RESOURCE MATERIAL

ON

CRYPTOGRAPHY

AND

NETWORK SECURITY

(FOR 6TH SEMESTER CSE/IT)

Prepared by

Smt.Archana Tripathy
Lect.Comp.Sc.
Govt.Polytechnic,Bhubaneswar.

Chapter-1

POSSIBLE ATTACKS ON COMPUTERS

1.1 Need for Security

Computer security basically is the protection of **computer** systems and information from harm, theft, and unauthorized use. It is the process of preventing and detecting unauthorized use of your **computer** system. Cyber security is defined as protecting **computer** systems, which communicate over the **computer** networks.

Computer security is **important** because it keeps your information protected. It's also **important** for your **computer's** overall health; proper **computer security** helps prevent viruses and malware, which allows programs to run quicker and smoother.

1.2 Security Approaches

Trusted system:

A trusted system is a computer system that can be trusted to a specific extent to enforce a specific policy.

SECURITY MODELS An organization can take several approaches to implement its security model. Let us summarize these approaches.

No Security: In this simplest case, the approach could be a decision to implement no security at all.

Security through obscurity: In this model, a system is secure simply because nobody knows about its existence and contents. This approach cannot work for too long, as there are many ways an attacker can come to know about it.

Hot Security: In this scheme, the security for each host is enforced individually. This is a very safe approach, but the trouble is that it cannot scale well. The complexity and diversity of modern sites/organizations makes the task even harder.

Network Security: Host security is tough to achieve as organizations grow and become more diverse. In this technique, the focus is to control network access to various hosts and their services, rather than individual host security. This is a very efficient and scalable model.

INTRODUCTION

Computer data often travels from one computer to another, leaving the safety of its protected physical surroundings. Once the data is out of hand, people with bad intention could modify or forge your data, either for amusement or for their own benefit. Cryptography can reformat and transform our data, making it safer on its trip between computers. The technology is based on the essentials of secret codes, augmented by modern mathematics that protects our data in powerful ways.

- Computer Security - generic name for the collection of tools designed to protect data and to thwart hackers

- Network Security - measures to protect data during their transmission

- Internet Security - measures to protect data during their transmission over a collection of interconnected networks Security Attacks, Services and Mechanisms To assess the security needs of an organization effectively, the manager responsible for security needs some systematic way of defining the requirements for security and characterization of approaches to satisfy those requirements. One **Approach is to consider three aspects of information security:**

Security Attack – Any action that compromises the security of information owned by an organization.

Security Mechanism – A mechanism that is designed to detect, prevent or recover from a security attack.

Security Service – A service that enhances the security of the data processing systems and the information transfers of an organization. The services are intended to counter security attacks and they make use of one or more security mechanisms to provide the service.

Principle of Security:-

The classification of security services are as follows:

Confidentiality: Ensures that the information in a computer system an n d transmitted information are accessible only for reading by authorized parties. E.g. Printing, displaying and other forms of disclosure.

Authentication: Ensures that the origin of a message or electronic document is correctly identified, with an assurance that the identity is not false.

Integrity: Ensures that only authorized parties are able to modify computer system assets and transmitted information.

Modification includes writing, changing status, deleting, creating and delaying or replaying of transmitted messages. Non repudiation: Requires that neither the sender nor the receiver of a message be able to deny the transmission.

Access control: Requires that access to information resources may be controlled by or the target system.

Availability: Requires that computer system assets be available to authorized parties when needed.

Types of Attack:-

SECURITY ATTACKS There are four general categories of attack which are listed below.

Interruption:- An asset of the system is destroyed or becomes unavailable or unusable. This is an attack on availability e.g., destruction of piece of hardware, cutting of a communication line or Disabling of file management system.

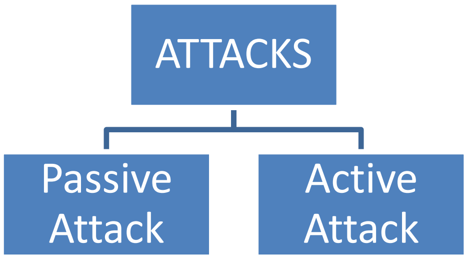
Interception:-An unauthorized party gains access to an asset. This is an attack on confidentiality. Unauthorized party could be a person, a program or a computer. e.g., wire tapping to capture data in the network, illicit copying of files Sender Receiver Eavesdropper or forger

Modification:- An unauthorized party not only gains access to but tampers with an asset. This is an attack on integrity. e.g., changing values in data file, altering a program, modifying the contents of messages being transmitted in a network. Sender Receiver Eavesdropper or forger

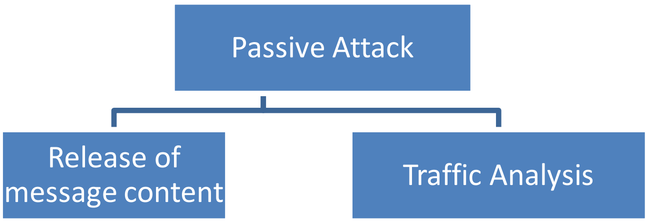
Fabrication:- An unauthorized party inserts counterfeit objects into the system. This is an attack on authenticity. e.g., insertion of spurious message in a network or addition of records to a file. Sender Receiver Eavesdropper or forger

Cryptographic Attacks

Types of Attack



Passive Attacks (Interception):-



Passive Attacks (Interception):-

Passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions. The goal of the opponent is to obtain information that is being transmitted. Passive attacks are of two types:

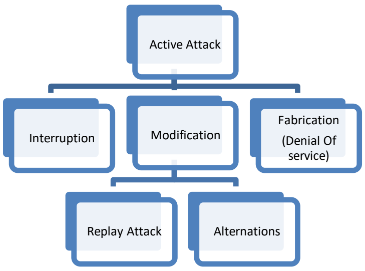
1. Release of message contents:

A telephone conversation, an e-mail message and a transferred file may contain sensitive or confidential information. We would like to prevent the opponent from learning the contents of these transmissions.

2. Traffic analysis:

If we had encryption protection in place, an opponent might still be able to observe the pattern of the message. The opponent could determine the location and identity of communication hosts and could observe the frequency and length of messages being exchanged. This information might be useful in guessing the nature of communication that was taking place. Passive attacks are very difficult to detect because they do not involve any alteration of data. However, it is feasible to prevent the success of these attacks.

Active Attacks:-



These attacks involve some modification of the data stream or the creation of a false stream. These attacks can be classified in to four categories:

Masquerade (Interruption):– One entity pretends to be a different entity.

Modification of messages: - Some portion of message is altered or the messages are delayed or recorded, to produce an unauthorized effect. Modifications are two types

Replay: - Involves passive capture of a data unit and its subsequent transmission to produce an unauthorized effect.

Alteration: - Alteration of message involves some changes to the original message. **Denial of service (Fabrication) (DOS)** – Prevents or inhibits the normal use or management of communication facilities. Another form of service denial is the disruption of an entire network, either by disabling the network or overloading it with messages so as to degrade performance. It is quite difficult to prevent active attacks absolutely, because to do so would require physical protection of all communication facilities and paths at all times. Instead, the goal is to detect them and to recover from any disruption or delays caused by them.

Model Questions

Chapter-1

Possible attack on computes:

1. What are the key principles of security? (10)
2. Define security? Explain the need of security. (6)
3. Explain different security model. (6)
4. Explain different security approaches available for security purpose. (10)
5. Describe the principle of security. (10)
6. What are the types of attack to a computer system? (10)
7. Define virus? (2)
8. Define worm? (2)
9. What do you mean trusted system? (2)
10. What do you mean by OSI standard for security model? (2)
11. Distinguish between identify theft and brand theft? (2)
12. Define Trojan horse? (2)
13. Define cookies? (2)

Chapter-2

CRYPTOGRAPHY CONCEPTS

Cryptography is the study and practice of techniques for secure communication in the presence of third parties called adversaries. It deals with developing and analyzing protocols which prevents malicious third parties from retrieving information being shared between two entities thereby following the various aspects of information security.

OR

Cryptography is the study and application of techniques that hide the real meaning of information by transforming it into nonhuman readable formats and vice versa.

Cryptography – Benefits

Cryptography is an essential information security tool. It provides the four most basic services of information security −

Confidentiality − Encryption technique can guard the information and communication from unauthorized revelation and access of information.

Authentication − the cryptographic techniques such as MAC and digital signatures can protect information against spoofing and forgeries.

Data Integrity − The cryptographic hash functions are playing vital role in assuring the users about the data integrity.

Non-repudiation − The digital signature provides the non-repudiation service to guard against the dispute that may arise due to denial of passing message by the sender.

All these fundamental services offered by cryptography has enabled the conduct of business over the networks using the computer systems in extremely efficient and effective manner.

The process of transforming information into nonhuman readable form is called **encryption.**

The process of reversing encryption is called **decryption**.

Decryption is done using a **secret key** which is only known to the legitimate recipients of the information. The key is used to decrypt the hidden messages. This makes the communication secure because even if the attacker manages to get the information, it will not make sense to them.

The encrypted information is known as a **Cipher**.

What is Cryptanalysis?

Cryptanalysis is the art of trying to decrypt the encrypted messages without the use of the key that was used to encrypt the messages. Cryptanalysis uses mathematical analysis & algorithms to decipher the ciphers. The success of cryptanalysis attacks depends

- Amount of time available
- Computing power available
- Storage capacity available

The following is a list of the commonly used Cryptanalysis attacks;

Brute force attack– this type of attack uses algorithms that try to guess all the possible logical combinations of the plaintext which are then ciphered and compared against the original cipher.

Dictionary attack– this type of attack uses a wordlist in order to find a match of either the plaintext or key. It is mostly used when trying to crack encrypted passwords.

Rainbow table attack– this type of attack compares the cipher text against pre-computed hashes to find matches.

Cryptanalysis:-

Cryptanalysis is the study of analyzing information systems in order to study the hidden aspects of the systems. Cryptanalysis is used to breach cryptographic security systems and gain access to the contents of encrypted messages, even if the cryptographic key is unknown.

What is Cryptology?

Cryptology combines the techniques of cryptography and cryptanalysis.

OR

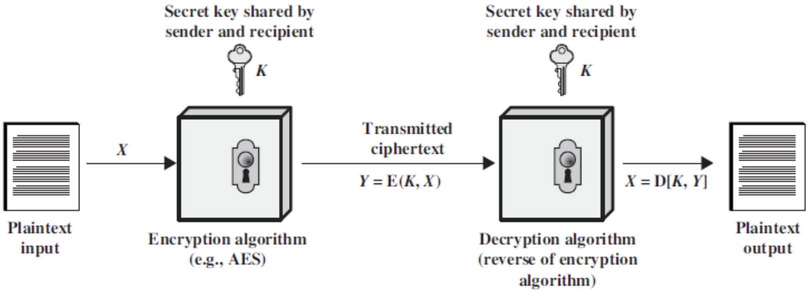
Cryptology: - Cryptology is a combination of Cryptography and Cryptanalysis:- Cryptanalysis is the technique of decoding messages from a non-readable format back to readable format without knowing how they were initially converted from readable format to non-readable format.

2.1 Plain text and Cipher text

Plain Text:-

Clear text or plain text signifies a message that can be understood by the sender, the recipient and also by anyone else who gets an access to that message.

Cipher text:- When a plain text message is codifies using any suitable scheme, the resulting message is called as cipher text.


Secret key shared by sender and recipient
K
Secret key shared by sender and recipient
K
X
Transmitted ciphertext
Y = E(K, X)
X = D[K, Y]
Plaintext input
Encryption algorithm (e.g., AES)
Decryption algorithm (reverse of encryption algorithm)
Plaintext output

There are two types of techniques used to covert plain text to cipher text.

- **Substitution Techniques**
- **Transposition Techniques**

2.2 SUBSTITUTION TECHNIQUES

A substitution technique is one in which the letters of plaintext are replaced by other letters or by numbers or symbols. If the plaintext is viewed as a sequence of bits, then substitution involves replacing plaintext bit patterns with cipher text bit patterns.

Caesar cipher (or) shift cipher

The earliest known use of a substitution cipher and the simplest was by Julius Caesar. TheCaesar cipher involves replacing each letter of the alphabet with the letter standing 3 placesfurther down the alphabet e.g., plain text: pay more money

Cipher text: SDB PRUH PRQHB Note that the alphabet is wrapped around, so that letter following „z‟ is „a‟. For each plaintext letter p, substitute the cipher text letter c such that

C = E(p) = (p+3) mod 26

A shift may be any amount, so that general Caesar algorithm is

C = E (p) = (p+k) mod 26

Where k takes on a value in the range 1 to 25. The decryption algorithm is simply

P = D(C) = (C-k) mod 26

Playfair cipher:-

The best known multiple letter encryption cipher is the playfair, which treats diagrams in the plaintext as single units and translates these units into cipher text diagrams. The playfair algorithm is based on the use of 5x5 matrix of letters constructed using a keyword. Let the keyword be „monarchy‟. The matrix is constructed by filling in the letters of the keyword(minus duplicates) from left to right and from top to bottom, and then filling in the remainder of the matrix with the remaining letters in alphabetical order. The letter „i‟ and „j‟ count as one letter. Plaintext is encrypted two letters at a time

According to the following rules:

Repeating plaintext letters that would fall in the same pair are separated with a Filler letter such as „x‟. Plaintext letters that fall in the same row of the matrix are each replaced by the letter to the right, with the first element of the row following the last. Plaintext letters that fall in the same column are replaced by the letter beneath, with the top Element of the column following the last. Otherwise, each plaintext letter is replaced by the letter that lies in its own row and the column occupied by the other plaintext letter.

Plaintext = meet me at the school house

Splitting two letters as a unit => me et me at the as ch o x ol ho us ex

Corresponding cipher text => CL KL CL RS PD IL HY AV MP HF XL IU

2.3 TRANSPOSITION TECHNIQUES

All the techniques examined so far involve the substitution of a cipher text symbol for a plaintext symbol. A very different kind of mapping is achieved by performing some sort of permutation on the plaintext letters. This technique is referred to as a transposition cipher.

Rail fence Technique:-

Rail fence Technique is simplest of such cipher, in which the plaintext is written down as a sequence of diagonals and then read off as a sequence of rows.

Plaintext = meet at the school house

To encipher this message with a rail fence of depth 2, we write the message as follows:

m e a t e c o l o s

e t t h s h o h u e

The encrypted message is

MEATECOLOSETTHSHOHUE

Row Transposition Ciphers-

A more complex scheme is to write the message in a rectangle, row by row, and read the message off, column by column, but permute the order of the columns. The order of columns then becomes the key of the algorithm.

e.g., plaintext = meet at the school house

Key = 4 3 1 2 5 6 7

PT = m e e t a t t

h e s c h o o

l h o u s e

CT = ESOTCUEEHMHLAHSTOETO

A pure transposition cipher is easily recognized because it has the same letter frequencies as the original plaintext. The transposition cipher can be made significantly more secure by performing more than one stage of transposition. The result is more complex permutation that is not easily reconstructed.

Feistel cipher structure

The input to the encryption algorithm are a plaintext block of length 2w bits and a key K.the plaintext block is divided into two halves L0 and R0. The two halves of the data passthrough „n‟ rounds of processing and then combine to produce the ciphertext block. Each round „i‟has inputs Li-1 and Ri-1, derived from the previous round, as well as the subkey Ki, derived from the overall key K. in general, the sub keys Ki are different from K and from each other. All rounds have the same structure. A substitution is performed on the left half of the data (as similar to S-DES). This is done by applying a round function F to the right half of the data and then taking the XOR of the output of that function and the left half of the data. The round function as the same general structure for each round but is parameterized by the round sub key ki. Following this substitution, a permutation is performed that consists of the interchange of the two halves of the data. This structure is a particular form of the substitution-permutation network.

The exact realization of a Festal network depends on the choice of the following parameters and design features:

Block size - Increasing size improves security, but slows cipher

Key size - Increasing size improves security, makes exhaustive key searching harder, but may slow cipher

Number of rounds - Increasing number improves security, but slows cipher

Sub key generation - Greater complexity can make analysis harder, but slows cipher

Round function - Greater complexity can make analysis harder, but slows cipher

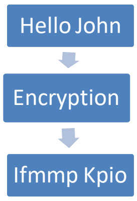
Fast software en/decryption & ease of analysis - are more recent concerns for practical use and testing.

Vernam Cipher (One-Time Pad):-

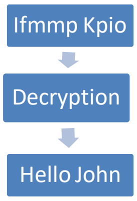
Vernam cipher uses a one-time pad, which is discarded after a single use and therefore is suitable for short messages.

2.4 Encryption and Decryption:-

Encryption:- The process of encoding plain text messages into cipher text messages is called as encryption.



Decryption:- The reverse process of transforming cipher text messages back to plain text messages is called as decryption.



2.5 Symmetric and Asymmetric Key Cryptography:

Symmetric key Cryptography:-

Symmetric key cryptography (or symmetric encryption) is a type of encryption scheme in which the same key is used both to encrypt and decrypt messages.

Asymmetric key Cryptography:-

Asymmetric encryption uses the public key for the encryption, and a private key is used for decryption.

Or

Asymmetric cryptography, also known as public-key cryptography, is a process that uses a pair of related keys -- one public key and one private key

Diffie-Helman key Exchange/Agreement Algorithm

Diffie Hellman (DH) key exchange algorithm is a method for securely exchanging cryptographic keys over a public communications channel. ... If Alice and Bob wish to communicate with each other, they first agree between them a large prime number p, and a generator (or base) g (where 0 < g < p).

ALICE	**BOB**
Public Keys available = P, G	Public Keys available = P, G
Private Key Selected = a	Private Key Selected = b
Key generated =	Key generated =
Exchange of generated keys takes place	
Key received = y	key received = x
Generated Secret Key =	Generated Secret Key =
Algebraically it can be shown that	
Users now have a symmetric secret key to encrypt	

Example
Step 1: Alice and Bob get public numbers P = 23, G = 9
Step 2: Alice selected a private key a = 4 and Bob selected a private key b = 3
Step 3: Alice and Bob compute public values Alice: x =(9^4 mod 23) = (6561 mod 23) = 6 Bob: y = (9^3 mod 23) = (729 mod 23) = 16
Step 4: Alice and Bob exchange public numbers
Step 5: Alice receives public key y =16 and Bob receives public key x = 6
Step 6: Alice and Bob compute symmetric keys Alice: ka=y^a mod p = 65536 mod 23 = 9 Bob: kb = x^b mod p = 216 mod 23 = 9
Step 7: 9 is the shared secret.

Model Questions

Chapter-2 Cryptography Concepts

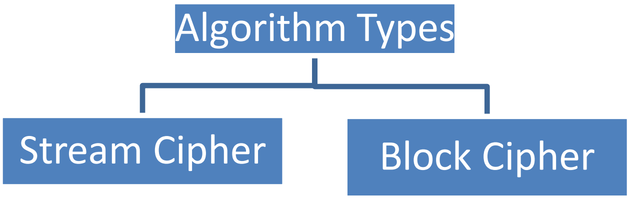
1. Define cryptography. (2)
2. What do you mean cryptanalysis? (2)
3. Distinguish between plain text and cipher text? (2)
4. Explain the substitution technique? (10)
5. Describe the transposition technique? (10)
6. What do you mean by symmetric &asymmetric cryptography? (10)
7. Explain poly alphabetic substitution cipher? (6)
8. What do you mean by rail fence technique? (6)
9. Explain Diffie-Helmans Key exchange /Agreement algorithm with suitable example. (6)
10. Define encryption? (2)
11. Distinguish between encryption & Decryption? (2)
12. What are the differences between encryption processes to decryption process? (6)
13. What is algorithm Mode? Explain various types of algorithm Modes. (10)

Chapter-3

Symmetric & Asymmetric Key Algorithms

3.1 Symmetric key algorithm types

Symmetric Algorithms Type



Stream Cipher:-

Stream Cipher technique involves the encryption of one plain text byte at a time. The decryption also happen one byte at a time.

Block Cipher:-

Block Cipher technique involves encryption of one block of text at a time. Decryption also takes one block of encrypted text at a time.

ALGORITHM MODES

ALGORITHM MODES:-
An Algorithm mode is a combination of series of basic algorithm steps on Block cipher and some kind of feedback from the previous step.

The four important Algorithm modes are

- Electronic Code Book (ECB)
- Cipher Block Chaining (CBC)
- Cipher Feedback (CFB)
- Output feedback (OFB)

Electronic Code Book (ECB) :-

Electronic code book is the easiest block cipher mode of functioning. It is easier because of direct encryption of each block of input plaintext and output is in form of blocks of encrypted cipher text. Generally, if a message is larger than *b* bits in size, it can be broken down into bunch of blocks and the procedure is repeated.

Cipher Block Chaining (CBC) :-
Cipher block chaining or CBC is an advancement made on ECB since ECB compromises some security requirements. In CBC, previous cipher block is given as input to next encryption algorithm after XOR with original plaintext block. In a nutshell here, a cipher block is produced by encrypting a XOR output of previous cipher block and present plaintext block.

Electronic Code Book (ECB) :-

Electronic code book is the easiest block cipher mode of functioning. It is easier because of direct encryption of each block of input plaintext and output is in form of blocks of encrypted cipher text. Generally, if a message is larger than *b* bits in size, it can be broken down into bunch of blocks and the procedure is repeated.

Cipher Block Chaining (CBC) :-
Cipher block chaining or CBC is an advancement made on ECB since ECB compromises some security requirements. In CBC, previous cipher block is given as input to next encryption algorithm after XOR with original plaintext block. In a nutshell here, a cipher block is produced by encrypting a XOR output of previous cipher block and present plaintext block.

Cipher Feedback Mode (CFB):-
In this mode the cipher is given as feedback to the next block of encryption with some new specifications: first an initial vector IV is used for first encryption and output bits are divided as set of *s* and *b-s* bits the

left hand side *s* bits are selected and are applied an XOR operation with plaintext bits. The result given as input to a shift register and the process continues. The encryption and decryption process for the same is shown below, both of them use encryption algorithm.

Output feedback (OFB):-

The output feedback mode follows nearly same process as the Cipher Feedback mode except that it sends the encrypted output as feedback instead of the actual cipher which is XOR output. In this output feedback mode, all bits of the block are send instead of sending selected *s* bits. The Output Feedback mode of block cipher holds great resistance towards bit transmission errors. It also decreases dependency or relationship of cipher on plaintext.

3.2 An Overview of Symmetric Key Cryptography

Symmetric key cryptography (or symmetric encryption) is a type of encryption scheme in which the same key is used both to encrypt and decrypt messages. Such a method of encoding information has been largely used in the past decades to facilitate secret communication between governments and militaries.

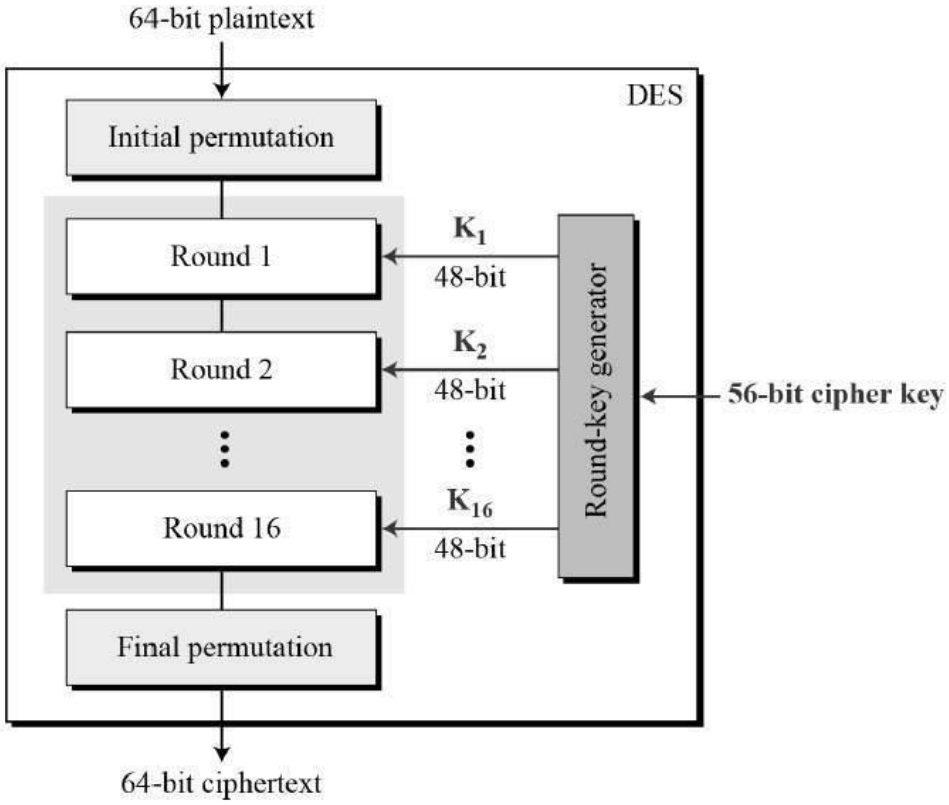
3.3 Data Encryption Standard:

The Data Encryption Standard (DES) is a symmetric-key block cipher published by the National Institute of Standards and Technology (NIST). DES is an implementation of a Feistel Cipher. It uses 16 round Feistel structure. The block size is 64-bit.

The Data Encryption Standard (DES) is a symmetric-key block cipher published by the National Institute of Standards and Technology (NIST).

How DES Works?

DES is an implementation of a Feistel Cipher. It uses 16 round Feistel structure. The block size is 64-bit. Though, key length is 64-bit, DES has an effective key length of 56 bits, since 8 of the 64 bits of the key are not used by the encryption algorithm (function as check bits only). General Structure of DES is depicted in the following illustration −



Since DES is based on the Feistel Cipher, all that is required to specify DES is –

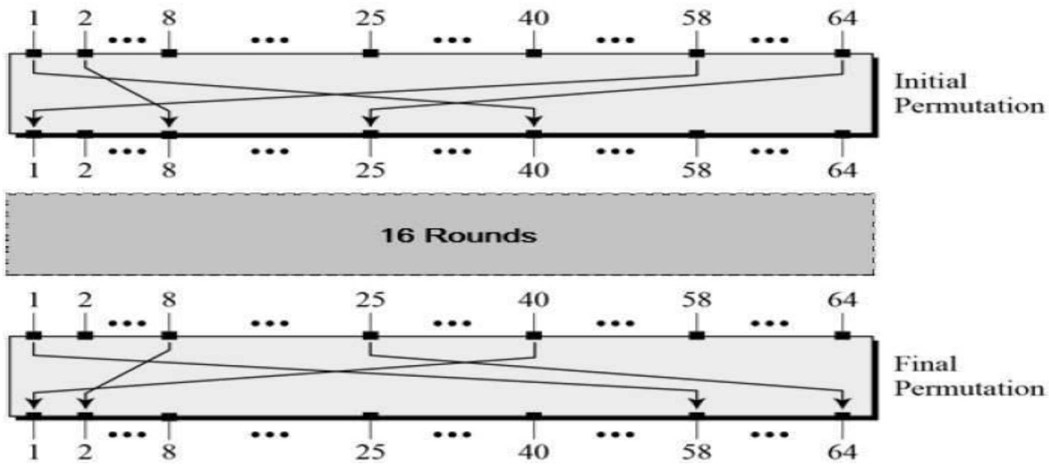
Round function

Key schedule

Any additional processing – Initial and final permutation

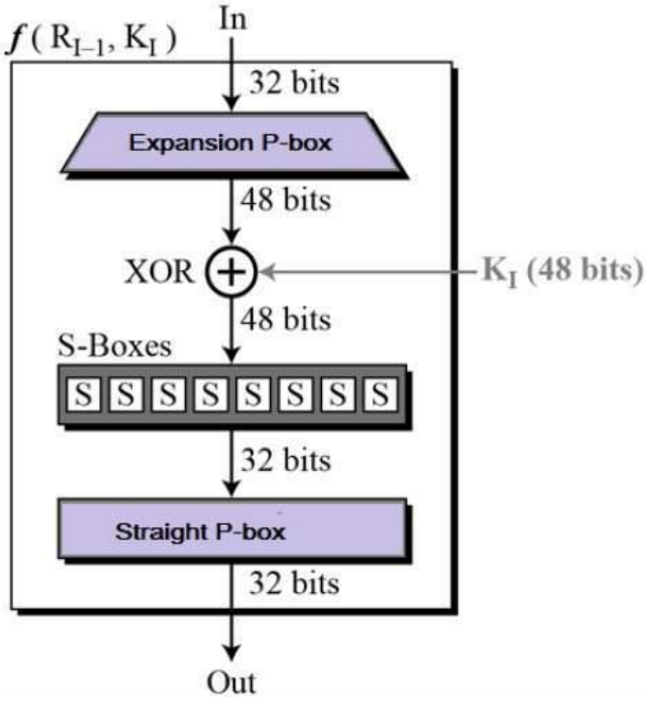
Initial and Final Permutation

The initial and final permutations are straight Permutation boxes (P-boxes) that are inverses of each other. They have no cryptography significance in DES. The initial and final permutations are shown as follows –

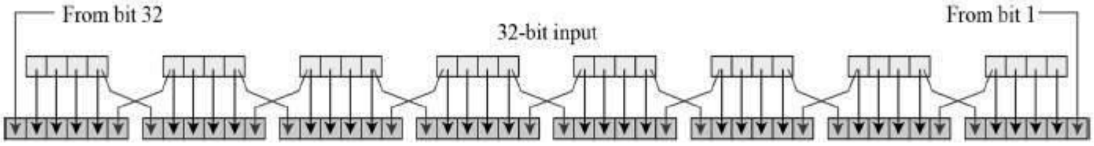


Round Function

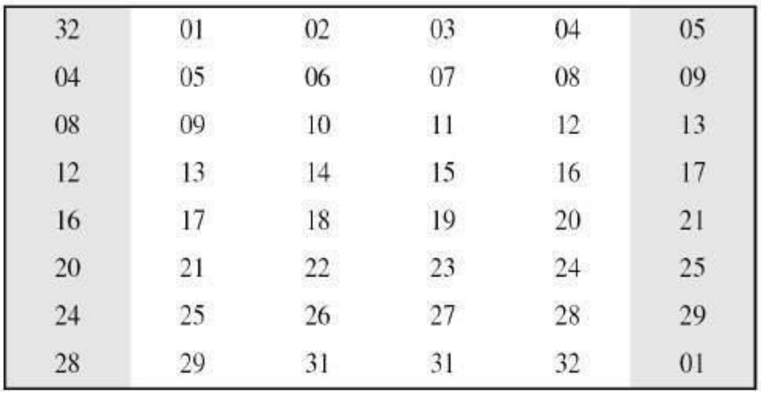
The heart of this cipher is the DES function, *f*. The DES function applies a 48-bit key to the rightmost 32 bits to produce a 32-bit output.



Expansion Permutation Box – Since right input is 32-bit and round key is a 48-bit, we first need to expand right input to 48 bits. Permutation logic is graphically depicted in the following illustration –



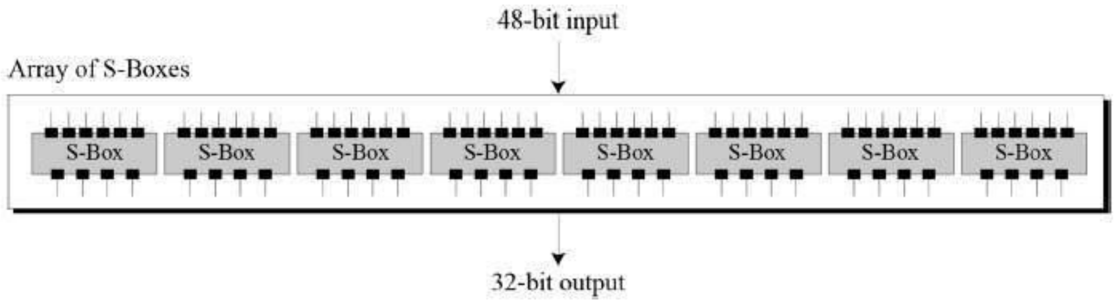
The graphically depicted permutation logic is generally described as table in DES specification illustrated as shown –



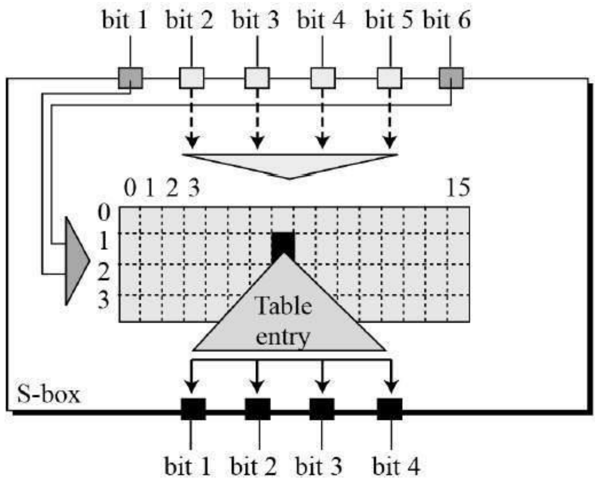
32	01	02	03	04	05
04	05	06	07	08	09
08	09	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	31	31	32	01

XOR (Whitener). – After the expansion permutation, DES does XOR operation on the expanded right section and the round key. The round key is used only in this operation.

Substitution Boxes. – The S-boxes carry out the real mixing (confusion). DES uses 8 S-boxes, each with a 6-bit input and a 4-bit output. Refer the following illustration –

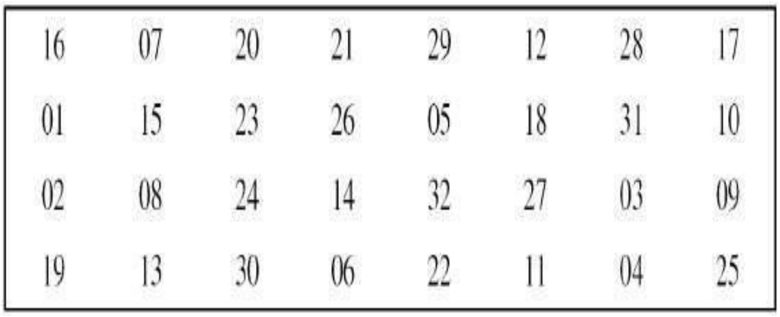


The S-box rule is illustrated below –



There are a total of eight S-box tables. The output of all eight s-boxes is then combined in to 32 bit section.

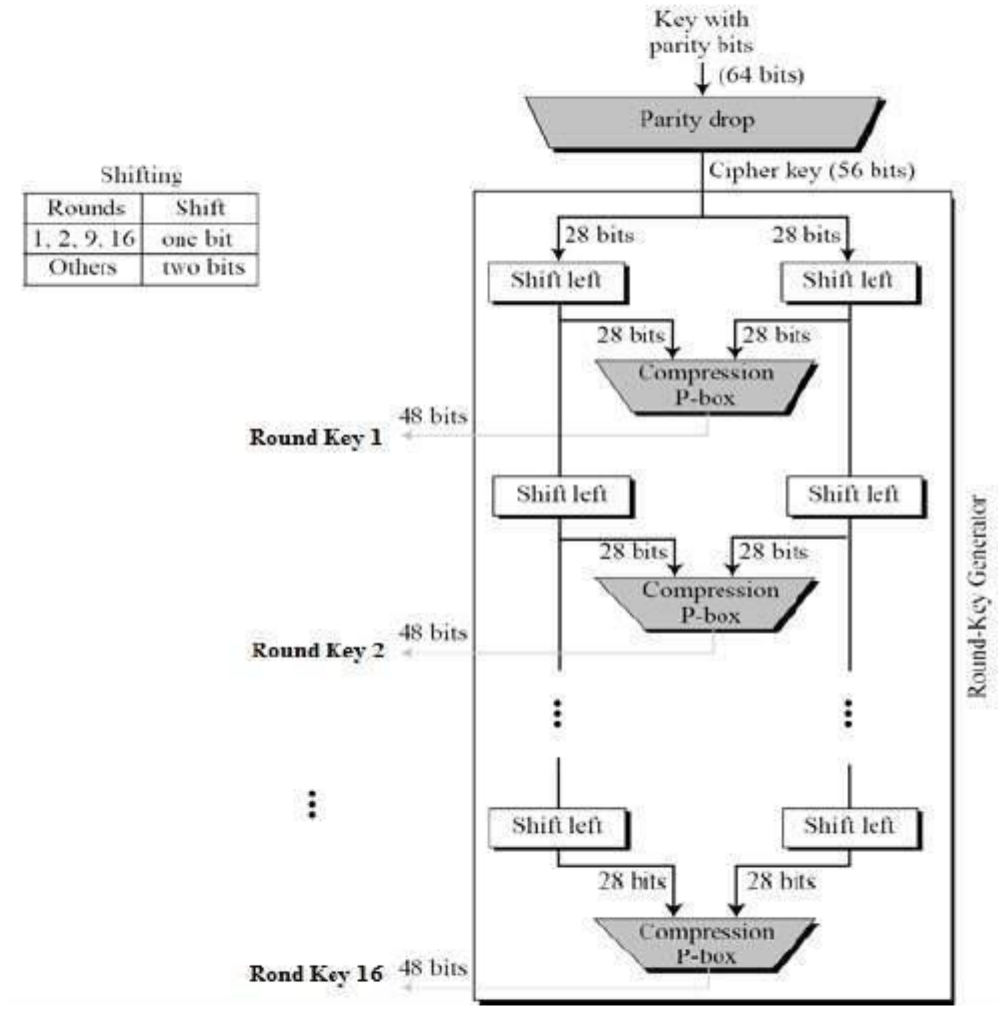
Straight Permutation – The 32 bit output of S-boxes is then subjected to the straight permutation with rule shown in the following illustration:



16	07	20	21	29	12	28	17
01	15	23	26	05	18	31	10
02	08	24	14	32	27	03	09
19	13	30	06	22	11	04	25

Key Generation

The round-key generator creates sixteen 48-bit keys out of a 56-bit cipher key. The process of key generation is depicted in the following illustration –



Shifting

Rounds	Shift
1, 2, 9, 16	one bit
Others	two bits

The logic for Parity drops, shifting, and Compression P-box is given in the DES description.

DES Analysis

The DES satisfies both the desired properties of block cipher. These two properties make cipher very strong.

Avalanche effect − A small change in plaintext results in the very great change in the cipher text.

Completeness − Each bit of cipher text depends on many bits of plaintext.

During the last few years, cryptanalysis has found some weaknesses in DES when key selected are weak keys. These keys shall be avoided.

DES has proved to be a very well designed block cipher. There have been no significant cryptanalytic attacks on DES other than exhaustive key search.

3.4 Over view of Asymmetric key Cryptography:-

What is an Asymmetric Key or Asymmetric Key Cryptography?

Asymmetric keys are the foundation of Public Key Infrastructure (PKI) a cryptographic scheme requiring two different keys, one to lock or encrypt the plaintext and one to unlock or decrypt the cipher text. Neither key will do both functions. One key is published (public key) and the other is kept private (private key). If the lock/encryption key is the one published, the system enables private communication from the public to the unlocking key's owner. If the unlock/decryption key is the one published, then the system serves as a signature verifier of documents locked by the owner of the private key. This system also is called asymmetric key cryptography.

Asymmetric cryptography, also known as public-key cryptography, is a process that uses a pair of related keys -- one public key and one private key -- to encrypt and decrypt a message and protect it from unauthorized access or use. A public key is a cryptographic key that can be used by any person to encrypt a message so that it can only be deciphered by the intended recipient with their private key. A private key -- also known as a secret key -- is shared only with key's initiator.

3.5 The RSA Algorithm:-

RSA algorithm is a public key encryption technique and is considered as the most secure way of encryption. It was invented by Rivest, Shamir and Adleman in year 1978 and hence name **RSA** algorithm.

Algorithm

The RSA algorithm holds the following features −

RSA algorithm is a popular exponentiation in a finite field over integers including prime numbers.

The integers used by this method are sufficiently large making it difficult to solve.

There are two sets of keys in this algorithm: private key and public key.

You will have to go through the following steps to work on RSA algorithm −

Step 1: Generate the RSA modulus

The initial procedure begins with selection of two prime numbers namely p and q, and then calculating their product N, as shown −

N=p*q

Here, let N be the specified large number.

Step 2: Derived Number (e)

Consider number e as a derived number which should be greater than 1 and less than (p-1) and (q-1). The primary condition will be that there should be no common factor of (p-1) and (q-1) except 1

Step 3: Public key

The specified pair of numbers **n** and **e** forms the RSA public key and it is made public.

Step 4: Private Key

Private Key **d** is calculated from the numbers p, q and e. The mathematical relationship between the numbers is as follows −

ed = 1 mod (p-1) (q-1)

The above formula is the basic formula for Extended Euclidean Algorithm, which takes p and q as the input parameters.

Encryption Formula

Consider a sender who sends the plain text message to someone whose public key is **(n,e).** To encrypt the plain text message in the given scenario, use the following syntax −

C = Pe mod n

Decryption Formula

The decryption process is very straightforward and includes analytics for calculation in a systematic approach. Considering receiver **C** has the private key **d**, the result modulus will be calculated as −

Plaintext = Cd mod n

3.6 Symmetric & Asymmetric key cryptography

Symmetric encryption uses a single key that needs to be shared among the people who need to receive the message while asymmetrical encryption uses a pair of public key and a private key to encrypt and decrypt messages when communicating.

Difference between Symmetric and Asymmetric Encryption

Symmetric encryption uses a single key that needs to be shared among the people who need to receive the message while asymmetrical encryption uses a pair of public key and a private key to encrypt and decrypt messages when communicating.

Symmetric encryption is an old technique while asymmetric encryption is relatively new.

Asymmetric encryption was introduced to complement the inherent problem of the need to share the key in symmetrical encryption model, eliminating the need to share the key by using a pair of public-private keys.

Asymmetric encryption takes relatively more time than the symmetric encryption.

SYMMETRIC KEY ENCRYPTION	ASYMMETRIC KEY ENCRYPTION
It only requires a single key for both encryption and decryption.	It requires two key one to encrypt and the other one to decrypt.
The size of cipher text is same or smaller than the original plain text.	The size of cipher text is 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 amount of data.

SYMMETRIC KEY ENCRYPTION	ASYMMETRIC KEY ENCRYPTION
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

3.7 Digital Signature

Cryptography Digital signatures. ... **Digital signature** is a **cryptographic** value that is calculated from the data and a secret key known only by the signer. In real world, the receiver of message needs assurance that the message belongs to the sender and he should not be able to repudiate the origination of that message.

Digital signatures are the public-key primitives of message authentication. In the physical world, it is common to use handwritten signatures on handwritten or typed messages. They are used to bind signatory to the message.

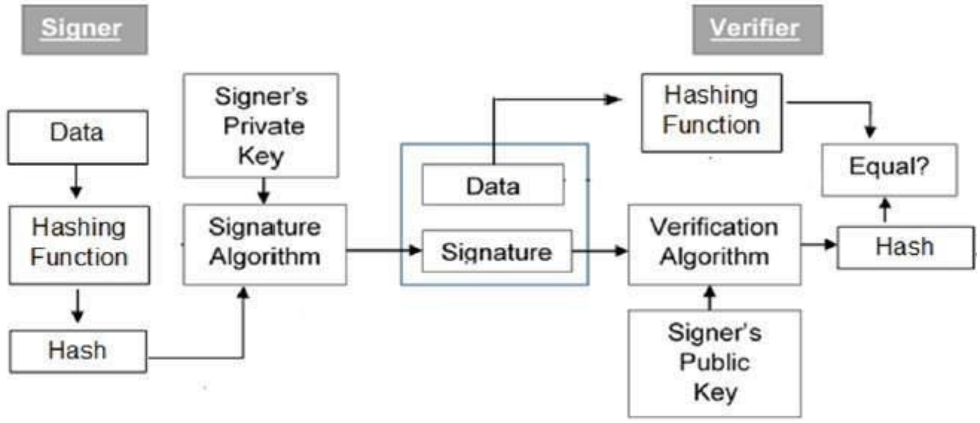
Similarly, a digital signature is a technique that binds a person/entity to the digital data. This binding can be independently verified by receiver as well as any third party.

Digital signature is a cryptographic value that is calculated from the data and a secret key known only by the signer.

In real world, the receiver of message needs assurance that the message belongs to the sender and he should not be able to repudiate the origination of that message. This requirement is very crucial in business applications, since likelihood of a dispute over exchanged data is very high.

Model of Digital Signature

As mentioned earlier, the digital signature scheme is based on public key cryptography. The model of digital signature scheme is depicted in the following illustration –



The following points explain the entire process in detail –

Each person adopting this scheme has a public-private key pair.

Generally, the key pairs used for encryption/decryption and signing/verifying are different. The private key used for signing is referred to as the signature key and the public key as the verification key.

Signer feeds data to the hash function and generates hash of data.

Hash value and signature key are then fed to the signature algorithm which produces the digital signature on given hash. Signature is appended to the data and then both are sent to the verifier.

Verifier feeds the digital signature and the verification key into the verification algorithm. The verification algorithm gives some value as output.

Verifier also runs same hash function on received data to generate hash value.

For verification, this hash value and output of verification algorithm are compared. Based on the comparison result, verifier decides whether the digital signature is valid.

Since digital signature is created by 'private' key of signer and no one else can have this key; the signer cannot repudiate signing the data in future.

It should be noticed that instead of signing data directly by signing algorithm, usually a hash of data is created. Since the hash of data is a unique representation of data, it is sufficient to sign the hash in place of data. The most important reason of using hash instead of data directly for signing is efficiency of the scheme.

Let us assume RSA is used as the signing algorithm. As discussed in public key encryption chapter, the encryption/signing process using RSA involves modular exponentiation.

Signing large data through modular exponentiation is computationally expensive and time consuming. The hash of the data is a relatively small digest of the data, hence **signing a hash is more efficient than signing the entire data**.

Importance of Digital Signature

Out of all cryptographic primitives, the digital signature using public key cryptography is considered as very important and useful tool to achieve information security.

Apart from ability to provide non-repudiation of message, the digital signature also provides message authentication and data integrity. Let us briefly see how this is achieved by the digital signature –

- **Message authentication** – When the verifier validates the digital signature using public key of a sender, he is assured that signature has been created only by sender who possess the corresponding secret private key and no one else.
- **Data Integrity** – In case an attacker has access to the data and modifies it, the digital signature verification at receiver end fails. The hash of modified data and the output provided by the verification algorithm will not match. Hence, receiver can safely deny the message assuming that data integrity has been breached.
- **Non-repudiation** – Since it is assumed that only the signer has the knowledge of the signature key, he can only create unique signature on a given data. Thus the receiver can present data and the digital signature to a third party as evidence if any dispute arises in the future.

By adding public-key encryption to digital signature scheme, we can create a cryptosystem that can provide the four essential elements of security namely − Privacy, Authentication, Integrity, and Non-repudiation.

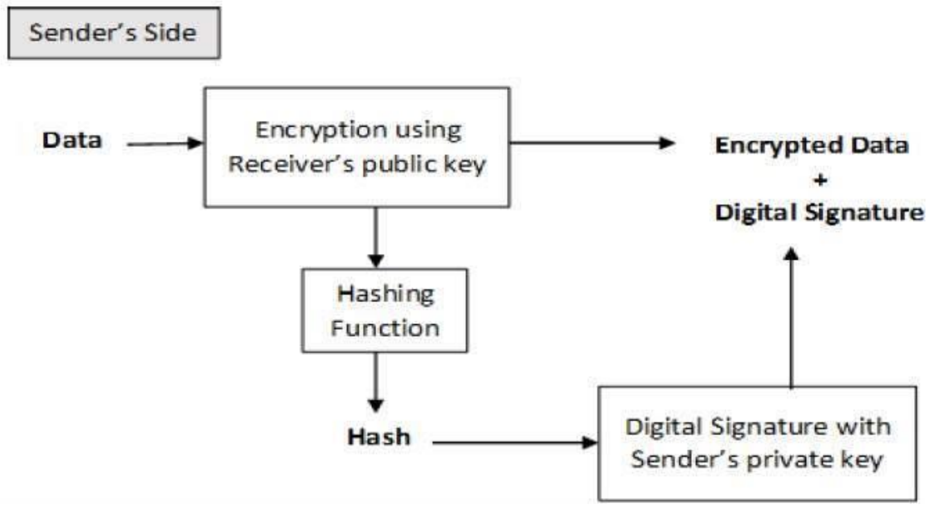
Encryption with Digital Signature

In many digital communications, it is desirable to exchange an encrypted message than plaintext to achieve confidentiality. In public key encryption scheme, a public (encryption) key of sender is available in open domain, and hence anyone can spoof his identity and send any encrypted message to the receiver.

This makes it essential for users employing PKC for encryption to seek digital signatures along with encrypted data to be assured of message authentication and non-repudiation.

This can archive by combining digital signatures with encryption scheme. Let us briefly discuss how to achieve this requirement. There are **two possibilities, sign-then-encrypt** and **encrypt-then-sign**.

However, the crypto system based on sign-then-encrypt can be exploited by receiver to spoof identity of sender and sent that data to third party. Hence, this method is not preferred. The process of encrypt-then-sign is more reliable and widely adopted. This is depicted in the following illustration −


Sender's Side
Data
Encryption using Receiver's public key
Encrypted Data
+
Digital Signature
Hashing Function
Hash
Digital Signature with Sender's private key

The receiver after receiving the encrypted data and signature on it, first verifies the signature using sender's public key. After ensuring the validity of the signature, he then retrieves the data through decryption using his private key.

MODEL QUESTIONS

<u>**Chapter-3**</u> **Symmetric & Asymmetric key algorithms:**

1. Define block cipher. (2)
2. Distinguish between block cipher and stream cipher. (2)
3. Data encryption standard (short note). (4)
4. Describe DES and explain the steps involve in DES. (10)
5. Describe DES and explain how DES works. (6)
6. State and explain RSA algorithm with suitable example. (10)
7. Write the difference between Symmetric key cryptography and Asymmetric key cryptography. (6)
8. Digital signature. (2)
9. Define digital signature, its technique apply for digital signature (10)

Chapter-4

Digital Certificate & Public key Infrastructure

4.1 Digital Certificate

Digital Certificate

For analogy, a certificate can be considered as the ID card issued to the person. People use ID cards such as a driver's license, passport to prove their identity. A digital certificate does the same basic thing in the electronic world, but with one difference.

Digital Certificates are not only issued to people but they can be issued to computers, software packages or anything else that need to prove the identity in the electronic world.

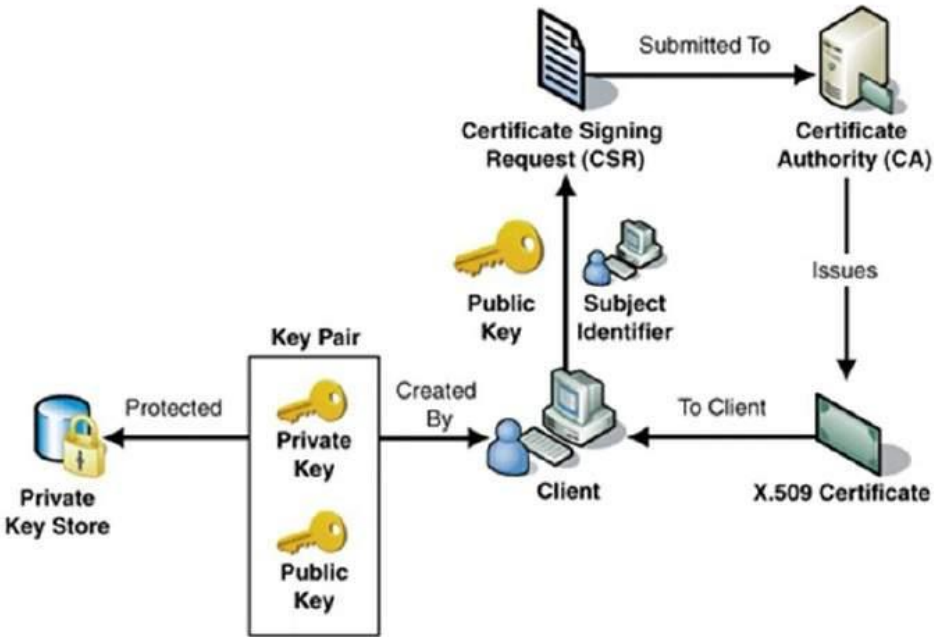
Digital certificates are based on the ITU standard X.509 which defines a standard certificate format for public key certificates and certification validation. Hence digital certificates are sometimes also referred to as X.509 certificates.

Public key pertaining to the user client is stored in digital certificates by The Certification Authority (CA) along with other relevant information such as client information, expiration date, usage, issuer etc.

CA digitally signs this entire information and includes digital signature in the certificate.

Anyone who needs the assurance about the public key and associated information of client, he carries out the signature validation process using CA’s public key. Successful validation assures that the public key given in the certificate belongs to the person whose details are given in the certificate.

The process of obtaining Digital Certificate by a person/entity is depicted in the following illustration.



As shown in the illustration, the CA accepts the application from a client to certify his public key. The CA, after duly verifying identity of client, issues a digital certificate to that client.

Certifying Authority (CA)

As discussed above, the CA issues certificate to a client and assist other users to verify the certificate. The CA takes responsibility for identifying correctly the identity of the client asking for a certificate to be issued, and ensures that the information contained within the certificate is correct and digitally signs it.

Key Functions of CA

The key functions of a CA are as follows −

Generating key pairs − The CA may generate a key pair independently or jointly with the client.

Issuing digital certificates − The CA could be thought of as the PKI equivalent of a passport agency − the CA issues a certificate after client provides the credentials to confirm his identity. The CA then signs the certificate to prevent modification of the details contained in the certificate.

Publishing Certificates − The CA need to publish certificates so that users can find them. There are two ways of achieving this. One is to publish certificates in the equivalent of an electronic telephone directory. The other is to send your certificate out to those people you think might need it by one means or another.

Verifying Certificates − The CA makes its public key available in environment to assist verification of his signature on clients' digital certificate.

Revocation of Certificates − At times, CA revokes the certificate issued due to some reason such as compromise of private key by user or loss of trust in the client. After revocation, CA maintains the list of all revoked certificate that is available to the environment.

Classes of Certificates

There are four typical classes of certificate −

Class 1 − These certificates can be easily acquired by supplying an email address.

Class 2 − These certificates require additional personal information to be supplied.

Class 3 − These certificates can only be purchased after checks have been made about the requestor's identity.

Class 4 − They may be used by governments and financial organizations needing very high levels of trust.

Registration Authority (RA)

CA may use a third-party Registration Authority (RA) to perform the necessary checks on the person or company requesting the certificate to confirm their identity. The RA may appear to the client as a CA, but they do not actually sign the certificate that is issued.

Certificate Management System (CMS)

It is the management system through which certificates are published, temporarily or permanently suspended, renewed, or revoked. Certificate management systems do not normally delete certificates because it may be necessary to prove their status at a point in time, perhaps for legal reasons. A CA along with associated RA runs certificate management systems to be able to track their responsibilities and liabilities.

Private Key Tokens

While the public key of a client is stored on the certificate, the associated secret private key can be stored on the key owner's computer. This method is generally not adopted. If an attacker gains access to the computer, he can easily gain access to private key. For this reason, a private key is stored on secure removable storage token access to which is protected through a password.

Different vendors often use different and sometimes proprietary storage formats for storing keys. For example, Entrust uses the proprietary .epf format, while Verisign, Global Sign, and Baltimore use the standard .p12 format.

4.2 Private Key management

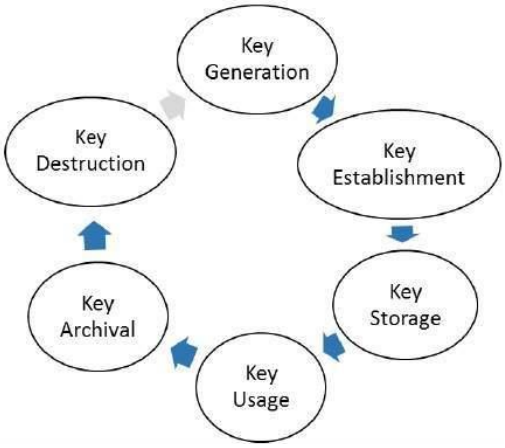
It goes without saying that the security of any cryptosystem depends upon how securely its keys are managed. Without secure procedures for the handling of cryptographic keys, the benefits of the use of strong cryptographic schemes are potentially lost.

It is observed that cryptographic schemes are rarely compromised through weaknesses in their design. However, they are often compromised through poor key management.

There are some important aspects of key management which are as follows –

Cryptographic keys are nothing but special pieces of data. Key management refers to the secure administration of cryptographic keys.

Key management deals with entire key lifecycle as depicted in the following illustration –



There are two specific requirements of key management for public key cryptography.

- **Secrecy of private keys.** Throughout the key lifecycle, secret keys must remain secret from all parties except those who are owner and are authorized to use them.
- **Assurance of public keys.** In public key cryptography, the public keys are in open domain and seen as public pieces of data. By default there are no assurances of whether a public key is correct, with whom it can be associated, or what it can be used for. Thus key management of public keys needs to focus much more explicitly on assurance of purpose of public keys.

The most crucial requirement of 'assurance of public key' can be achieved through the public-key infrastructure (PKI), a key management systems for supporting public-key cryptography.

4.3 PKIX Model

PKIX is an IETF (Internet Engineering Task Force) working group with the goal of supporting public key infrastructures based on X. 509 on the Internet. The working group has produced a number of Requests for Comments (RfC). These are often referred to as "**PKIX** standards."

Public Key Infrastructure (PKI)

PKI provides assurance of public key. It provides the identification of public keys and their distribution. An anatomy of PKI comprises of the following components.

Public Key Certificate commonly referred to as 'digital certificate'.

- Private Key tokens.
- Certification Authority.
- Registration Authority.
- Certificate Management System.

Public key infrastructure (**PKI**) **is used for:-**

A **public key infrastructure** (**PKI**) is a set of roles, policies, hardware, software and procedures needed to create, manage, distribute, **use**, store and revoke digital certificates and manage **public**-**key** encryption. ... In a Microsoft **PKI**, a registration authority is usually called a subordinate CA.

How does Public Key Infra structure works?

PKI (or **Public Key Infrastructure**) is the framework of encryption and cyber security that protects communications between the server (your website) and the client (the users). It works by using two different cryptographic keys: a public key and a private key. ... This protects the user's information from theft or tampering.

4.4 Public key Cryptography Standards

PKIX is an IETF (Internet Engineering Task Force) working group with the goal of supporting public key infrastructures based on X. 509 on the Internet. The working group has produced a number of Requests for Comments (RfC). These are often referred to as "**PKIX standards**."

In cryptography, **PKCS** stands for "Public Key Cryptography Standards". These are a group of **public-key cryptography standards** devised and published by RSA Security LLC, starting in the early 1990s. The company published the standards to promote the use of the cryptography techniques to which they had patents, such as the RSA algorithm, the Schnorr signature algorithm and several others. Though not industry standards (because the company retained control over them), some of the standards in recent years have begun to move into the "standards-track" processes of relevant standards organizations such as the IETF and the PKIX working-group.

PKCS Standards Summary			
	Version	**Name**	**Comments**
PKCS #1	2.2	RSA Cryptography Standard	See RFC 8017. Defines the mathematical properties and format of RSA public and private keys (ASN.1-encoded in clear-text), and the basic algorithms and encoding/padding schemes for performing RSA encryption, decryption, and producing and verifying signatures.
PKCS #2	-	Withdrawn	No longer active as of 2010. Covered RSA encryption of message digests; subsequently merged into PKCS #1.
PKCS #3	1.4	Diffie–Hellman Key Agreement Standard	A cryptographic protocol that allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel.
PKCS #4	-	Withdrawn	No longer active as of 2010. Covered RSA key syntax; subsequently merged into PKCS #1.
PKCS #5	2.1	Password-based Encryption Standard[	See RFC 8018 and PBKDF2.
PKCS #6	1.5	Extended-Certificate Syntax Standard[4]	Defines extensions to the old v1 X.509 certificate specification. Obsoletes by v3 of the same.
PKCS #7	1.5	Cryptographic Message Syntax Standard[5]	See RFC 2315. Used to sign and/or encrypt messages under a PKI. Used also for certificate dissemination (for instance as a response to a PKCS #10 message). Formed the basis for S/MIME, which is as of 2010 based on RFC 5652, an updated Cryptographic Message Syntax Standard (CMS). Often used for single sign-on.
PKCS #8	1.2	Private-Key Information Syntax Standard	See RFC 5958. Used to carry private certificate key pairs (encrypted or unencrypted).
PKCS #9	2.0	Selected Attribute Types	See RFC 2985. Defines selected attribute types for use in PKCS #6 extended certificates, PKCS #7 digitally signed messages, PKCS #8 private-key information, and PKCS #10 certificate-signing requests.
PKCS #10	1.7	Certification Request Standard	See RFC 2986. Format of messages sent to a certification authority to request certification of a public key. See certificate signing request.
PKCS #11	2.40	Cryptographic Token Interface	Also known as "Cryptoki". An API defining a generic interface to cryptographic tokens (see also hardware security module). Often used in single sign-on, public-key cryptography and disk encryption[10] systems. RSA Security has turned over further development of the PKCS #11 standard to the OASIS

			PKCS 11 Technical Committee.
PKCS #12	1.1	Personal Information Exchange Syntax Standard	See RFC 7292. Defines a file format commonly used to store private keys with accompanying public key certificates, protected with a password-based symmetric key. PFX is a predecessor to PKCS #12. This container format can contain multiple embedded objects, such as multiple certificates. Usually protected/encrypted with a password. Usable as a format for the Java key store and to establish client authentication certificates in Mozilla Firefox. Usable by Apache Tomcat.
PKCS #13	–	Elliptic Curve Cryptography Standard	*(Apparently abandoned, only reference is a proposal from 1998.)*
PKCS #14	–	Pseudo-random Number Generation	(Apparently abandoned, no documents exist.)
PKCS #15	1.1	Cryptographic Token Information Format Standard	Defines a standard allowing users of cryptographic tokens to identify themselves to applications, independent of the application's Cryptoki implementation (PKCS #11) or other API. RSA has relinquished IC-card-related parts of this standard to ISO/IEC 7816-15.[14]

MODEL QUESTIONS

Chapter-4 Digital certificate & public key infrastructure:

1. Digital Certificate. (2)
2. Who is the Certificate Authority? (2)
3. Explain the procedure for Digital Certificate creation. (10)
4. What do you mean by private key management? (2)
5. Explain the PKIA model. (6)
6. Explain the PKIA services. (6)
7. Explain different cryptography standard. (10)

Chapter-5

Internet Security Protocol

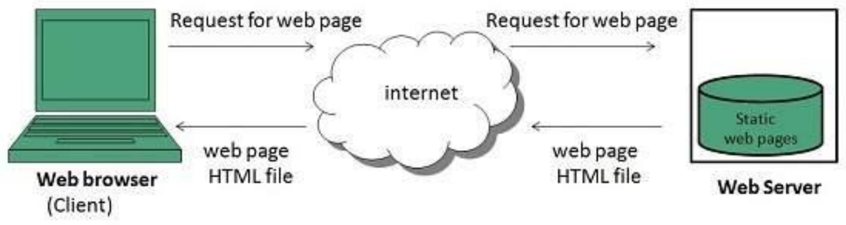
5.1 Basic concept

In computing, Internet Protocol Security (IPSec) is a secure network protocol suite that authenticates and encrypts the packets of data to provide secure encrypted communication between two computers over an Internet Protocol network. It is used in virtual private networks (VPNs).

Static Web page

Static web pages are also known as flat or stationary web page. They are loaded on the client's browser as exactly they are stored on the web server. Such web pages contain only static information. User can only read the information but can't do any modification or interact with the information.

Static web pages are created using only HTML. Static web pages are only used when the information is no more required to be modified.



Dynamic Web page

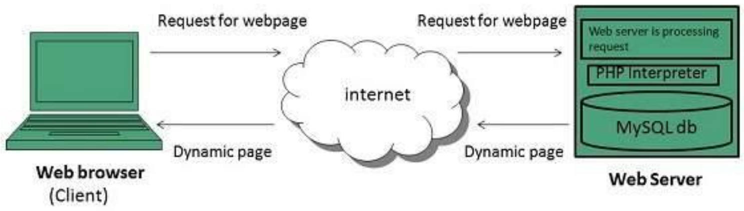
Dynamic web page shows different information at different point of time. It is possible to change a portion of a web page without loading the entire web page. It has been made possible using **Ajax** technology.

Server-side dynamic web page

It is created by using server-side scripting. There are server-side scripting parameters that determine how to assemble a new web page which also includes setting up of more client-side processing.

Client-side dynamic web page

It is processed using client side scripting such as JavaScript. And then passed in to **Document Object Model (DOM).**



A **static web page** (sometimes called a **flat page** or a **stationary page**) is a web page that is delivered to the user's web browser exactly as stored,[1] in contrast to dynamic web pages which are generated by a web application.

Consequently, a static web page displays the same information for all users, from all contexts, subject to modern capabilities of a web server to negotiate content-type or language of the document where such versions are available and the server is configured to do so

Advantages of a static website:-

- Provide improved security over dynamic websites (dynamic websites are at risk to web shell attacks if a vulnerability is present)
- Improved performance for end users compared to dynamic websites
- Fewer or no dependencies on systems such as databases or other application servers
- Cost savings from utilizing cloud storage, as opposed to a hosted environment

Disadvantages of a static website

- Dynamic functionality must be performed on the client side.

Active Web Page:-

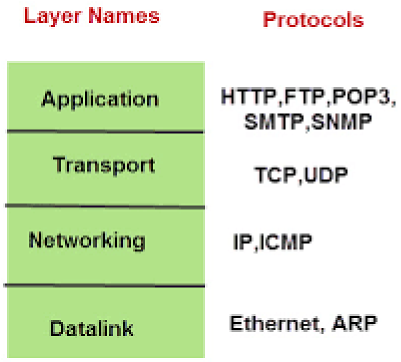
An **active web page** is a **page** where the browser performs the logic instead of the server. So for example when you've got a **page** where you're showing share prices, then you want it to update e.g. every 5 seconds. A solution would be to use AJAX with JavaScript.

Protocol:-

Network Protocols are a set of rules governing exchange of information in an easy, reliable and secure way.

TCP/IP:-

TCP/IP stands for **Transmission Control Protocol/Internet Protocol**. TCP/IP is a set of layered protocols used for communication over the Internet. The communication model of this suite is client-server model. A computer that sends a request is the client and a computer to which the request is sent is the server.



TCP/IP Networking Model

TCP/IP has four layers –

Application layer – Application layer protocols like HTTP and FTP are used.

Transport layer – Data is transmitted in form of datagrams using the Transmission Control Protocol (TCP). TCP is responsible for breaking up data at the client side and then reassembling it on the server side.

Network layer – Network layer connection is established using Internet Protocol (IP) at the network layer. Every machine connected to the Internet is assigned an address called IP address by the protocol to easily identify source and destination machines.

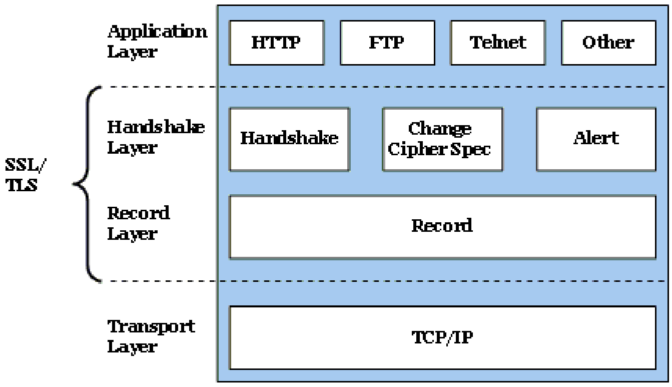
Data link layer – Actual data transmission in bits occurs at the data link layer using the destination address provided by network layer.

TCP/IP is widely used in many communication networks other than the Internet.

5.2 Secure Socket Layer:-

Secure Sockets Layer (**SSL**) is a protocol developed by Netscape for transmitting private documents via the Internet. **SSL** uses a cryptographic system that uses two keys to encrypt data – a public key known to everyone and a private or secret key known only to the recipient of the message..

SSL/TLS Protocol Layers



How SSL works?

As you learned in the previous chapter, https uses SSL protocol to secure the communication by transferring encrypted data. Before going deeper, learn how SSL works.

SSL fundamentally works with the following concepts:

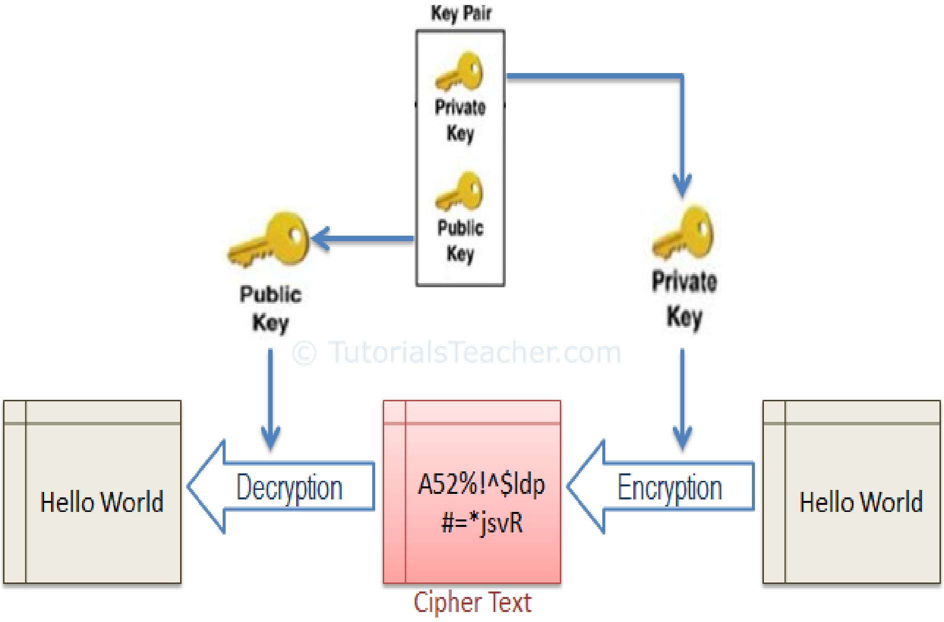
- Asymmetric Cryptography
- Symmetric Cryptography

Asymmetric Cryptography

Asymmetric cryptography (also known as Asymmetric Encryption or Public Key Cryptography) uses a mathematically-related key pair to encrypt and decrypt data. In a key pair, one key is shared with anyone who is interested in a communication. This is called **Public Key**. The other key in the key pair is kept secret and is called **Private Key**.

Here, the keys referred to a mathematical value and were created using a mathematical algorithm which encrypts or decrypts the data.

In the asymmetric cryptography, the data can be signed with a private key, which can only be decrypted using the related public key in a pair.

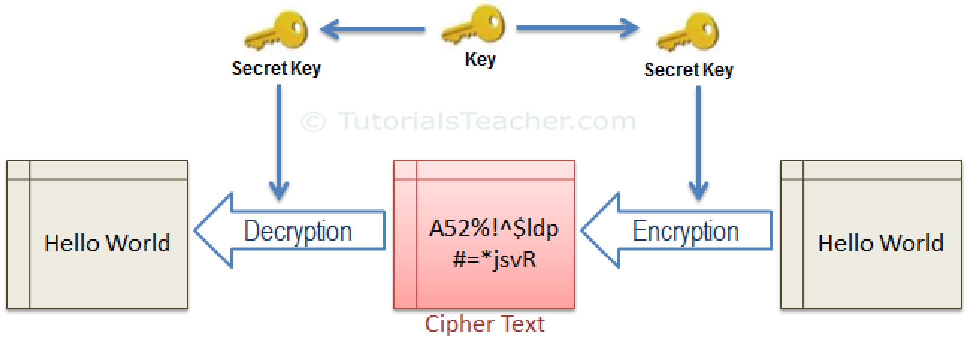


Asymmetric
Cryptography

SSL uses asymmetric cryptography to initiate the communication which is known as SSL handshake. Most commonly used asymmetric key encryption algorithms include EIGamal, RSA, DSA, Elliptic curve techniques and PKCS.

Symmetric Cryptography

In the symmetric cryptography, there is only one key which encrypts and decrypts the data. Both sender and receiver should have this key, which is only known to them.

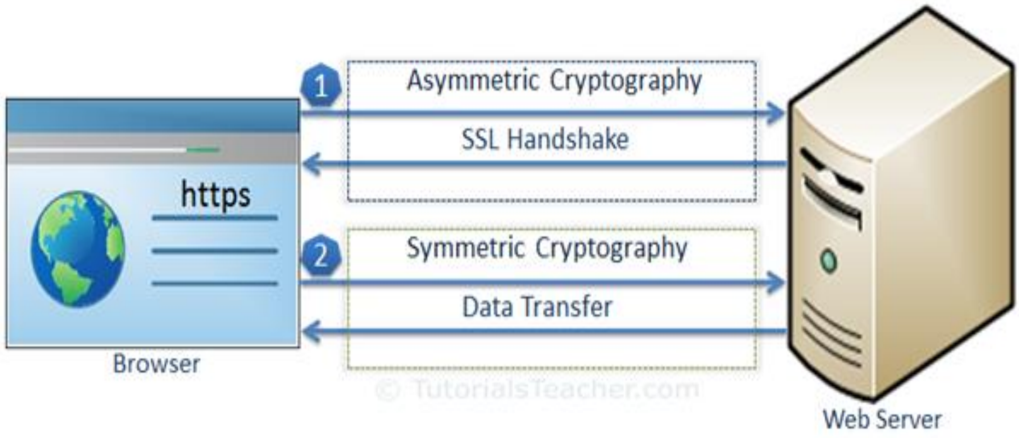


Symmetric Cryptography

SSL uses symmetric cryptography using the session key after the initial handshake is done. The most widely used symmetric algorithms are AES-128, AES-192 and AES-256.

Data Transfer over SSL

SSL protocol uses asymmetric and symmetric cryptography to transfer data securely. The following figure illustrates the steps of SSL communication:



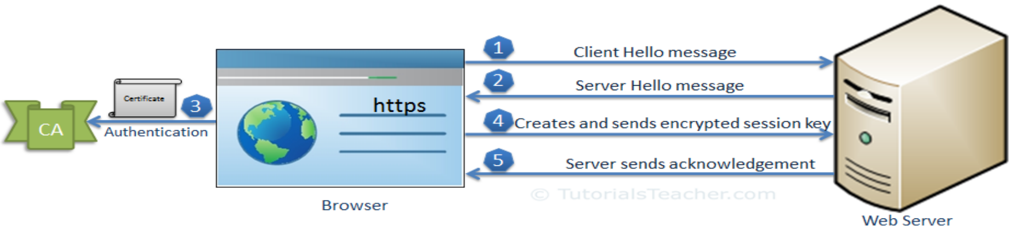
SSL Communication

As you can see in the above figure, SSL communication between the browser and the web server (or any other two systems) is mainly divided into two steps: the SSL handshake and the actual data transfer.

SSL Handshake

The communication over SSL always begins with the SSL handshake. The SSL handshake is an asymmetric cryptography which allows the browser to verify the web server, get the public key and establish a secure connection before the beginning of the actual data transfer.

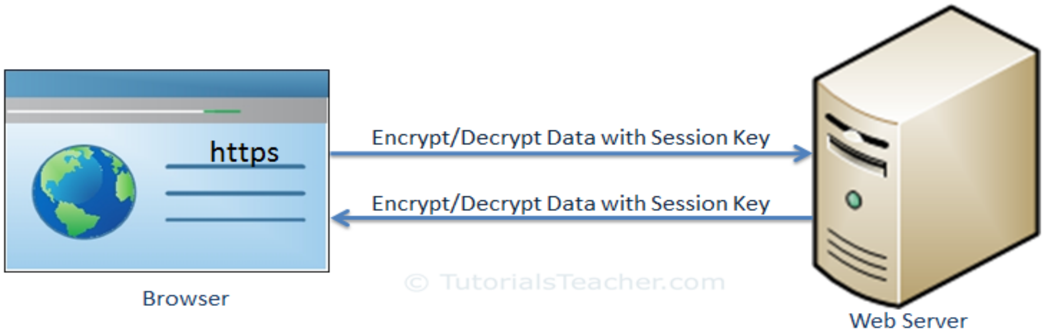
The following figure illustrates the steps involved in the SSL handshake:



SSL Handshake

Let's understand the above steps:

1. The client sends a "client hello" message. This includes the client's SSL version number, cipher settings, session-specific data and other information that the server needs to communicate with the client using SSL.
2. The server responds with a "server hello" message. This includes the server's SSL version number, cipher settings, session-specific data, an SSL certificate with a public key and other information that the client needs to communicate with the server over SSL.
3. The client verifies the server's SSL certificate from CA (Certificate Authority) and authenticates the server. If the authentication fails, then the client refuses the SSL connection and throws an exception. If the authentication succeeds, then proceed to step 4.
4. The client creates a session key, encrypts it with the server's public key and sends it to the server. If the server has requested client authentication (mostly in server to server communication), then the client sends his own certificate to the server.
5. The server decrypts the session key with its private key and sends the acknowledgement to the client encrypted with the session key.
6. Thus, at the end of the SSL handshake, both the client and the server have a valid session key which they will use to encrypt or decrypt actual data. The public key and the private key will not be used any more after this.
7. Actual Data Transfer
8. The client and the server now use a shared session key to encrypt and decrypt actual data and transfer it. This is done using the same session key at both ends and so, it is a symmetric cryptography. The actual SSL data transfer uses symmetric cryptography because it is easy and takes less CUP consumption compared with the asymmetric cryptography.


https
Encrypt/Decrypt Data with Session Key
Encrypt/Decrypt Data with Session Key
Browser
© TutorialsTeacher.com
Web Server

SSL Data Transfer

Thus, SSL fundamentally works using asymmetric cryptography and symmetric cryptography. There are certain infrastructures involved in achieving SSL communication in real life, which are called Public Key Infrastructure.

Public Key Infrastructure

The public key infrastructure (PKI) is a set of roles, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage public key encryption.

PKI includes the following elements:

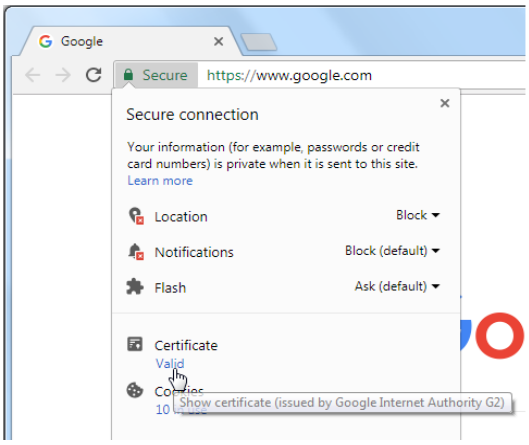
- Certificate Authority: The authority that authenticates the identity of individuals, computers and other entities.
- Registration Authority: A subordinate CA that issues a certificate on the behalf of root CA for specific uses.
- SSL Certificate: The Data file that includes the public key and other information.
- Certificate Management System: The system which stores, validates and revokes certificates.

What is the SSL Certificate?

The SSL certificate (also known as digital certificate) plays an important role in securing the communication between two systems.

The SSL certificate is a data file issued by the authorised Certificate Authority (CA). As you learned in the previous chapter, SSL uses asymmetric cryptography to establish an encrypted link between the two systems using a key pair (public key and private key). The SSL certificate contains the owner's public key and other details. The web server sends a public key to the browser through an SSL certificate and the browser verifies it and authenticates the web server using the SSL certificate.

You can open the certificate of any https website. For example, enter the url https://www.google.com in Google Chrome browser to check the SSL certificate of google.com. Any https website will have a padlock Secure in the address bar, as shown below.



https://www.google.com

Secure connection

Your information (for example, passwords or credit card numbers) is private when it is sent to this site.

Learn more

Location: Block

Notifications: Block (default)

Flash: Ask (default)

Certificate: Valid

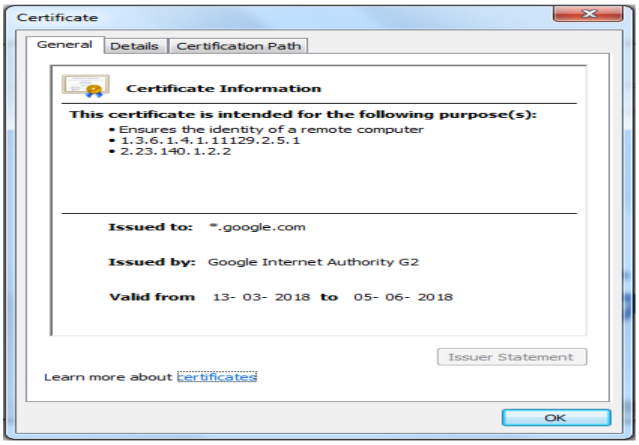
Cookies: 10

Show certificate (issued by Google Internet Authority G2)

Click on the padlock symbol and click on Certificate, as shown below.

SSL Certificate

This will open the certificate as shown below.



Certificate Information

This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer
- 1.3.6.1.4.1.11129.2.5.1
- 2.23.140.1.2.2

Issued to: *.google.com

Issued by: Google Internet Authority G2

Valid from 13- 03- 2018 to 05- 06- 2018

Learn more about certificates

SSL Certificate

As you can see, in the General tab, the certificate displays Issued to, Issued by and Valid from and to dates. The Details tab includes other information. The Certificate Path tab includes information about all the intermediate certificates and the root CA certificate.

How to Get an SSL Certificate?

You can get an SSL certificate from any authorized Certificate Authority (CA) to secure the communication between two systems. There are two ways to get an SSL certificate:

- Buy a certificate from CA
- Get a free certificate from a non-profit open CA

Should you buy an SSL certificate?

The decision of whether you should buy an SSL certificate depends on your need, whether you need a DV, an EV or an OV certificate. Also, do you need to secure a single domain, sub domains or multiple domains?

If you have an e-commerce web site, you gather user's information or you perform monetary transactions, then it is recommended to buy EV or OV certificates from a reputed CA. If you have a static website or you are not doing any monetary transactions, then you may use a free DV certificate. However, there is some hassle for renewing a free certificate every three months or so. So, it depends on what you can afford.

Buying an SSL Certificate

You can buy an SSL certificate from CA. The prices vary depending on the CA and type of the SSL certificate.

The following are overall steps for buying SSL certificates from a CA:

1. **Choose a Certificate Authority (CA):**
   You can choose your CA from where you want to buy an SSL certificate. There are many CAs such as Comodo, DigiCert, RapidSSL, GeoTrust, thawte, Certum etc. You may choose the CA based on your budget and the features you need to manage the certificate. There are resellers who provide cheap SSL certificates from these CAs. Visit https://www.thesslstore.com to buy cheap certificates from reputed CAs at one place.

2. **Select the certificate you need:**
   Once you select a CA, you can choose the certificate you require for your website based on the validation method and the number of web sites you want to secure.
3. **Purchase the certificate:**
   Once you choose the certificate you require, make the payment to proceed. For some CA, this step comes after submitting a CSR.
4. **Generate and submit a CSR (Certificate Signing Request) to the CA:**
   You need to generate a CSR from your web server and submit it to the CA. Learn more about what a CSR is and how to generate it in the next chapter.
5. **Download the SSL certificate (after successful validation):**
   After submitting a CSR, the CA will take some time for validating your information. This may vary based on the validation certificate you purchase. For a DV certificate, it should be quick. But, it will take a little longer to validate for an OV and an EV certificates. Once the CA successfully validates your information, you will get an email containing the certificate or you can download it from your account on the CA's website.
6. **Install an SSL certificate on your web server:**
   Once you get your SSL certificate, you need to install it on the web server from where you generated your CSR. The installation process depends on the OS of your server. Learn about it here.

5.3 Transport layer Security

Transport layer security (TLS) is a protocol that provides communication security between client/server applications that communicate with each other over the Internet. It enables privacy, integrity and protection for the data that's transmitted between different nodes on the Internet. TLS is a successor to the secure socket layer (SSL) protocol.

5.4 Secure hyper text transfer protocol (SHTTP)

S-HTTP (Secure HTTP) is an extension to the Hypertext Transfer Protocol (HTTP) that allows the secure exchange of files on the World Wide Web. Each S-HTTP file is either encrypted, contains a digital certificate, or both. For a given document, S-HTTP is an alternative to another well-known security protocol, Secure Sockets Layer (SSL). A major difference is that S-HTTP allows the client to send a certificate to authenticate the user whereas, using SSL, only the server can be authenticated. S-HTTP is more likely to be used in situations where the server represents a bank and requires authentication from the user that is more secure than a user id and password.

S-HTTP does not use any single encryption system, but it does support the Rivest-Shamir-Adelman public key infrastructure encryption system. SSL works at a program layer slightly higher than the Transmission Control Protocol (TCP) level. S-HTTP works at the even higher level of the HTTP application. Both security protocols can be used by a browser user, but only one can be used with a given document. Teresa Systems includes both SSL and S-HTTP in their Internet security tool kits.

5.5 Time stamping Protocol

The **Timestamp** Ordering **Protocol** is used to order the transactions based on their **Timestamps**. ... To determine the **timestamp** of the transaction, this **protocol** uses system **time** or logical counter. The lock-based **protocol** is used to manage the order between conflicting pairs among transactions at the execution **time**.

5.6 Secure Electronic Transaction (SET)

What Is Secure Electronic Transaction (SET)?

Secure electronic transaction (SET) was an early communications protocol used by e-commerce websites to secure electronic debit and credit card payments. Secure electronic transaction was used to facilitate the secure transmission of consumer card information via electronic portals on the Internet. Secure electronic transaction protocols were responsible for blocking out the personal details of card information, thus preventing merchants, hackers, and electronic thieves from accessing consumer information.

OR

Secure Electronic Transaction

It is a secure protocol developed by MasterCard and Visa in collaboration. Theoretically, it is the best security protocol. It has the following components −

1. **Card Holder's Digital Wallet Software** − Digital Wallet allows the card holder to make secure purchases online via point and click interface.
2. **Merchant Software** − This software helps merchants to communicate with potential customers and financial institutions in a secure manner.
3. **Payment Gateway Server Software** − Payment gateway provides automatic and standard payment process. It supports the process for merchant's certificate request.
4. **Certificate Authority Software** − This software is used by financial institutions to issue digital certificates to card holders and merchants, and to enable them to register their account agreements for secure electronic commerce.

Secure Electronic Transaction SET is an open encryption and security specification designed to protect credit card transactions on the Internet. The current version, SETv1, emerged from a call for security standards by MasterCard and Visa in February 1996. A wide range of companies were involved in developing the initial specification, including IBM, Microsoft, Netscape, RSA, Terisa, and Verisign. Beginning in 1996, there have been numerous tests of the concept, and by 1998 the first wave of SET-compliant products was available. SET is not itself a payment system. Rather it is a set of security protocols and formats that enables users to employ the existing credit card payment infrastructure on an open network, such as the Internet, in a secure fashion. In essence, SET provides three services:

- Provides a secure communications channel among all parties involved in a transaction
- Provides trust by the use of X.509v3 digital certificates
- Ensures privacy because the information is only available to parties in a transaction when and where necessary Book 1: Business Description (80 pages)
- Book 2: Programmer's Guide
- Book 3: Formal Protocol Definition (262 pages)

SET Overview

A good way to begin our discussion of SET is to look at the business requirements for SET, its key features, and the participants in SET transactions.

Requirements Book 1 of the SET specification lists the following business requirements for secure payment processing with credit cards over the Internet and other networks:

- Provide confidentiality of payment and ordering information: It is necessary to assure cardholders that this information is safe and accessible only to the intended recipient. Confidentiality also reduces the risk of fraud by either party to the transaction or by malicious third parties. SET uses encryption to provide confidentiality
- Ensure the integrity of all transmitted data: That is, ensure that no changes in content occur during transmission of SET messages. Digital signatures are used to provide integrity.
- Provide authentication that a cardholder is a legitimate user of a credit card account: A mechanism that links a cardholder to a specific account number reduces the incidence of fraud and the overall cost of payment processing. Digital signatures and certificates are used to verify that a cardholder is a legitimate user of a valid account.
- Provide authentication that a merchant can accept credit card transactions through its relationship with a financial institution: This is the complement to the preceding requirement. Cardholders need to be able to identify merchants with whom they can conduct secure transactions. Again, digital signatures and certificates are used.
- Ensure the use of the best security practices and system design techniques to protect all legitimate parties in an electronic commerce transaction: SET is a well-tested specification based on highly secure cryptographic algorithms and protocols.
- Create a protocol that neither depends on transport security mechanisms nor prevents their use: SET can securely operate over a "raw" TCP/IP stack. However, SET does not interfere with the use of other security mechanisms, such as IPSec and SSL/TLS.
- Facilitate and encourage interoperability among software and network providers: The SET protocols and formats are independent of hardware platform, operating system, and Web software.

Key Features of SET

To meet the requirements just outlined, SET incorporates the following features:

Confidentiality of information: Cardholder account and payment information is secured as it travels across the network. An interesting and important feature of SET is that it prevents the merchant from learning the cardholder's credit card number; this is only provided to the issuing bank. Conventional encryption by DES is used to provide confidentiality.

- **Integrity of data:** Payment information sent from cardholders to merchants includes order information, personal data, and payment instructions. SET guarantees that these message contents are not altered in transit. RSA digital signatures, using SHA-1 hash codes, provide message integrity. Certain messages are also protected by HMAC using SHA-1.
- **Cardholder account authentication**: SET enables merchants to verify that a cardholder is a legitimate user of a valid card account number. SET uses X.509v3 digital certificates with RSA signatures for this purpose.
- **Merchant authentication**: SET enables cardholders to verify that a merchant has a relationship with a financial institution allowing it to accept payment cards. SET uses X.509v3 digital certificates with RSA signatures for this purpose.

- Note that unlike IPSec and SSL/TLS, SET provides only one choice for each cryptographic algorithm.

This makes sense, because SET is a single application with a single set of requirements, where as IPSec and SSL/TLS are intended to support a range of applications.

SET Participants

The participants in the SET system, which include the following:

- **Cardholder:** In the electronic environment, consumers and corporate purchasers interact with merchants from personal computers over the Internet. A cardholder is an authorized holder of a payment card (e.g., MasterCard, Visa) that has been issued by an issuer.
- **Merchant:** A merchant is a person or organization that has goods or services to sell to the cardholder. Typically, these goods and services are offered via a Web site or by electronic mail. A merchant that accepts payment cards must have a relationship with an acquirer.
- Issuer: This is a financial institution, such as a bank, that provides the cardholder with the payment card. Typically, accounts are applied for and opened by mail or in person. Ultimately, it is the issuer that is responsible for the payment of the debt of the cardholder.
- **Acquirer:** This is a financial institution that establishes an account with a merchant and processes payment card authorizations and payments. Merchants will usually accept more than one credit card brand but do not want to deal with multiple bankcard associations or with multiple individual issuers. The acquirer provides authorization to the merchant that a given card accounts is active and that the proposed purchase does not exceed the credit limit. The acquirer also provides electronic transfer of payments to the merchant's account. Subsequently, the acquirer is reimbursed by the issuer over some sort of payment network for electronic funds transfer.
- **Payment gateway:** This is a function operated by the acquirer or a designated third party that processes merchant payment messages. The payment gateway interfaces between SET and the existing bankcard payment networks for authorization and payment functions. The merchant exchanges SET messages with the payment gateway over the Internet, while the payment gateway has some direct or network connection to the acquirer's financial processing system.
- **Certification authority (CA):** This is an entity that is trusted to issue X.509v3 public-key certificates for cardholders, merchants, and payment gateways. The success of SET will depend on the existence of a CA infrastructure available for this purpose. As was discussed in previous chapters, a hierarchy of CAs is used, so that participants need not be directly certified by a root authority.

Secure Electronic Commerce Processes--

We now briefly describe the sequence of events that are required for a transaction. We will then look at some of the cryptographic details.

- The customer opens an account. The customer obtains a credit card account, such as MasterCard or Visa, with a bank that supports electronic payment and SET.
- The customer receives a certificate. After suitable verification of identity, the customer receives an X.509v3 digital certificate, which is signed by the bank. The certificate verifies the customer's RSA public key and its expiration date. It also establishes a relationship, guaranteed by the bank, between the customer's key pair and his or her credit card.

- Merchants have their own certificates. A merchant who accepts a certain brand of card must be in possession of two certificates for two public keys owned by the merchant: one for signing messages, and one for key exchange. The merchant also needs a copy of the payment gateway's public-key certificate.
- The customer places an order. This is a process that may involve the customer first browsing through the merchant's Web site to select items and determine the price. The customer then sends a list of the items to be purchased to the merchant, who returns an order form containing the list of items, their price, a total price, and an order number.
- The merchant is verified. In addition to the order form, the merchant sends a copy of its certificate, so that the customer can verify that he or she is dealing with a valid store.
- The order and payment are sent. The customer sends both order and payment information to the merchant, along with the customer's certificate. The order confirms the purchase of the items in the order form. The payment contains credit card details. The payment information is encrypted in such a way that it cannot be read by the merchant. The customer's certificate enables the merchant to verify the customer.
- The merchant requests payment authorization. The merchant sends the payment information to the payment gateway, requesting authorization that the customer's available credit is sufficient for this purchase.
- The merchant confirms the order. The merchant sends confirmation of the order to the customer.
- The merchant provides the goods or service. The merchant ships the goods or provides the service to the customer. 10. The merchant requests payment. This request is sent to the payment gateway, which handles all of the payment

Payment Processing:-

Lists the transaction types supported by SET. In what follows we look in some detail at the following transactions:

- Purchase request
- Payment authorization
- Payment capture

SET Transaction Types

- Cardholder registration:-Cardholders must register with aCA before they can send SET messages to merchants.
- Merchant registration:- Merchants must register with a CA before they can exchange SET messages with customers and payment gateways.
- Purchase request Message:-from customer to merchant containing OI for merchant and PI for bank.
- Payment authorization:- Exchange between merchant and payment gateway to authorize a given amount for a purchase on a given credit card account.
- Payment capture:- Allows the merchant to request payment from the payment gateway.
- Certificate inquiry :-and status If the CA is unable to complete the processing of a certificate request quickly, it will send a reply to the cardholder or merchant indicating that the requester should check back later. The cardholder or merchant sends the

Certificate Inquiry message to determine the status of the certificate request and to receive the certificate if the request has been approved.

- Purchase inquiry:- Allows the cardholder to check the status of the processing of an order after the purchase response has been received. Note that this message does not include information such as the status of back ordered goods, but does indicate the status of authorization, capture and credit processing.
- Authorization:-reversal Allows a merchant to correct previous authorization requests. If the order will not be completed, the merchant reverses the entire authorization. If part of the order will not be completed (such as when goods are back ordered), the merchant reverses part of the amount of the authorization.
- Capture reversal:-Allows a merchant to correct errors in capture requests such as transaction amounts that were entered incorrectly by a clerk.
- Credit: - Allows a merchant to issue a credit to a cardholder's account such as when goods are returned or were damaged during shipping. Note that the SET Credit message is always initiated by the merchant, not the cardholder. All communications between the cardholder and merchant that result in a credit being processed happen outside of SET.
- Credit reversal:- Allows a merchant to correct a previously request credit.
- Payment gateway:-certificate request Allows a merchant to query the payment gateway and receive a copy of the gateway's current key-exchange and signature certificates.
- Batch administration:- Allows a merchant to communicate information to the payment gateway regarding merchant batches.
- Error message indicates that a responder rejects a message because it fails format or content verification tests.

Payment Authorization--

During the processing of an order from a cardholder, the merchant authorizes the transaction with the payment gateway. The payment authorization ensures that the transaction was approved by the issuer. This authorization guarantees that the merchant will receive payment; the merchant can therefore provide the services or goods to the customer. The payment authorization exchange consists of two messages: Authorization Request and Authorization response.

The merchant sends an Authorization Request message to the payment gateway consisting of the following:

1. Purchase-related information. This information was obtained from the customer and consists of –

--The PI - The dual signature, calculated over the PI and OI, signed with the customer's private signature key –

--The OI message digests (OIMD) –

--The digital envelope

2. Authorization-related information. This information is generated by the merchant and consists of –

--An authorization block that includes the transaction ID, signed with the merchant's private signature key and encrypted with a one-time symmetric key generated by the merchant

--A digital envelope. This is formed by encrypting the one-time key with the payment gateway's public key-exchange key.

3. Certificates. The merchant includes the cardholder's signature key certificate (used to verify the dual signature), the merchant's signature key certificate (used to verify the merchant's signature), and the merchant's key-exchange certificate (needed in the payment gateway's response).

The payment gateway performs the following tasks:

1. Verifies all certificates

2. Decrypts the digital envelope of the authorization block to obtain the symmetric key and then decrypts the authorization block

3. Verifies the merchant's signature on the authorization block

4. Decrypts the digital envelope of the payment block to obtain the symmetric key and then decrypts the payment block

5. Verifies the dual signature on the payment block

6. Verifies that the transaction ID received from the merchant matches that in the PI received (indirectly) from the customer

7. Requests and receives an authorization from the issuer

Having obtained authorization from the issuer, the payment gateway returns an Authorization Response message to the merchant. It includes the following elements:

1. Authorization-related information. Includes an authorization block, signed with the gateway's private signature key and encrypted with a one-time symmetric key generated by the gateway. Also includes a digital envelope that contains the one-time key encrypted with the merchant’s public key-exchange key.

2. Capture token information. This information will be used to effect payment later. This block is of the same form as (1), namely, a signed, encrypted capture token together with a digital envelope. This token is not processed by the merchant. Rather, it must be returned, as is, with a payment request.

3. Certificate. The gateway's signature key certificate.

With the authorization from the gateway, the merchant can provide the goods or service to the customer.

Payment Capture--

To obtain payment, the merchant engages the payment gateway in a payment capture transaction, consisting of a capture request and a capture response message.

For the Capture Request message, the merchant generates, signs, and encrypts a capture request block, which includes the payment amount and the transaction ID. The message also includes the encrypted capture token received earlier (in the Authorization Response) for this transaction, as well as the merchant's signature key and key-exchange key certificates.

When the payment gateway receives the capture request message, it decrypts and verifies the capture request block and decrypts and verifies the capture token block. It then checks for consistency between the capture request and capture token. It then creates a clearing request that is sent to the issuer over the private payment network. This request causes funds to be transferred to the merchant's account.

The gateway then notifies the merchant of payment in a Capture Response message. The message includes a capture response block that the gateway signs and encrypts. The message also includes the gateway's signature key certificate. The merchant software stores the capture response to be used for reconciliation with payment received from the acquirer.

MODEL QUESTIONS

Chapter-5 Internet security protocol

1. Explain SSL & Explain how it works. (10)
2. Describe SSL position in TCP/IP protocol. (6)
3. Explain Secure Hyper Text Transfer Protocol. (10)
4. Write short note on (4)
    A. Transport protocol.
    B. Time stamping protocol.
    C. Secure hyper text protocol.
    D. Transport layer protocol.
5. What is secure electronic transaction? Describe the process involve in SET. (10)
6. Write the difference between Static Web page and Dynamic Web page? (2)
7. What is Active Web page? (2)
8. Write the difference between SSL and TSL. (2)
9. What is secure electronic transaction? Explain SET participation. (6)

Chapter-6

User Authentication

6.1 Authentication basics

User authentication, the most important methods involve cryptographic keys and some- thing the individual knows, such as a password. ... To prevent masquerade and to prevent compromise of session keys, essential identification and session-key information must be communicated in encrypted form.

A security token (sometimes called an authentication token) is a small hardware device that the owner carries to authorize access to a network service. The device may be in the form of a smart card or may be embedded in a commonly used object such as a key fob.

6.2 Password:

A **password** is a string of characters used for authenticating a user on a **computer** system. For example, you may have an account on your **computer** that requires you to log in. ... Most **passwords** are comprised of several characters, which can typically include letters, numbers, and most symbols, but not spaces.

Clear text password:-

The password is stored in clear text in user database against the user id on the server. The authentication mechanism works as follows:

- Prompt for user id and password.
- User enters user id and password.
- User id and password validation.
- Authentication Result.
- Inform user accordingly**.**

6.3 Authentication Token

An Authentication Token is an extremely useful alternative to password. An Authentication Token is a small device the generates a new random value every time. This random value becomes the basis for authentication. Usually an Authentication Token ha following features:

- Processor
- Liquid Crystal Display (LCD) for displaying output.
- Battery
- A small keypad for entering information
- Areal-time clock

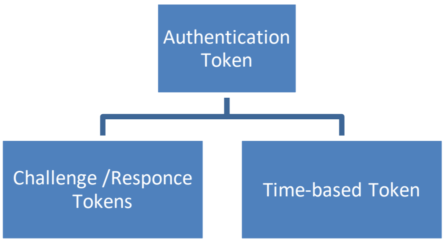
Each Authentication Token is programmed with unique number called as a **random seed**.

How does it work?

- Creation of a token
- Use of token
- Serve returns an appropriate message back to the user.

Authentication Token Types:-

There are two main types of Authentication Tokens



Challenge/Response Token:-

Challenge-response authentication uses a **cryptographic** protocol that allows to prove that the user knows the password without revealing the password itself. Using this method, the application first obtains a random **challenge** from the server.

How challenge-response authentication works

When a user attempts to log onto a system or network resource, the challenge-response system server generates a challenge, usually a random number that is then sent to the client machine.

The client software uses a secret key, or a key based on its password, to encrypt the challenge data using an encryption algorithm or one-way hash function. It then sends the result back to the network server.

The challenge-response authentication system performs the same cryptographic process on the challenge, comparing its result to the response from the client. If the two values match, the authentication system is able to authenticate the client.

There are two types of challenge questions: static and dynamic.

Static questions enable the user to choose from a bank of predefined questions or allow the user to create custom challenge questions. The user then provides the answers to the challenge questions he has selected. For example, a static challenge might be to provide the name of the user's first pet, first car or first-grade teacher -- the correct values will not change over time, and the user can specify the correct values as part of their account setup.

Dynamic questions are created by extracting public data about the user that the individual should know, such as a previous street address or the make and model of a previous vehicle. The system presents the user with random questions and answers that utilize this data from which the user must select the correct answer.

Challenge-response authentication can defend against session replay attacks, in which an attacker listens to previous messages and resends them later to get the same credentials as the original message. Challenge-response systems defend against replay attacks, because each challenge and response is unique. An attacker monitoring credentials exchanges and then attempting to reuse credentials will not succeed in gaining access.

Some types of challenge-response systems can help defend against man-in-the-middle attacks, particularly when the challenge and response requires some knowledge to which the attacker does not have access. For example, challenge and response values that are digitally signed by an endpoint using a private key, or that depend on any other data that has not been compromised by an attacker, should protect the endpoint from a man-in-the-middle attack.

Time-based Token:-

Time-**based** One-**Time** Password (TOTP) is a single-use pass code typically used for authenticating users. The user is assigned a TOPT generator delivered as a hardware key fob or software **token**.

OR

A **time**-**based token** exists between the client's **token** and the authentication server, which changes constantly at a set **time** interval, e.g. once per minute.

The process work as follows:-

- Password generation and login request
- Server-side verification
- Severer return an appropriate message back to the user.

6.4 Certificate based Authentication

A certificate-based authentication scheme is a scheme that uses a public key cryptography and digital certificate to authenticate a user. ... The server then confirms the validity of the digital signature and if the certificate has been issued by a trusted certificate authority or not.

How does Certificate –based Authentication Work?

- Creation and distribution of digital certificates
- Login request
- Server creates a random challenge
- User signs the random challenge
- Server returns an appropriate message back to the user.

Use of smart card:-

Smart cards can provide personal identification, authentication, data storage, and **application** processing. Applications include identification, financial, mobile phones (SIM), public transit, computer security, schools, and healthcare.

OR

Smart cards can provide personal identification, authentication, data storage, and **application** processing. Applications include identification, financial, mobile phones (SIM), public transit, computer security, schools, and healthcare.

6.5 Biometric Authentication

A biometric authentication is a digitizing measurement of a physiological or behavioural characteristic for human. Biometric authentication systems can theoretically be used to distinguish one person from. However, many biometric authentication systems have been proposed which are categorized as; face detection authentication system, finger print authentication system, Iris authentication system, and voice authentication system.

MODEL QUESTIONS

Chapter-6 User Authentication

1. What is Password? (2)
2. What is clear Text password? How it works? (6)
3. Explain the different type of Authentication Token. (10)
4. Explain how Certificate Based Authentication works? (6)
5. Smart card (short note). (4)
6. What do you mean by Biometric authentication? How does it work? (6)
7. Biometric authentication (short note) (4)
8. Define biometric authentication .Explain its working principle ` (6)
9. What is the use of Smart Card? Give example. (2)

Chapter-7

Network Security & VPN

7.1 Brief Introduction to TCP/IP

What is TCP/IP?

- TCP/IP is the communication protocol for communication between computers on the Internet.
- TCP/IP stands for **T**ransmission **C**ontrol **P**rotocol / **I**nternet **P**rotocol.
- TCP/IP defines how electronic devices (like computers) should be connected to the Internet, and how data should be transmitted between them.

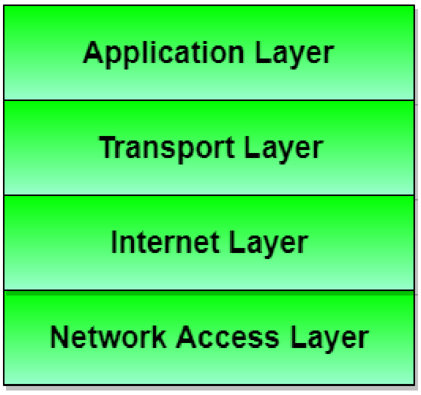
Inside TCP/IP

Inside the TCP/IP standard there are several protocols for handling data communication:

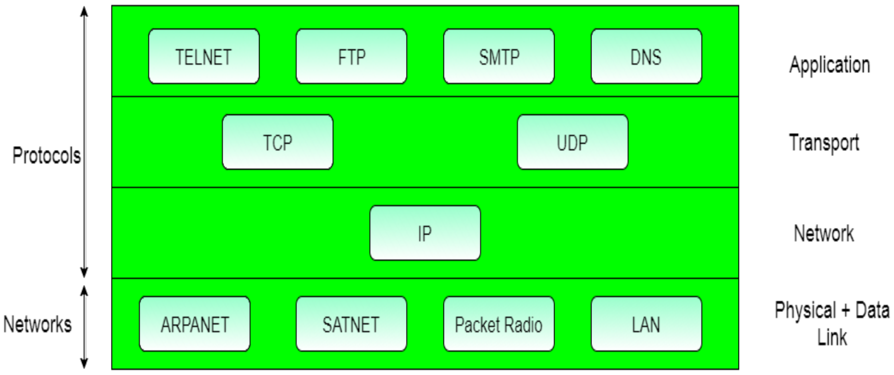
- ✓ TCP (Transmission Control Protocol) communication between applications
- ✓ UDP (User Datagram Protocol) simple communication between applications
- ✓ IP (Internet Protocol) communication between computers
- ✓ ICMP (Internet Control Message Protocol) for errors and statistics
- ✓ DHCP (Dynamic Host Configuration Protocol) for dynamic addressing

The TCP/IP Reference Model

TCP/IP means Transmission Control Protocol and Internet Protocol. It is the network model used in the current Internet architecture as well. **Protocols** are set of rules which govern every possible communication over a network. These protocols describe the movement of data between the source and destination or the internet. They also offer simple naming and addressing schemes.



Protocols and networks in the TCP/IP model:



Overview of TCP/IP reference model

TCP/IP that is Transmission Control Protocol and Internet Protocol was developed by Department of **Defence's Project Research Agency** (ARPA, later DARPA) as a part of a research project of network interconnection to connect remote machines.

The features that stood out during the research, which led to making the TCP/IP reference model were:

Support for a flexible architecture. Adding more machines to a network was easy.

The network was robust, and connections remained intact untill the source and destination machines were functioning.

The overall idea was to allow one application on one computer to talk to(send data packets) another application running on different computer

Different Layers of TCP/IP Reference Model

Below we have discussed the 4 layers that form the TCP/IP reference model:

Layer 1: Host-to-network Layer

- Lowest layer of the all.
- Protocol is used to connect to the host, so that the packets can be sent over it.
- Varies from host to host and network to network.

Layer 2: Internet layer

- Selection of a packet switching network which is based on a connectionless internetwork layer is called a internet layer.
- It is the layer which holds the whole architecture together.
- It helps the packet to travel independently to the destination.
- Order in which packets are received is different from the way they are sent.
- IP (Internet Protocol) is used in this layer.
- The various functions performed by the Internet Layer are:
- Delivering IP packets
- Performing routing
- Avoiding congestion

Layer 3: Transport Layer

- It decides if data transmission should be on parallel path or single path.
- Functions such as multiplexing, segmenting or splitting on the data is done by transport layer.
- The applications can read and write to the transport layer.
- Transport layer adds header information to the data.
- Transport layer breaks the message (data) into small units so that they are handled more efficiently by the network layer.
- Transport layer also arrange the packets to be sent, in sequence.

Layer 4: Application Layer

- The TCP/IP specifications described a lot of applications that were at the top of the protocol stack. Some of them were TELNET, FTP, SMTP, DNS etc.
- TELNET is a two-way communication protocol which allows connecting to a remote machine and run applications on it.
- FTP(File Transfer Protocol) is a protocol, that allows File transfer amongst computer users connected over a network. It is reliable, simple and efficient.
- SMTP(Simple Mail Transport Protocol) is a protocol, which is used to transport electronic mail between a source and destination, directed via a route.
- DNS(Domain Name Server) resolves an IP address into a textual address for Hosts connected over a network.
- It allows peer entities to carry conversation.
- It defines two end-to-end protocols: TCP and UDP
- TCP(Transmission Control Protocol): It is a reliable connection-oriented protocol which handles byte-stream from source to destination without error and flow control.
- UDP(User-Datagram Protocol): It is an unreliable connection-less protocol that do not want TCPs, sequencing and flow control. Eg: One-shot request-reply kind of service.

Merits of TCP/IP model

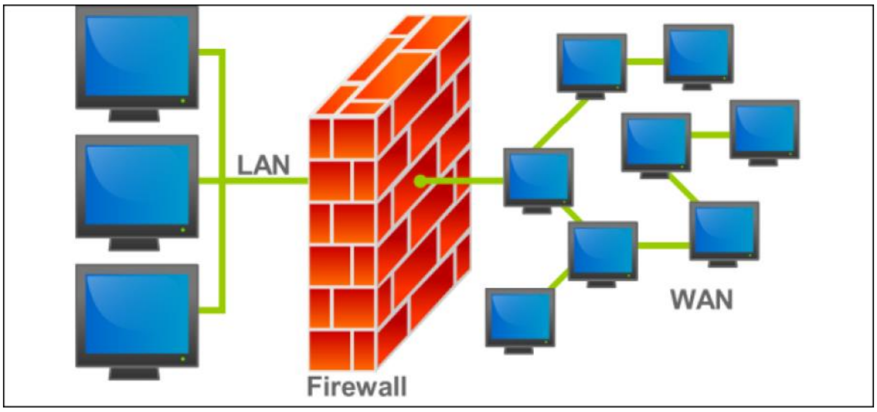
- It operated independently.
- It is scalable.
- Client/server architecture.
- Supports a number of routing protocols.
- Can be used to establish a connection between two computer

Demerits of TCP/IP

- In this, the transport layer does not guarantee delivery of packets.
- The model cannot be used in any other application.
- Replacing protocol is not easy.
- It has not clearly separated its services, interfaces and protocols.

7.2 Firewall

A firewall is a system designed to prevent unauthorized access to or from a private network. You can implement a firewall in either hardware or software form, or a combination of both. Firewalls prevent unauthorized internet users from accessing private networks connected to the internet, especially intranets.



How Firewall Works

Firewall match the network traffic against the rule set defined in its table. Once the rule is matched, associate action is applied to the network traffic.

For example, Rules are defined as any employee from HR department cannot access the data from code server and at the same time another rule is defined like system administrator can access the data from both HR and technical department.

Rules can be defined on the firewall based on the necessity and security policies of the organization. From the perspective of a server, network traffic can be either outgoing or incoming. Firewall maintains a distinct set of rules for both the cases. Mostly the outgoing traffic, originated from the server itself, allowed to pass.
Still, setting a rule on outgoing traffic is always better in order to achieve more security and prevent unwanted communication.

Incoming traffic is treated differently. Most traffic which reaches on the firewall is one of these three major Transport Layer protocols- TCP, UDP or ICMP. All these types have a source address and destination address. Also, TCP and UDP have port numbers. ICMP uses *type code* instead of port number which identifies purpose of that packet.

Firewalls can be categorized based on its generation.

1. **First Generation- Packet Filtering Firewall :** Packet filtering firewall is used to control network access by monitoring outgoing and incoming packet and allowing them to pass or stop based on source and destination IP address, protocols and ports. It analyses traffic at the transport protocol layer (but mainly uses first 3 layers). Packet firewalls treat each packet in isolation. They have no ability to tell whether a packet is part of an existing stream of traffic. Only It can allow or deny the packets based on unique packet headers.

2. **Second Generation- Stateful Inspection Firewall :** Stateful firewalls (performs Stateful Packet Inspection) are able to determine the connection state of packet, unlike Packet filtering firewall, which makes it more efficient. It keeps track of the state of networks connection travelling across it, such as TCP streams. So the filtering decisions would not only be based on defined rules, but also on packet's history in the state table.
3. **Third Generation- Application Layer Firewall :** Application layer firewall can inspect and filter the packets on any OSI layer, up to the application layer. It has the ability to block specific content, also recognize when certain application and protocols (like HTTP, FTP) are being misused.

In other words, Application layer firewalls are hosts that run proxy servers. A proxy firewall prevents the direct connection between either side of the firewall, each packet has to pass through the proxy. It can allow or block the traffic based on predefined rules.

4. **Next Generation Firewalls (NGFW) :** Next Generation Firewalls are being deployed these days to stop modern security breaches like advance malware attacks and application-layer attacks. NGFW consists of Deep Packet Inspection, Application Inspection, SSL/SSH inspection and many functionalities to protect the network from these modern threats.

Types of Firewall

Firewalls are generally of two types: *Host-based* and *Network-based.*

1. **Host- based Firewalls :** Host-based firewall is installed on each network node which controls each incoming and outgoing packet. It is a software application or suite of applications, comes as a part of the operating system. Host-based firewalls are needed because network firewalls cannot provide protection inside a trusted network. Host firewall protects each host from attacks and unauthorized access.
2. **Network-based Firewalls:** Network firewall function on network level. In other words, these firewalls filter all incoming and outgoing traffic across the network. It protects the internal network by filtering the traffic using rules defined on the firewall. A Network firewall might have two or more network interface cards (NICs). A network-based firewall is usually a dedicated system with proprietary software installed.

7.3 IP Security

The **IP security** (IPSec) is an Internet Engineering Task Force (IETF) standard suite of protocols between 2 communication points across the **IP** network that provide data authentication, integrity, and confidentiality. It also defines the encrypted, decrypted and authenticated packets.

Benefits of IPSe:-.

Good compatibility. You can apply IPSec to all **IP**-based application systems and services without modifying them. Encryption on a per-packet rather than per-flow basis. Per-packet encryption allows for flexibility and greatly enhances **IP security**.

IP Sec Overview:-

Application s is as follows:-

- Secure remote Internet access
- Secure branch office connectivity
- Set up communication with other organizations**.**

7.4 Virtual private Network (VPN)

A **virtual private network** (**VPN**) is a **network** that is constructed using public wires — usually the internet — to connect remote users or regional offices to a company's **private**, **internal network**.

What Is a VPN?

A virtual private network, or VPN, is an encrypted connection over the Internet from a device to a network. The encrypted connection helps ensure that sensitive data is safely transmitted. It prevents unauthorized people from eavesdropping on the traffic and allows the user to conduct work remotely. VPN technology is widely used in corporate environments**.**

How does a virtual private network (VPN) work?

At its most basic level, VPN tunnelling creates a point-to-point connection that cannot be accessed by unauthorized users. To actually create the VPN tunnel, the endpoint device needs to be running a VPN client (software application) locally or in the cloud. The VPN client runs in the background and is not noticeable to the end user unless there are performance issues.

The performance of a VPN can be affected by a variety of factors, among them the speed of users' internet connections, the types of protocols an internet service provider may use and the type of encryption the VPN uses. In the enterprise, performance can also be affected by poor quality of service (QoS) outside the control of an organization's information technology (IT) department.

OR

A VPN extends a corporate network through encrypted connections made over the Internet. Because the traffic is encrypted between the device and the network, traffic remains private as it travels. An employee can work outside the office and still securely connect to the corporate network. Even smart phones and tablets can connect through a VPN.

Why do I need a VPN?

- **Hide your IP address**

  Connecting to a Virtual Private Network often conceals your real IP address.
- **Change your IP address**

  Using a VPN will almost certainly result in getting a different IP address.
- **Encrypt data transfers**

  A Virtual Private Network will protect the data you transfer over public WiFi.
- **Mask your location**

  With a Virtual Private Network, users can choose the country of origin for their Internet connection.
- **Access blocked websites**

  Access government blocked websites with VPN.

MODEL QUESTIONS

Chapter-7 Network Security & VPN

1. Define TCP/IP. (2)
2. Explain the header field between TCP Server. (6)
3. What do you mean by IP Datagram? (2)

4. Define Firewall. (2)
5. Define Firewall. Explain different types of Firewall. (10)
6. Describe the application and advantages of IP security. (10)
7. Define IP Security. (2)
8. Short notes (4)
    - TCPI/IP
    - VPN

9. Explain the working principle of VPN. (6)

10. What are advantages of IPSec? (6)