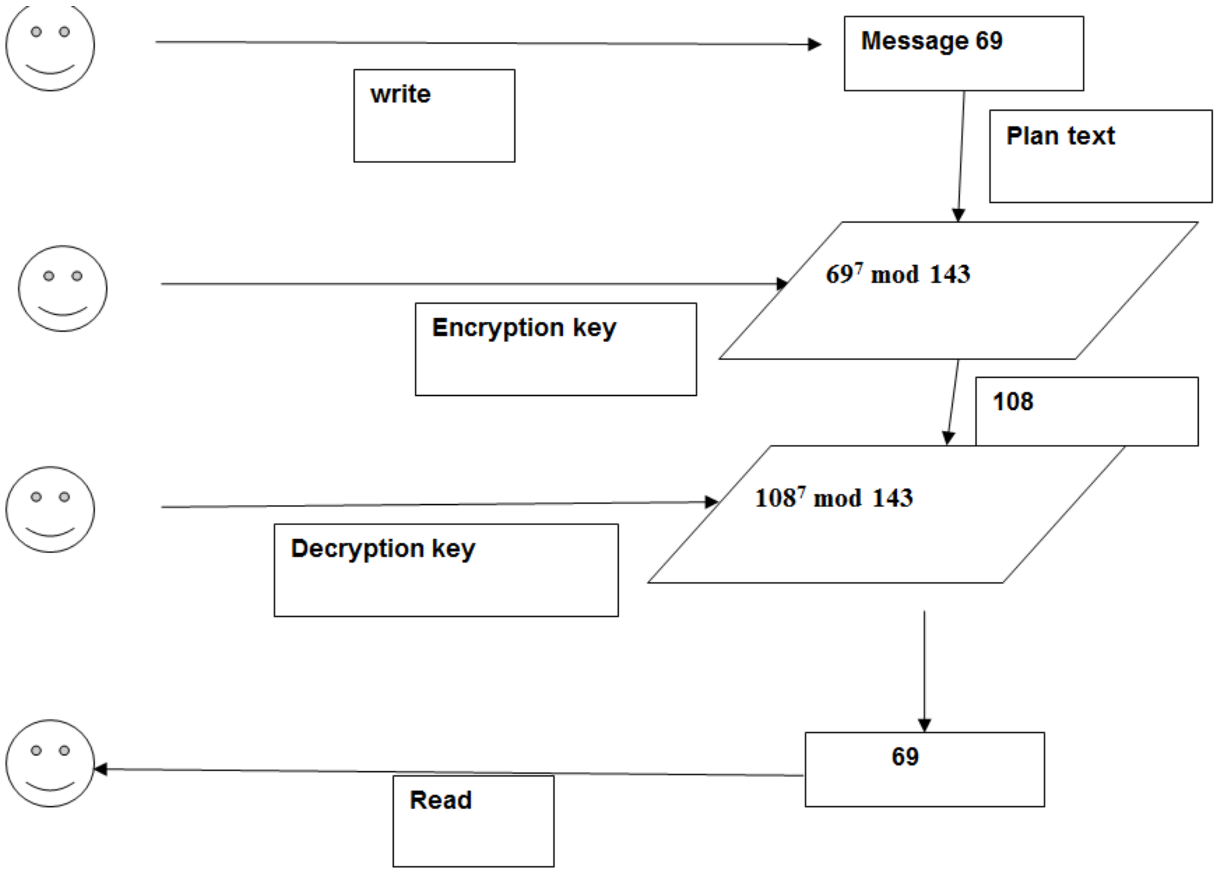
Then N= p*q = 11*13 =143 and Then z= (p-1)*(q-1) = 120

Public key, K_e = 7; choose a prime number that is 1< K_e < z, such that K_e is co-prime to z, i.e, z is not divisible by K_e

We can get K_d by K_e * K_d = 1 (mod z) So Private key, K_d = 103

Public key, $k_{e,}$ N = 7, 143 Private key, k_d , N = 103, 143

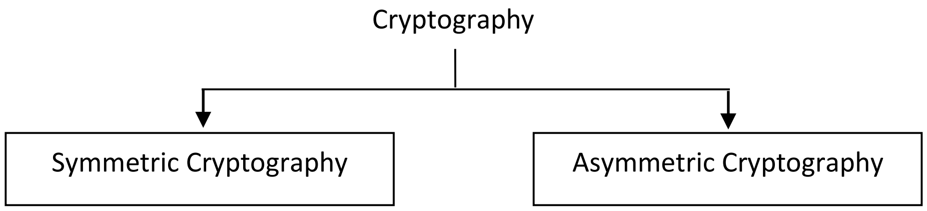
Encrypting the message 69 with the public key results in the cyphertext 108.



4. Write down the categories of cryptography? 2

Ans:

Categories of cryptography:



5. Write about the asymmetric cryptography? 2

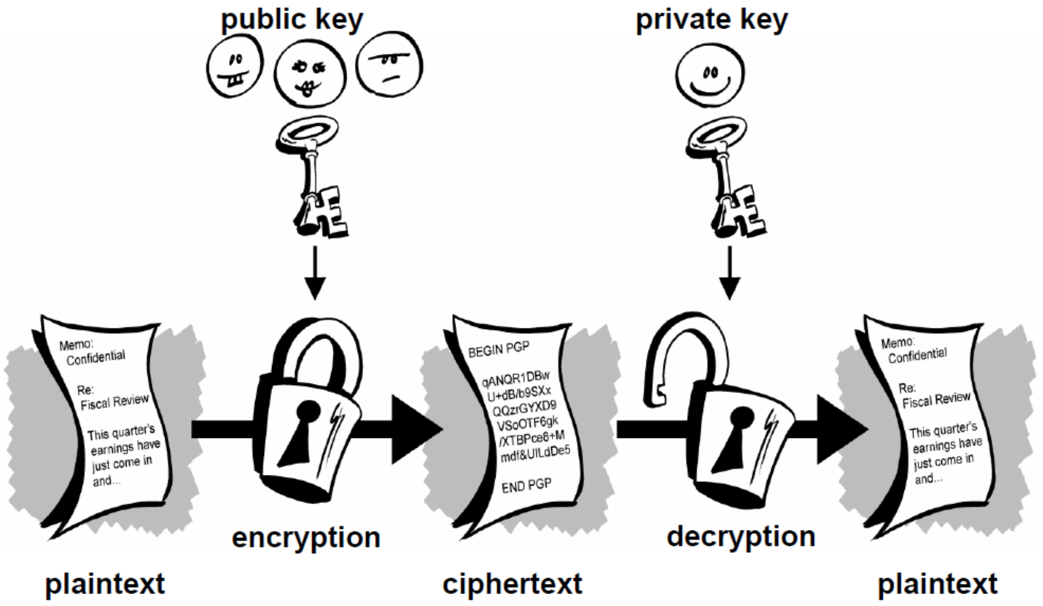
Or

What is public-key encryption? 2

Ans:

Asymmetric cryptography / Pubic-Key encryption / Asymmetric encryption:

- Different keys used to encrypt and decrypt message (One public, one private)
- Provides non-repudiation of message or message integrity
- Examples include RSA, DSA.



How it works:

- Alice generates a key value which she makes public.
- Alice uses her public key to determine a second key (her private key).
- Alice keeps her private key secret.
- Bob can use Alice's public key to encrypt a message for Alice.
- Alice can use her private key to decrypt this message.
- No-one without access to Alice's private key can easily decrypt the message.

6. What are the problems with symmetric cryptography? 3

Or

Write down the pros and cons of symmetric and asymmetric cryptography.

Or

What are the advantages and disadvantages of public-key cryptography compared with secret-key cryptography? 4

Ans:

Symmetric cryptography / Private-Key encryption / Secret-Key encryption:

Pros. / Advantages:

1. Key generation is simple.
2. Light computation load.
3. Easy to implement, esp., by hardware.
4. Uses less computer resources.
5. Keys for symmetric-key ciphers are relatively short.
6. Prevents widespread message security compromise.
7. Symmetric key encryption is much faster than asymmetric key encryption.
8. Symmetric-key ciphers can be used as primitives to construct various cryptographic mechanisms (i.e. pseudorandom number generators).

Cons. / Disadvantages / Problems:

Symmetric encryption, although fast, suffers from several problems in the modern digital communication environment including:

1. The biggest problem - that of a single key that must be shared in pairs of each sender and receiver. In a distributed environment with large numbers of combination pairs involved in many-to-one communication topology, it is difficult for the one recipient to keep so many keys in order to support all communication.
2. The size of the communication space presents problems. Because of the massive potential number of individuals who can carry on communication in a many-to-one, one-to-many, and many-to-many topologies supported by the Internet for example, the secret-key cryptography, if strictly used, requires billions of secret keys pairs to be created, shared, and stored.
3. The integrity of data can be compromised because the receiver cannot verify that the message has not been altered before receipt.
4. It is possible for the sender to repudiate the message because there are no mechanisms for the receiver to make sure that the message has been sent by the claimed sender.
5. The method does not give a way to ensure secrecy even if the encryption process is compromised.
6. The secret key may not be changed frequently enough to ensure confidentiality.

Asymmetric cryptography / Pubic-Key encryption / Asymmetric encryption:

Pros. / Advantages:

1. No shared secrets.
2. Key management easier.
3. Provides secrecy and authenticity.
4. Provide for non-repudiation.
5. Detection of tampering.

Cons. / Disadvantages / Problems:

Although public key encryption seems to have solved the major chronic encryption problems of key exchange and message repudiation, it still has its own problems.

1. The biggest problem for public key cryptographic scheme is *speed*. Public key algorithms are *extremely slow* compared to symmetric algorithms. This is because public key calculations take longer than symmetric key calculations since they involve the use of exponentiation of very large numbers which in turn take longer to compute. For example, the fastest public key cryptographic algorithm such as RSA is still far slower than any typical symmetric algorithm. This makes these algorithms and the public key scheme less desirable for use in cases of long messages.
2. Public key encryption algorithms have a potential to suffer from the *man-in-the-middle* attack. The man-in-the-middle attack is a well-known attack, especially in the network community where an attacker sniffs packets off a communication channel, modifies them, and inserts them back on to the channel.
3. Large key size.
4. Key generation is more difficult.
5. Uses up more computer resources.
6. Loss of private key may be irreparable.
7. No asymmetric-key scheme has been proven to be secure.

7. Write about the Symmetric cryptography / Private-Key / Secret-Key encryption? 2

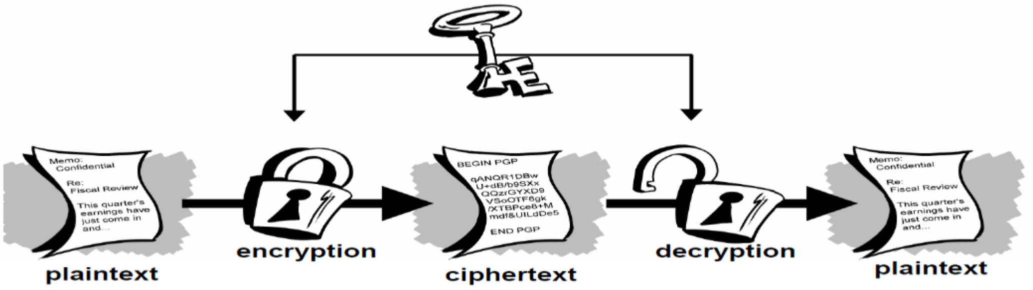
Ans:

Symmetric Cryptography:

❖ Same key used to encrypt and decrypt message. Faster than asymmetric encryption

❖ Used by IPSec to encrypt actual message data. Examples: DES, 3DES, RC5.

Shared Secret Key



Can also add advantage, disadvantages according to your choice.

8. How does Secure Socket Layer (SSL) work? 3

Or

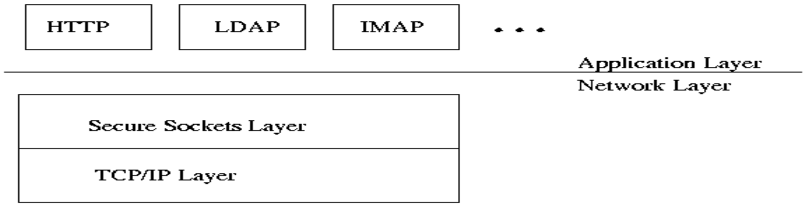
Describe with example how digital certificate, certificate authorities and SSL works together to exchange data on the web securely and reliably. 6

Ans:

Secure Socket Layer (SSL):

The Secure Sockets Layer (SSL) is a commonly-used protocol for managing the security of a message transmission on the Internet. It is developed by Netscape. It is a whole new layer of protocol which operates above the Internet TCP protocol and below high-level application protocols. SSL has recently been succeeded by Transport Layer Security (TLS).

Figure 1 SSL runs above TCP/IP and below high-level application protocols



What Can SSL Do?

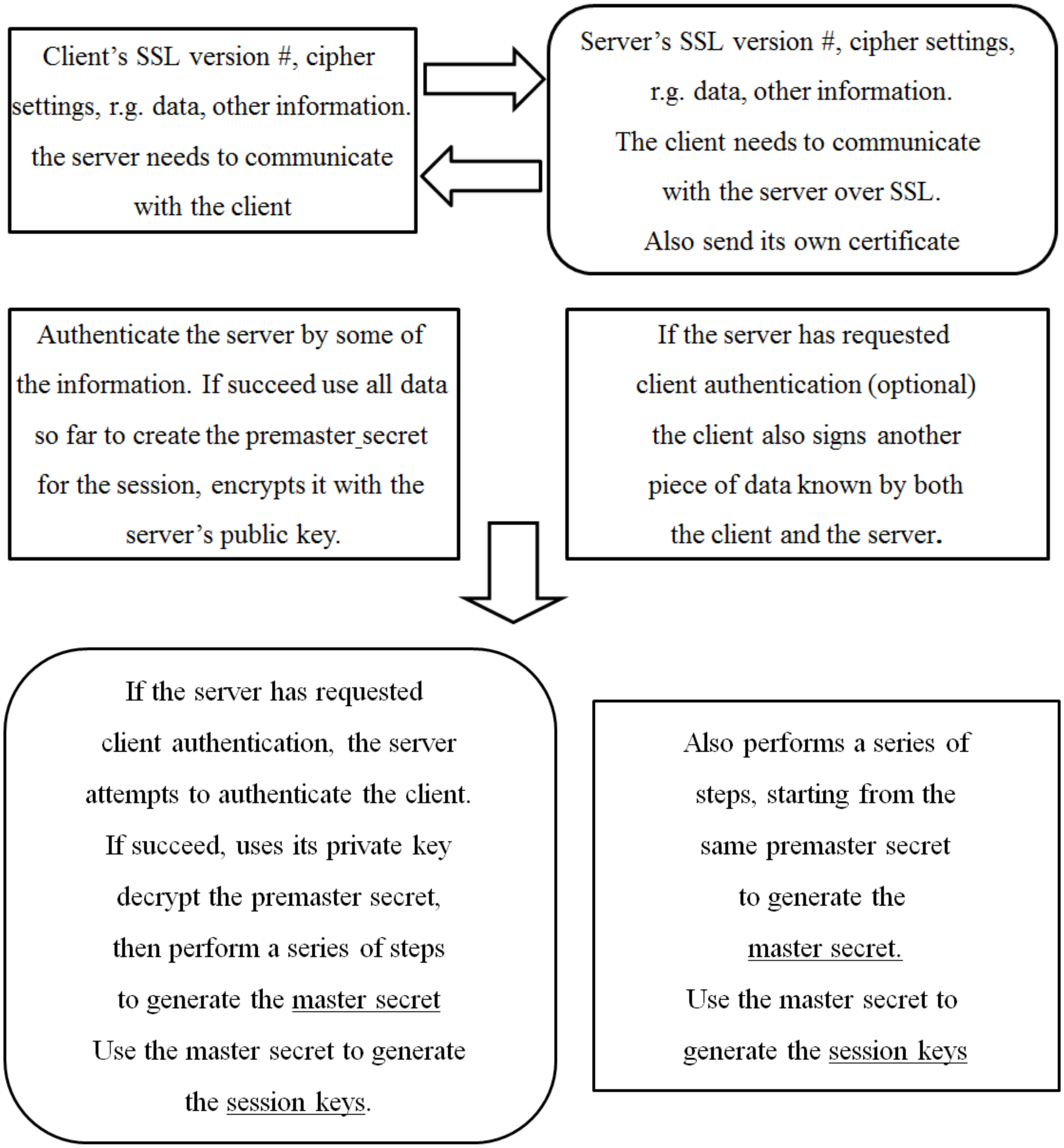
- SSL uses TCP/IP on behalf of the higher-level protocols.
- Allows an SSL-enabled server to authenticate itself to an SSL-enabled client;
- Allows the client to authenticate itself to the server;
- Allows both machines to establish an encrypted connection.

What Does SSL Concern?

- SSL server authentication.
- SSL client authentication. (optional)
- An encrypted SSL connection or Confidentiality. This protects against electronic eavesdropper.
- Integrity. This protects against hackers.
- SSL includes two sub-protocols: the SSL Record Protocol and the SSL Handshake Protocol.
- Record Protocol -- defines the format used to transmit data.
- Handshake Protocol -- using the Record protocol to exchange messages b/t an SSL-enable server and an SSL-enable client.
- The exchange of messages facilitates the following actions:
  Authenticate the server to the client; Allows the client and server to select a cipher that they both support; optionally authenticate the client to the server; Use public-key encryption techniques to generate share secrets; Establish an encrypted SSL conn.

How does SSL Work?

- The SSL protocol uses RSA public key cryptography for Internet Security.
- Public key encryption uses a pair of asymmetric keys for encryption and decryption.
- Each pair of keys consists of a public key and a private key. The public key is made public by distributing it widely; the private key is always kept secret.
- Data encrypted with the public key can be decrypted only with the private key, and vice versa.



Client's SSL version #, cipher settings, r.g. data, other information. the server needs to communicate with the client

Server's SSL version #, cipher settings, r.g. data, other information. The client needs to communicate with the server over SSL. Also send its own certificate

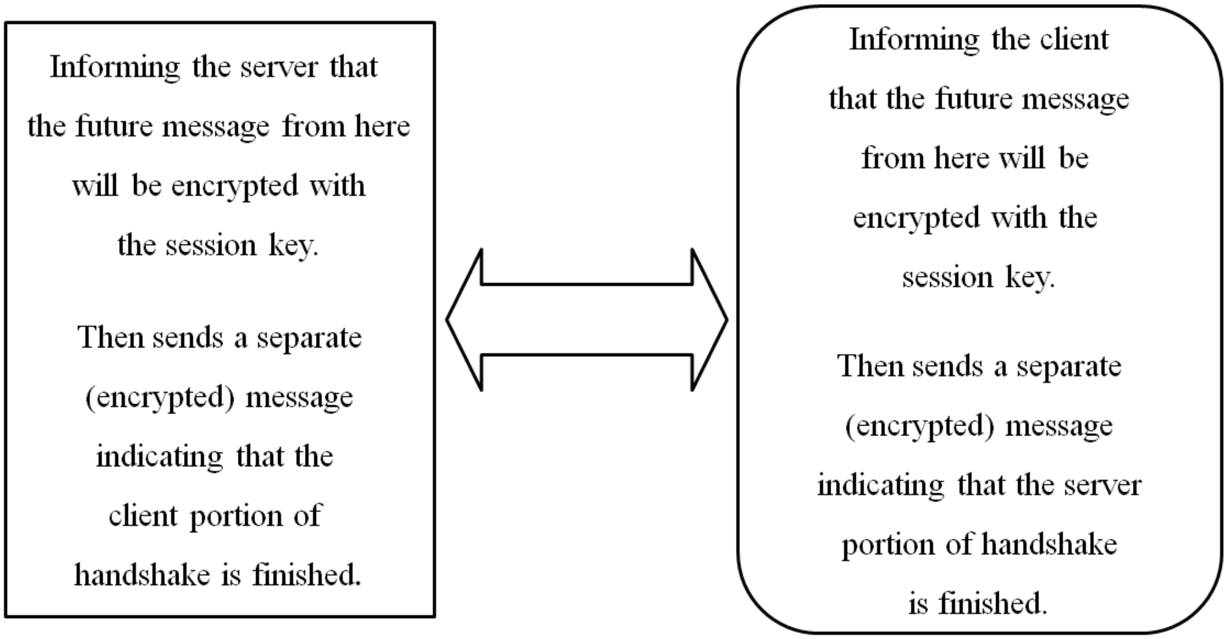
Authenticate the server by some of the information. If succeed use all data so far to create the premaster_secret for the session, encrypts it with the server's public key.

If the server has requested client authentication (optional) the client also signs another piece of data known by both the client and the server.

If the server has requested client authentication, the server attempts to authenticate the client. If succeed, uses its private key decrypt the premaster secret, then perform a series of steps to generate the master secret Use the master secret to generate the session keys.

Also performs a series of steps, starting from the same premaster secret to generate the master secret. Use the master secret to generate the session keys

Session keys are used to encrypt and decrypt information exchange during the SSL session and to verify its integrity. Master secrets protect session keys in transit.



Informing the server that the future message from here will be encrypted with the session key.

Then sends a separate (encrypted) message indicating that the client portion of handshake is finished.

Informing the client that the future message from here will be encrypted with the session key.

Then sends a separate (encrypted) message indicating that the server portion of handshake is finished.

The SSL handshake is now complete. The server and the client use the session keys to encrypt and decrypt the data they send to each other and to validate its integrity.

Note that both client and server authentication involve encrypting some pieces of data with one key of a public-private key pair and decrypting it with the other key.

9. Write Short Notes on the following: c) SSL Vs TLS 2.5
Ans:

Secure Socket Layer (SSL):
The Secure Sockets Layer (SSL) is a commonly-used protocol for managing the security of a message transmission on the Internet. It is developed by Netscape. It is a whole new layer of protocol which operates above the Internet TCP protocol and below high-level application protocols. SSL has recently been succeeded by Transport Layer Security (TLS)

Transport Layer Security (TLS):
Transport Layer Security (TLS) is a protocol that ensures privacy between communicating applications and their users on the Internet. When a server and client communicate, TLS ensures that no third party may eavesdrop or tamper with any message. TLS is the successor to the Secure Sockets Layer (SSL).

- TLS and SSL are *not interoperable*. However, a message sent with TLS can be handled by a client that handles SSL but not TLS.

- If you *are configuring a server*, you should install software that supports the latest version of the TLS standard, and configure it properly. This ensures that the connection that your user makes is as secure as possible.

  If you are *configuring a program* (especially an email program) and have the option to connect securely via SSL or TLS, you should feel free to choose either one…. as long as it is supported by your server.

- TLS v1.0 is marginally more *secure* than SSL v3.0, its predecessor. However, subsequent versions of TLS — v1.1 and v1.2 are significantly more secure and fix many vulnerabilities present in SSL v3.0 and TLS v1.0.

10. What is Secure Electronic Transaction (SET)? How SET works? 3
Ans:

Secure Electronic Transaction (SET):

- An open encryption and security specification.
- Protect credit card transaction on the Internet.
- Companies involved:
  - MasterCard, Visa, IBM, Microsoft, Netscape, RSA, Terisa and Verisign
- Not a payment system.
- Set of security protocols and formats.

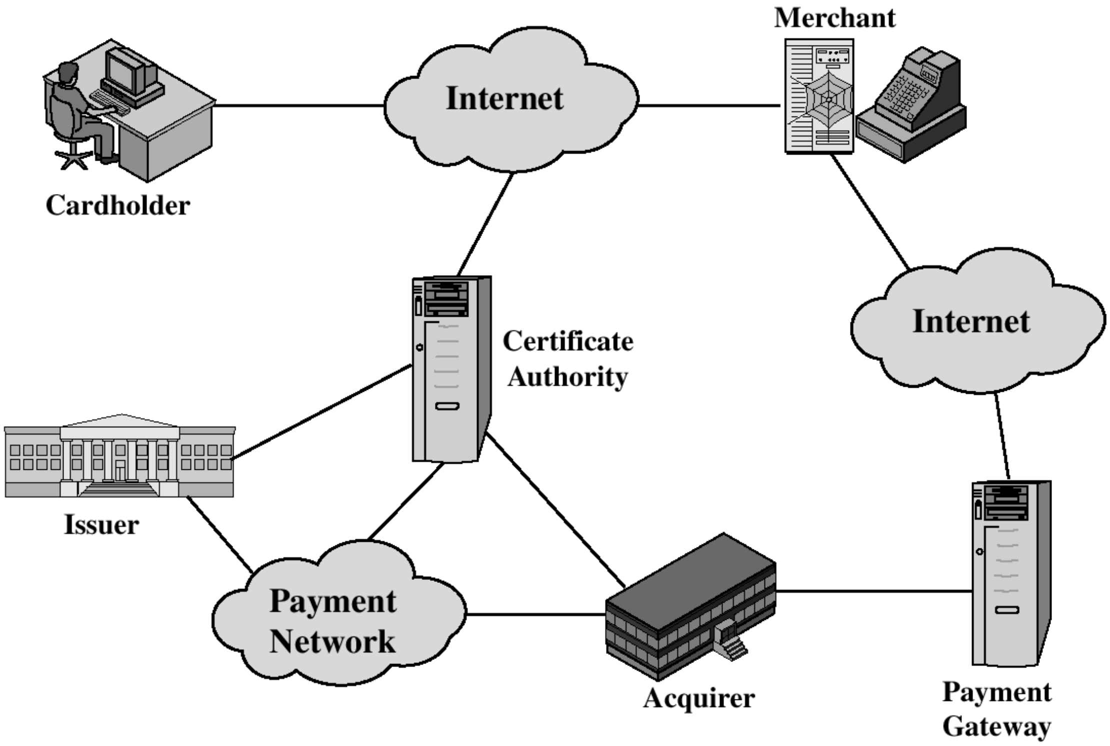
SET Services:

- Provides a secure communication channel in a transaction.
- Provides tust by the use of X.509v3 digital certificates.
- Ensures privacy.

Key Features of SET:

- Confidentiality of information
- Integrity of data
- Cardholder account authentication
- Merchant authentication

SET Participants:



Sequence of events for transactions / How SET Works:

1. The customer opens an account.
2. The customer receives a certificate.
3. Merchants have their own certificates.
4. The customer places an order.
5. The merchant is verified.
6. The order and payment are sent.
7. The merchant request payment authorization.
8. The merchant confirm the order.
9. The merchant provides the goods or service.
10. The merchant requests payments.

11. What is handshaking? How handshaking works?
Ans:

Handshaking:

Handshaking is an automated process of negotiation that dynamically sets parameters of a communications channel established between two entities before normal communication over the channel begins. It follows the physical establishment of the channel and precedes normal information transfer.

It is usually a process that takes place when a computer is about to communicate with a foreign device to establish rules for communication. When a computer communicates with another device like a modem, printer, or network server, it needs to handshake with it to establish a connection.

How it works? / Example:

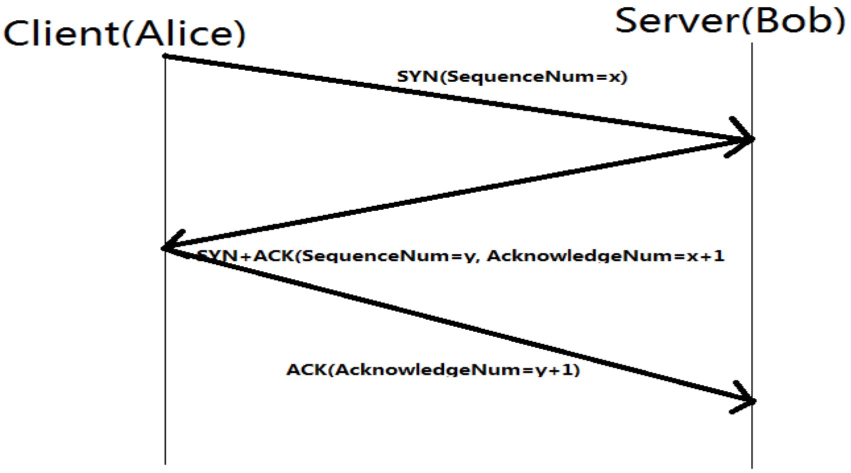
The TLS Handshake Protocol is used to negotiate the secure attributes of a session.

Three way handshake:

Establishing a normal TCP connection requires three separate steps:

1. The first host (Alice) sends the second host (Bob) a "synchronize" (SYN) message with its own sequence number x, which Bob receives.
2. Bob replies with a synchronize-acknowledgment (SYN-ACK) message with its own sequence number y and acknowledgement number $x+1$, which Alice receives.
3. Alice replies with an acknowledgment message with acknowledgement number $y+1$, which Bob receives and to which he doesn't need to reply.

In this setup, the synchronize messages act as service requests from one server to the other, while the acknowledgement messages return to the requesting server to let it know the message was received.



12. How message digest works?
Ans:

A message digest is a cryptographic hash function containing a string of digits created by a one-way hashing formula.

Message digests are designed to protect the integrity of a piece of data or media to detect changes and alterations to any part of a message. They are a type of cryptography utilizing hash values that can warn the copyright owner of any modifications applied to their work.

A cryptographic hash function is a hash function which is considered practically impossible to invert, that is, to recreate the input data from its hash value alone. The input data is often called the message, and the hash value is often called the message digest or simply the digest.

The ideal cryptographic hash function has four main properties:

- it is easy to compute the hash value for any given message
- it is infeasible to generate a message that has a given hash
- it is infeasible to modify a message without changing the hash
- it is infeasible to find two different messages with the same hash.

Illustration:
An illustration of the potential use of a cryptographic hash is as follows: Alice poses a tough math problem to Bob and claims she has solved it. Bob would like to try it himself, but would yet like to be sure that Alice is not bluffing. Therefore, Alice writes down her solution, computes its hash and tells Bob the hash value (whilst keeping the solution secret). Then, when Bob comes up with the solution himself a few days later, Alice can prove that she had the solution earlier by revealing it and having Bob hash it and check that it matches the hash value given to him before.

13. Digital certificate.
Ans:

Digital Certificate:
A digital certificate is an electronic "passport" that allows a person, computer or organization to exchange information securely over the Internet using the public key infrastructure (PKI). PKI comprises of the technology to enables secure e-commerce and Internet based communication.A digital certificate may also be referred to as a public key certificate.

14. RSA algorithm.

Ans:

RSA involves a public key and private key. The public key can be known to everyone, it is used to encrypt messages. Messages encrypted using the public key can only be decrypted with the private key. The keys for the RSA algorithm are generated the following way:

1. Choose two different large random prime numbers p and q
2. Calculate $n = pq$
   - $n$is the modulus for the public key and the private keys
3. Calculate the totient: $\phi(n) = (p-1)(q-1)$.
4. Choose an integer e such that 1 < e < $\phi(n)$,
   and e is coprime to $\phi(n)$ **ie:** e and $\phi(n)$ share no factors other than 1; gcd(e,$\phi(n)$) = 1.
   - $e$is released as the public key exponent
5. Compute d to satisfy the congruence relation $de \equiv 1 \pmod{\phi(n)}$ **ie:** $de = 1 + k\phi(n)$ for some integer k.
   - $d$is kept as the private key exponent