ICS Mid I Answer Key

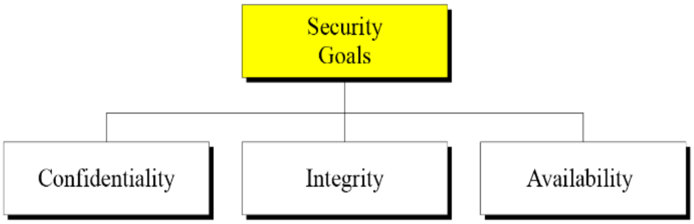
Part A

1. a . state the principles of information Security?
   There are three security principles.

❑ Confidentiality

❑ Integrity

❑ Availability



b. Illustrate the difference between Threat and Attack?

A Threat is a possible security risk that might exploit the vulnerability of a system or asset. The origin of the threat may be accidental or environmental, human negligence, or human failure. There are various types of security threats such as Interruption, Interception, Fabrication, and Modification.

An Attack is an intentional unauthorized action on a system. Attacks can be grouped into two categories −

- **Active Attacks** − An active attack is an attempt to change system resources or influence their operation.
- **Passive Attacks** − A passive attack is an attempt to understand or retrieve sensitive data from a system without influencing the system resources.

c. Define Encryption and Decryption?

Encryption: The process of converting plain text to cipher text.

Decryption: The process of converting cipher text to plain text.

d. Describe VPN and its importance in Network Model?

VPN stands for **"Virtual Private Network"** and describes the opportunity to establish a protected network connection when using public networks. VPNs encrypt your internet traffic and disguise your online identity. This makes it more difficult for third parties to track your activities online and steal data. The encryption takes place in **real time**.

e. List out the four principal components in OpenSSL

- libcrypto.

This is the core library for **providing** implementations of **numerous cryptographic primitives.** In **addition it provides** a set of supporting services which are **used by** libssl

- Engine. The functionality of libcrypto can be extended through the Engine API.

Typically engines are dynamically loadable modules that are registered with libcrypto to provide **cryptographic algorithm implementation**

- Libssl

This library **depends** on libcrypto and **implements** the TLS and DTLS protocols.

- Applications

The applications are a set of command line tools that use the underlying libssl and libcrypto components to **provide a set of cryptographic** and **other features** such as

a) Key and parameter generation and inspection

b)Certificate generation and inspection

c)SSL/TLS test tools

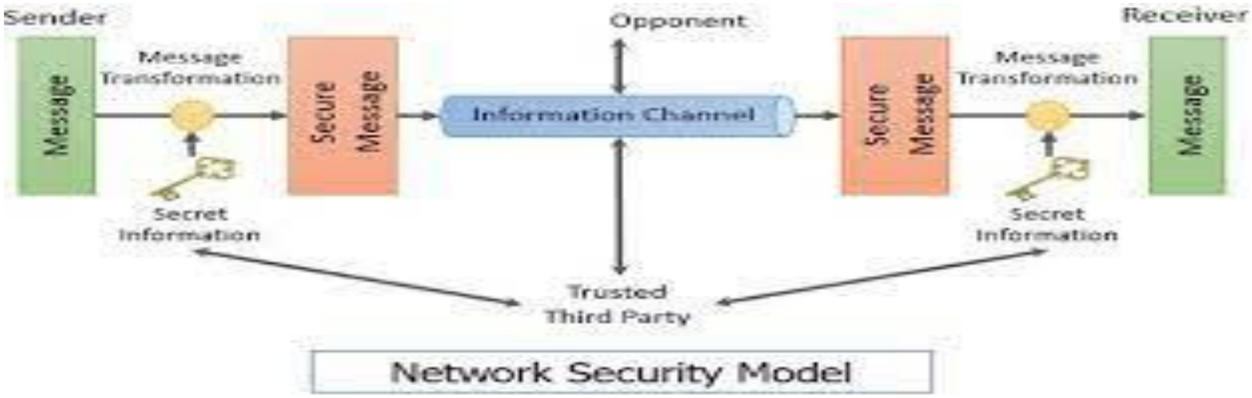
d)ASN.1 inspection

Part B

2. Explain the model of a network security with neat diagram?

Security aspects come into play when it is necessary or desirable to protect the information transmission from an opponent who may present a threat to confidentiality, authenticity, and so on.

All the techniques for providing security have two components:



- A security-related transformation on the information to be sent.
- Examples include the encryption of the message, which scrambles the message so that it is unreadable by the opponent, and the addition of a code based on the contents of the message, which can be used to verify the identity of the sender.
- Some secret information shared by the two principals and, it is hoped, unknown to the opponent.
- An example is an encryption key used in conjunction with the transformation to scramble the message before transmission and unscramble it on reception.
- A trusted third party may be needed to achieve secure transmission.

For example, a third party may be responsible for distributing the secret information to the two principals while keeping it from any opponent.

- This general model shows that there are four basic tasks in designing a particular security service:

1. Design an algorithm for performing the security-related transformation. The algorithm should be such that an opponent cannot defeat its purpose.
2. Generate the secret information to be used with the algorithm.
3. Develop methods for the distribution and sharing of the secret information.
4. Specify a protocol to be used by the two principals that makes use of the security algorithm and the secret information to achieve a particular security service.

3. Discuss various Risks and Attacks types in information and Cyber Security?

The term “information security risk” refers to the damage that attacks against IT systems can cause.

IT risk encompasses a wide range of potential events, including data breaches, regulatory enforcement actions, financial costs, reputational damage, and more.

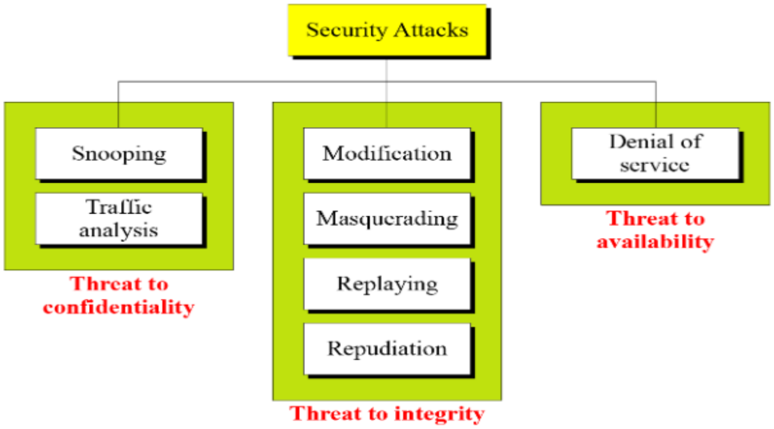
Although “risk” is often conflated with “threat,” the two are subtly different.

“Risk” is a more conceptual term: something that may or may not happen.

A “threat” is a specific, actual danger.

- The three goals of security confidentiality, integrity, and availability can be threatened by security attacks.
- Attacks Threatening Confidentiality
- Attacks Threatening Integrity

Attacks Threatening Availability



Attacks Threatening Confidentiality–refer unit-1 pdf for diagrams

Snooping refers to unauthorized access to or interception of data.

Traffic analysis refers to obtaining some other type of information by monitoring online traffic.

Attacks Threatening Integrity–refer unit-1 pdf for diagrams

Modification means that the attacker intercepts the message and changes it.

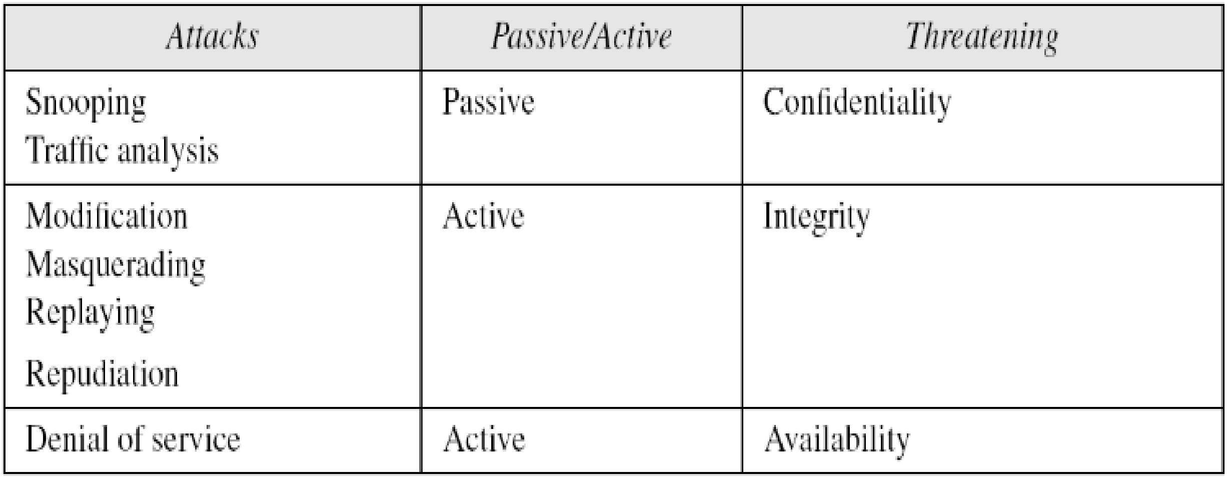
Masquerading or spoofing happens when the attacker impersonates somebody else.

Replaying means the attacker obtains a copy of a message sent by a user and later tries to replay it.

Repudiation means that sender of the message might later deny that she has sent the message; the receiver of the message might later deny that he has received the message.

Attacks Threatening Availability–refer unit-1 pdf for diagrams

Denial of service (DoS) is a very common attack. It may slow down or totally interrupt the service of a system.



Attacks	*Passive/Active*	*Threatening*
Snooping Traffic analysis	Passive	Confidentiality
Modification Masquerading Replaying Repudiation	Active	Integrity
Denial of service	Active	Availability

4. Discuss Operating System vulnerabilities and its possible attacks?

- **Operating Systems attacks**, **"attackers look for vulnerabilities in OS such that they can exploit through vulnerabilities and gain access to the target system or network".**
- The vulnerabilities in the OS can be **open ports and services** as most of the operating systems install these services and ports by default. These are the most common vulnerabilities found by attackers to gain access to an operating system.
- Some of the OS vulnerabilities list
    - Buffer Overflow Vulnerability
    - Bugs in the operating system
    - Unpatched Operating System
- Some of the attacks performed by OS Level
    - Exploiting specific network protocol implementation
    - Attacking built-in Authentication System
    - Breaking file-system Security
    - Cracking Passwords and Encryption Mechanism

- Misconfiguration Attacks: Misconfiguration Attacks can be defined as "**occurrence of errors while implementing all security controls**"

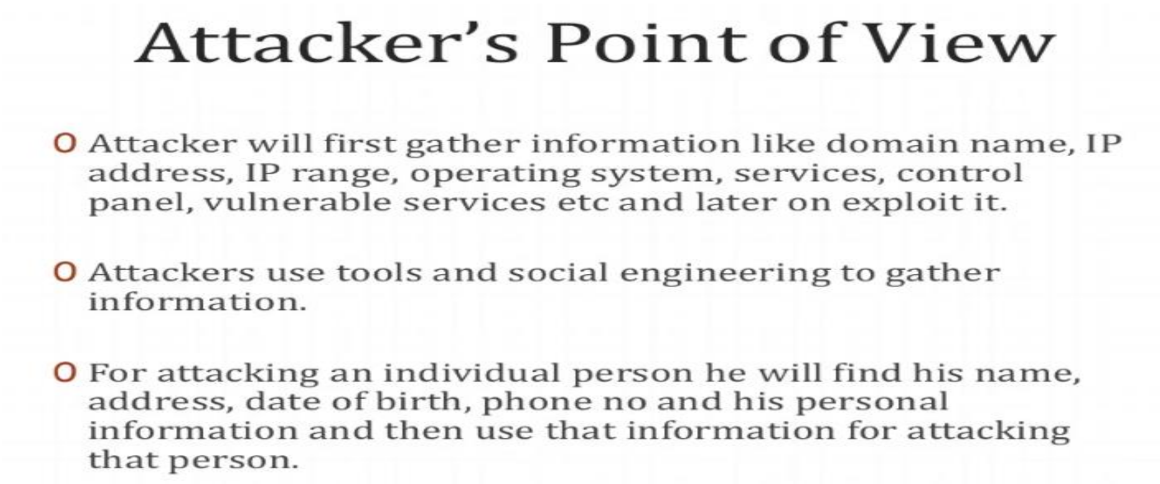
    - It may occur either at any stage like developing, deploying, or maintaining, etc. Due to this attackers gain unauthorized access to the systems and affect web servers, databases, etc.

    - **Prevention**: Administrators need to change default configuration of the devices and deploy automated scanners.

- Application-level Attacks: Defined as “**A program or software which can perform a specific function to an end-user or for some other application**”.
  - Since, the code for an application comes with more **features and functionalities**, there may be some **undiscovered security holes** or vulnerabilities leaving behind.
  - This is the opportunity for an attacker to find these vulnerabilities and exploit using different techniques to gain access and steal data.
  - **Prevention**: these kind of attacks error checking or handling of applications must be strict.
- Shrink-Wrap code Attacks:: It is defined as “**exploiting the default configuration and settings of libraries and code”**.
  - **Prevention:** have to fine-tune every part of the code and make it more secure.

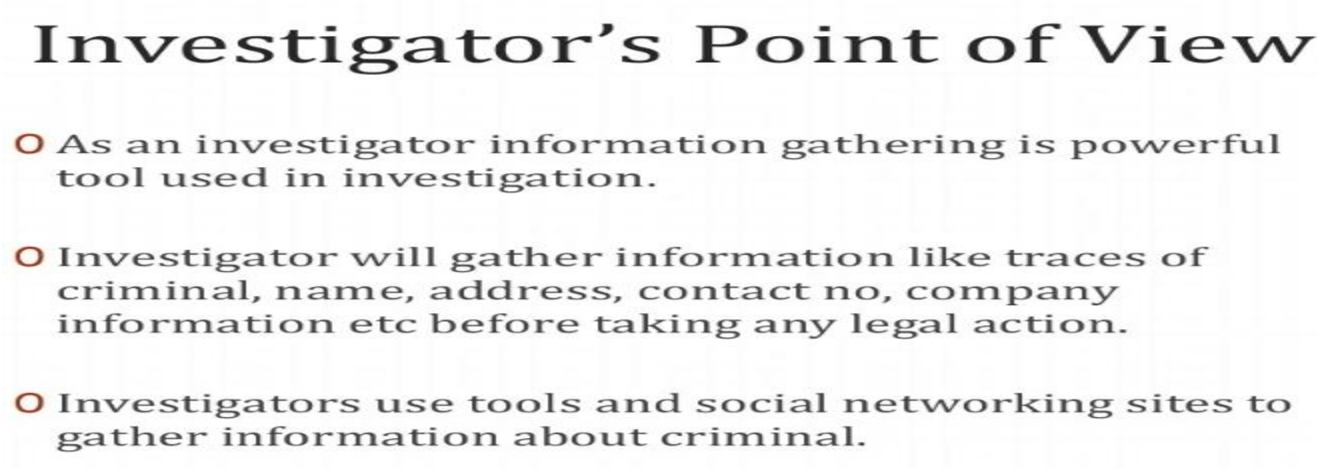
5. Define Exploits. Explain information gathering techniques.

- An **exploit** is a code that takes advantage of a software vulnerability or security flaw.
- exploits allow an intruder to remotely access a network and gain elevated privileges, or move deeper into the network.
- In some cases, an exploit can be used as part of a multi-component attack. Instead of using a malicious file, the exploit may instead drop another malware, which can include backdoor Trojans and spyware that can steal user information from the infected systems.
- Gathering information is the first step where a hacker tries to get information about the target.
- Information Gathering is the act of gathering different kinds of information against the targeted victim or system.
- It is the first step or the beginning stage of Ethical Hacking, where the penetration testers or hackers (both black hat or white hat) performed this stage; this is a necessary and crucial step to be performed.
- The more the information gathered about the target, the more the probability to obtain relevant results.
- Information gathering is not just a phase of security testing; it is an art that every penetration-tester (pen-tester) and hacker should master for a better experience in penetration testing.
- There are various tools, techniques, and websites, including public sources such as Whois, nslookup that can help hackers gather information.
- This step is necessary because you may need any information (such as his pet name, best friend's name, age, or phone number to perform password guessing attack or other kinds of attacks) while performing attacks on any target.



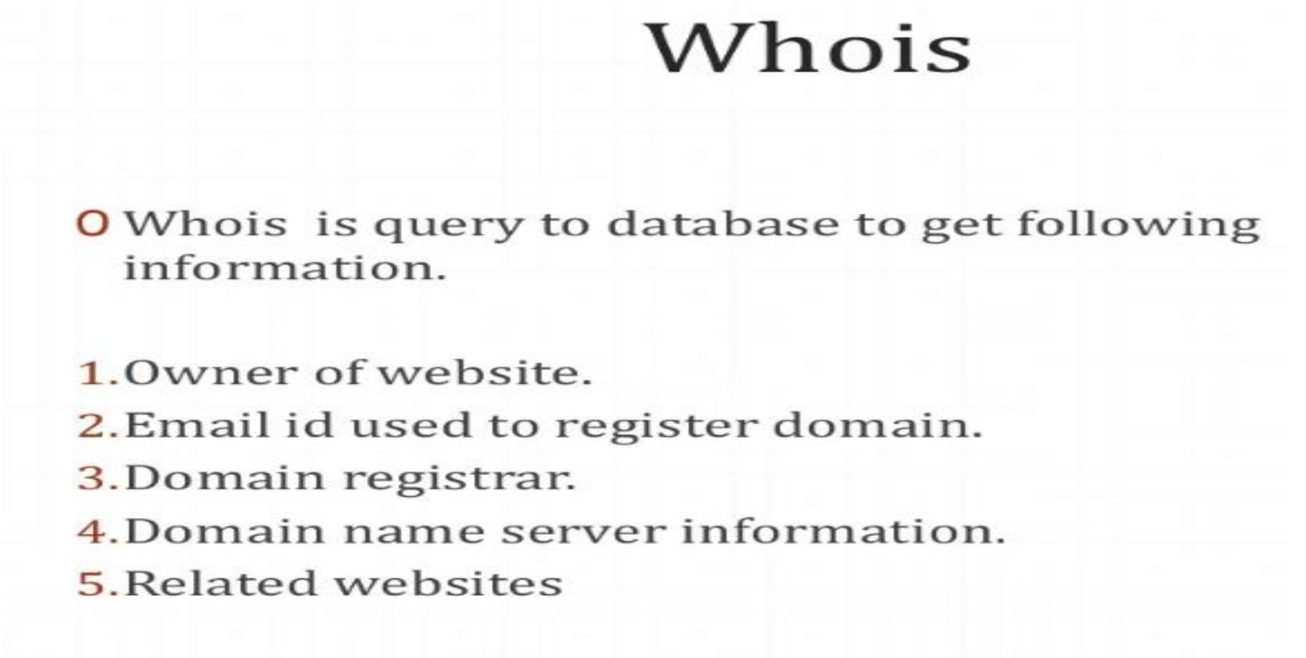
Attacker's Point of View

- Attacker will first gather information like domain name, IP address, IP range, operating system, services, control panel, vulnerable services etc and later on exploit it.
- Attackers use tools and social engineering to gather information.
- For attacking an individual person he will find his name, address, date of birth, phone no and his personal information and then use that information for attacking that person.



Investigator's Point of View

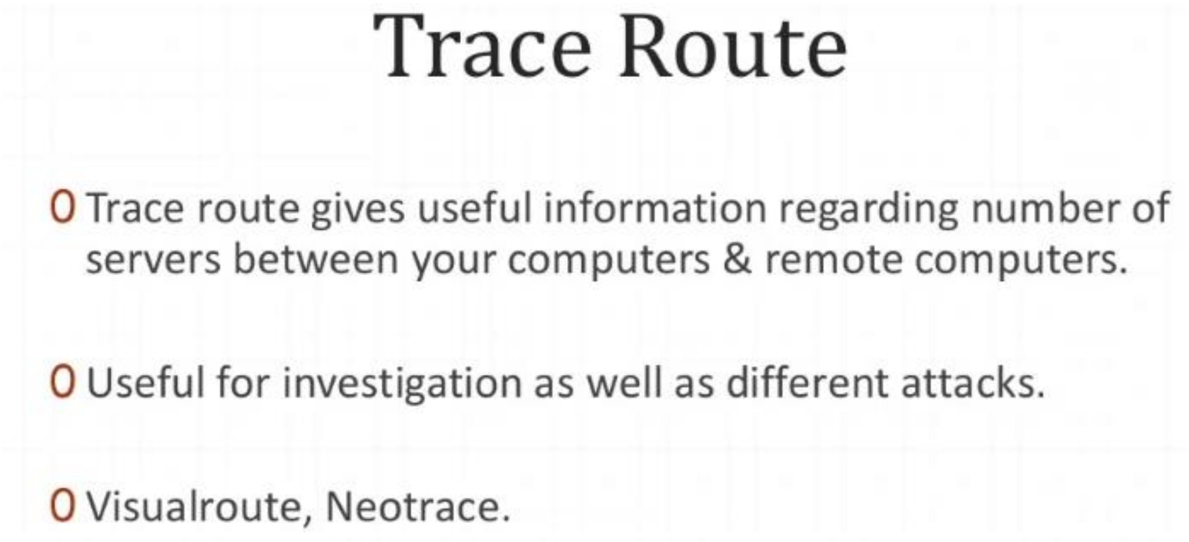
- As an investigator information gathering is powerful tool used in investigation.
- Investigator will gather information like traces of criminal, name, address, contact no, company information etc before taking any legal action.
- Investigators use tools and social networking sites to gather information about criminal.



Whois

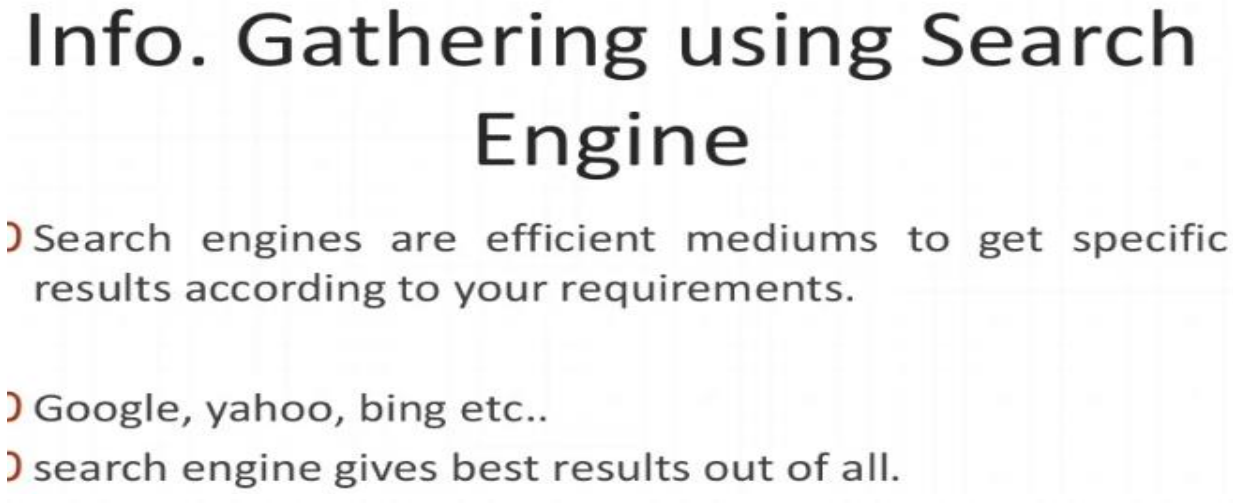
- Whois is query to database to get following information.

1. Owner of website.
2. Email id used to register domain.
3. Domain registrar.
4. Domain name server information.
5. Related websites



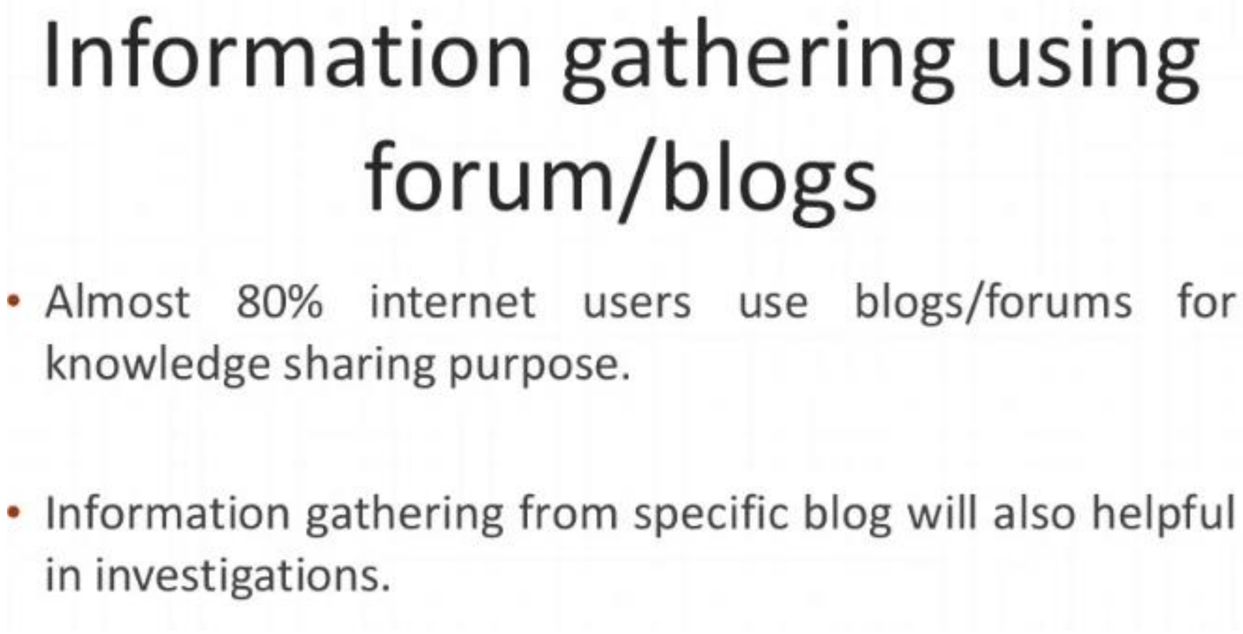
Trace Route

- Trace route gives useful information regarding number of servers between your computers & remote computers.
- Useful for investigation as well as different attacks.
- Visualroute, Neotrace.



Info. Gathering using Search Engine

- Search engines are efficient mediums to get specific results according to your requirements.
- Google, yahoo, bing etc..
- search engine gives best results out of all.



Information gathering using forum/blogs

- Almost 80% internet users use blogs/forums for knowledge sharing purpose.
- Information gathering from specific blog will also helpful in investigations.

6. Describe Digital Signatures Algorithm with neat diagram?

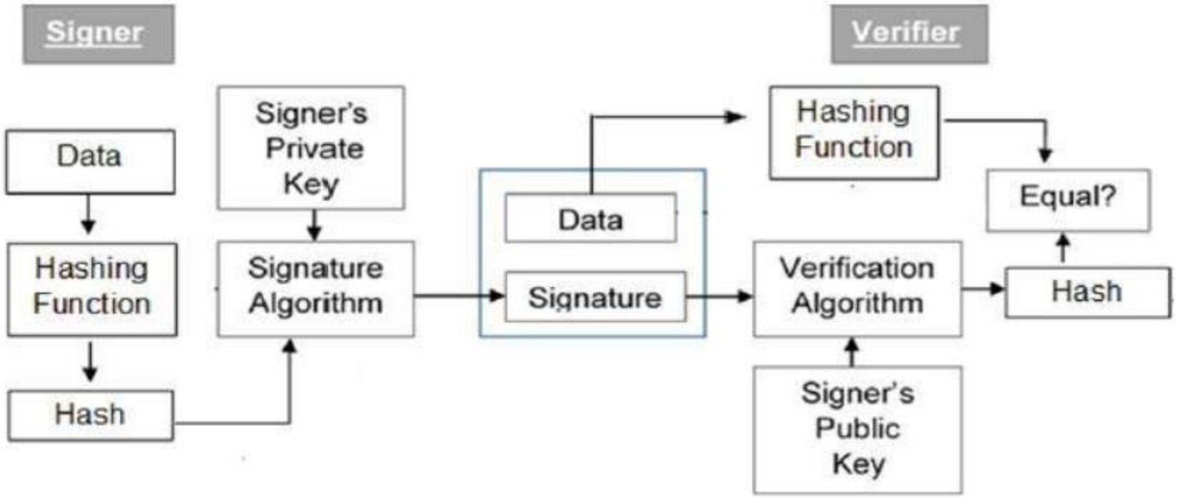
Digital signatures are the public-key primitives of message authentication. In the physical world, it is common to use handwritten signatures on handwritten or typed messages. They are used to bind signatory to the message.

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.

Model of Digital Signature

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

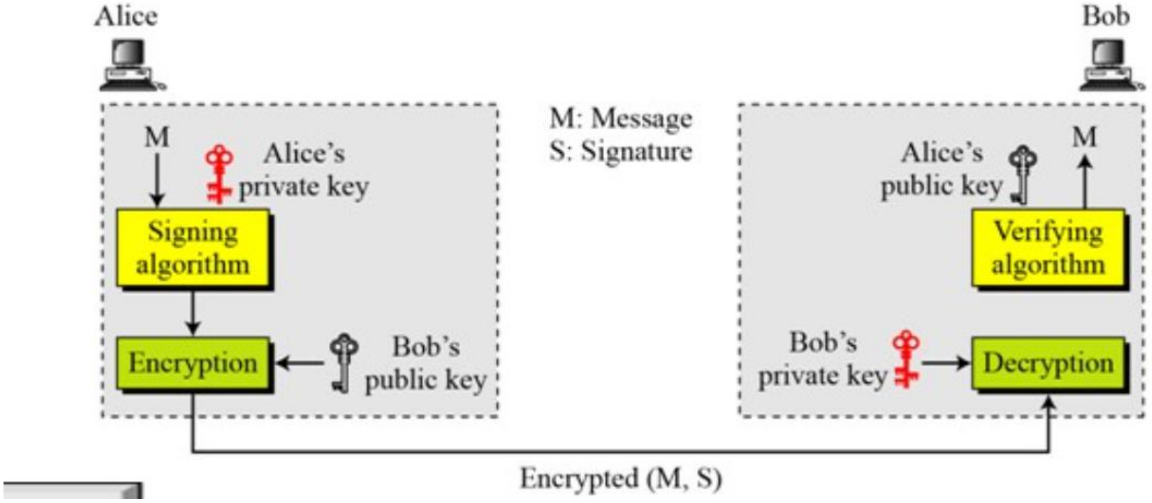


The following points explain the entire process in detail –

- 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.

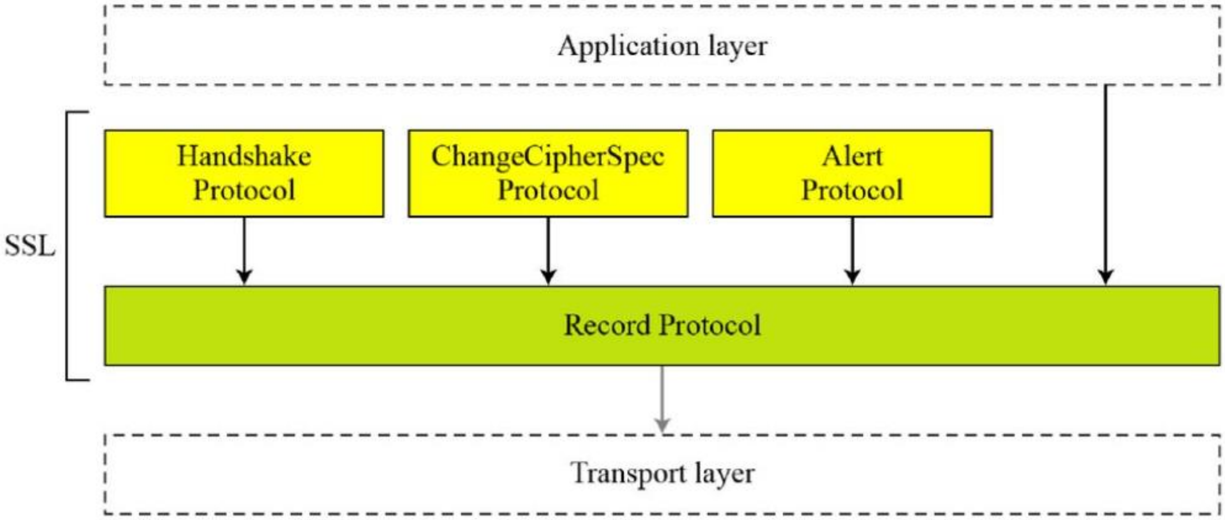
- Verifier feeds the digital signature and the verification key into the verification algorithm. The verification algorithm gives some value as output.
- Verifier also runs same hash function on received data to generate hash value.
- For verification, this hash value and output of verification algorithm 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.

Figure 13.5 *Adding confidentiality to a digital signature scheme*

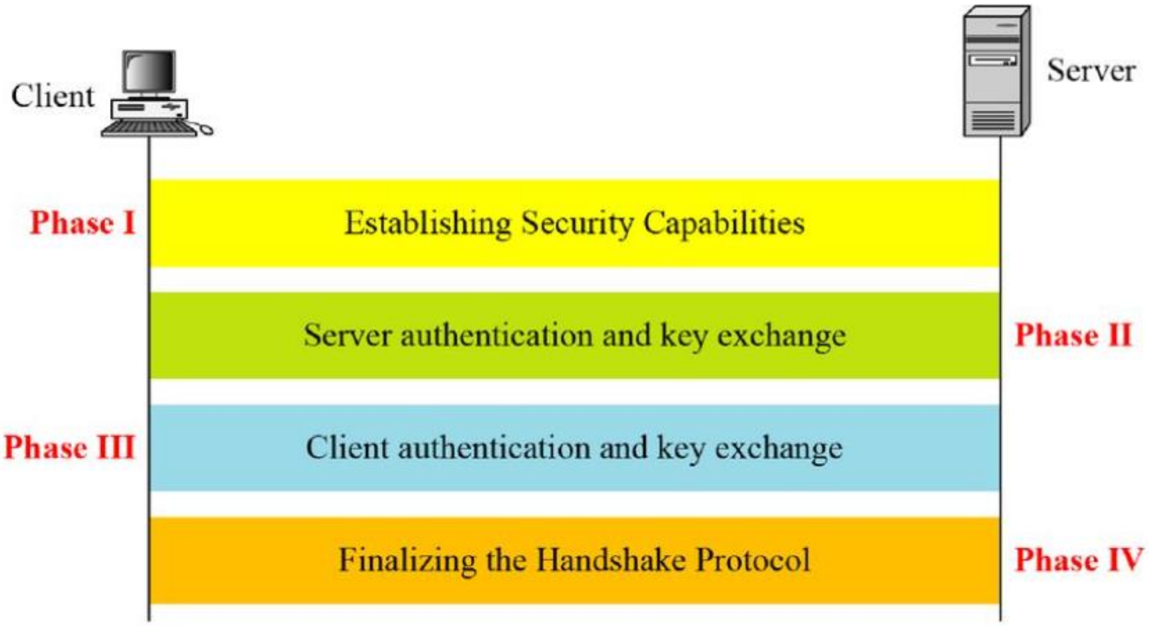


7. Illustrate with neat diagram the different phases in SSL handshake protocol mechanism?

   SSL is designed to provide security and compression services to data generated from the application layer.originally developed by Netscape.version 3 designed with public input. uses TCP to provide a reliable end-to-end service



Handshake Protocol


Client
Server
Phase I
Establishing Security Capabilities
Server authentication and key exchange
Phase II
Phase III
Client authentication and key exchange
Finalizing the Handshake Protocol
Phase IV

Phase I of Handshake Protocol

After Phase I, the client and server know the following:

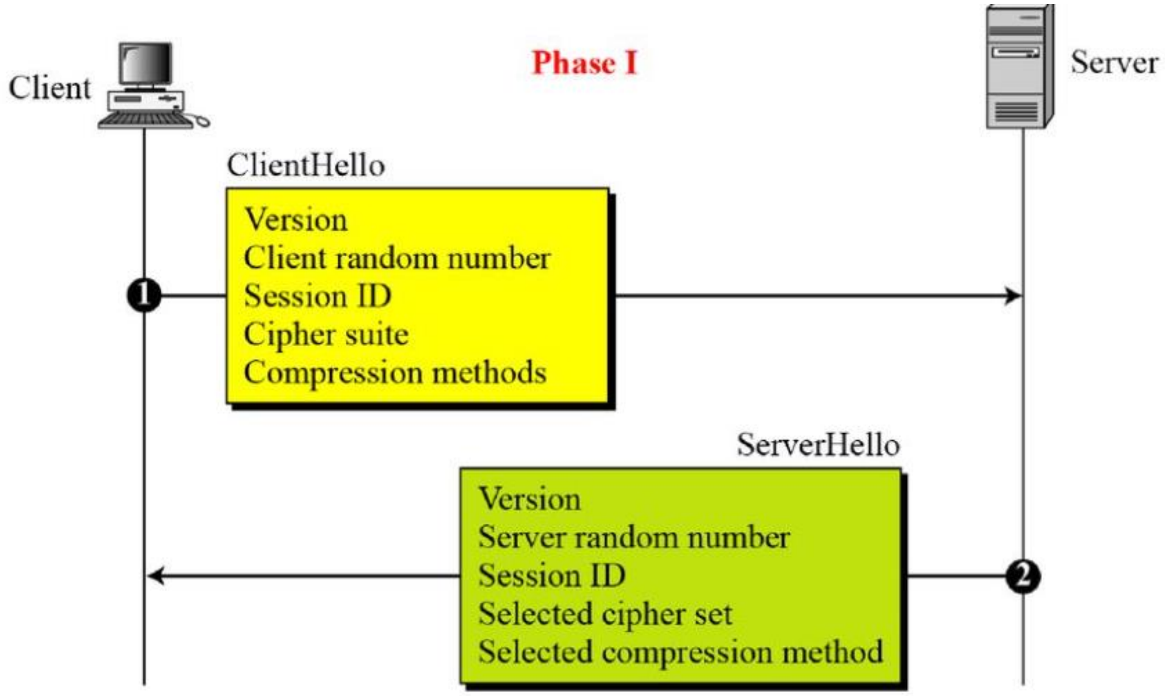
❑The version of SSL

❑The algorithms for

key exchange, message authentication, and encryption

❑The compression method

❑The two random numbers for key generation

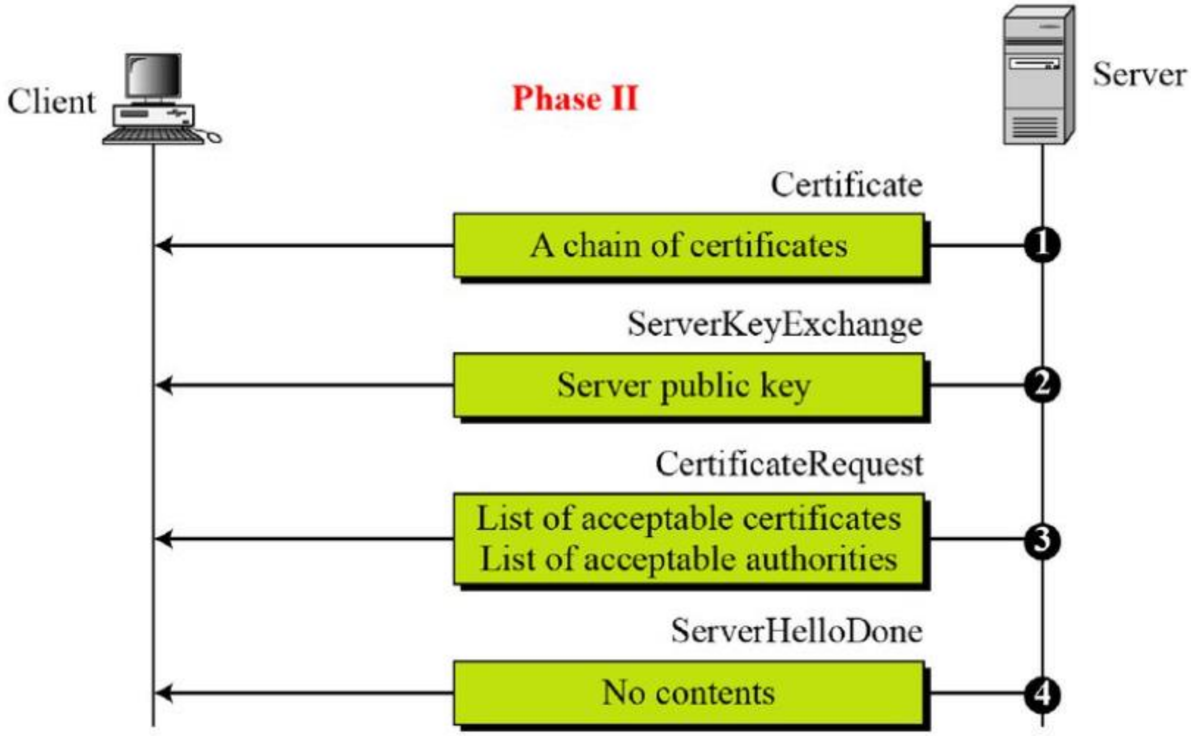


Phase II of Handshake Protocol

After Phase II,

❑The server is authenticated to the client.

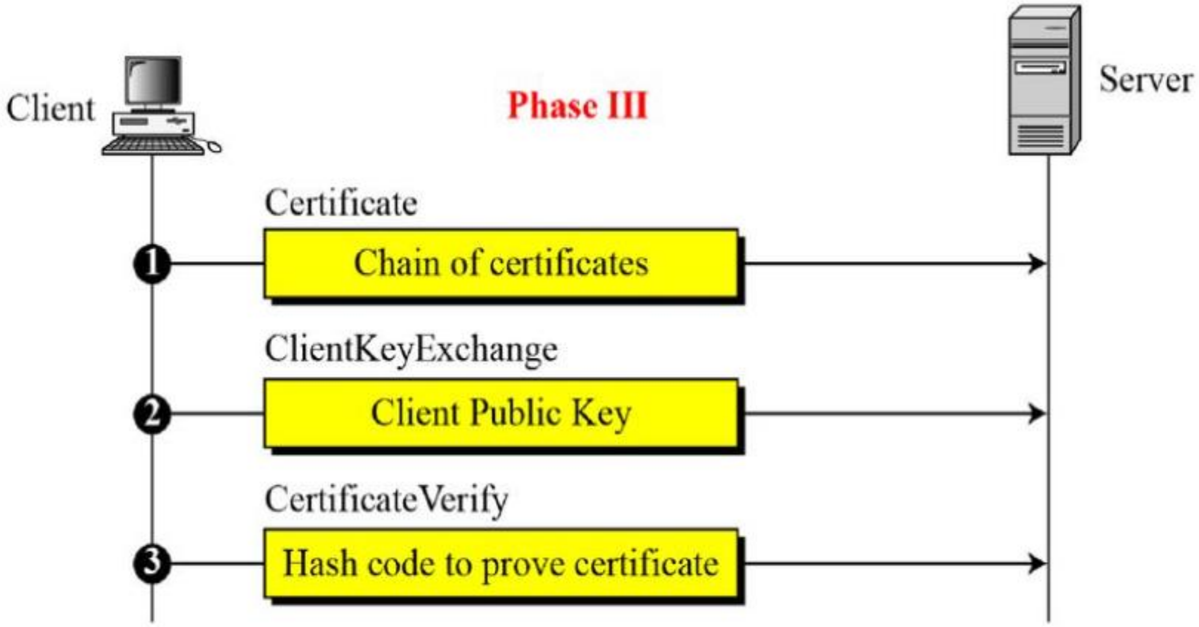
❑The client knows the public key of the server if required.



Phase III of Handshake Protocol
After Phase III,

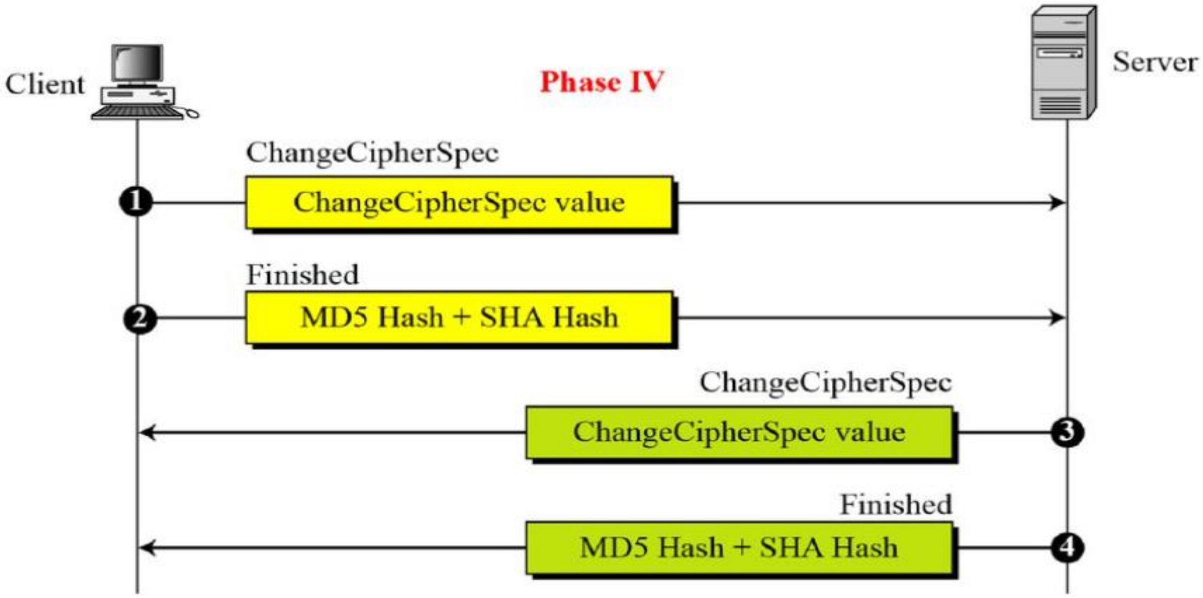
❑The client is authenticated for the server.

❑Both the client and the server know the pre-master secret.



Phase IV of Handshake Protocol

After Phase IV, the client and server are ready to exchange data.



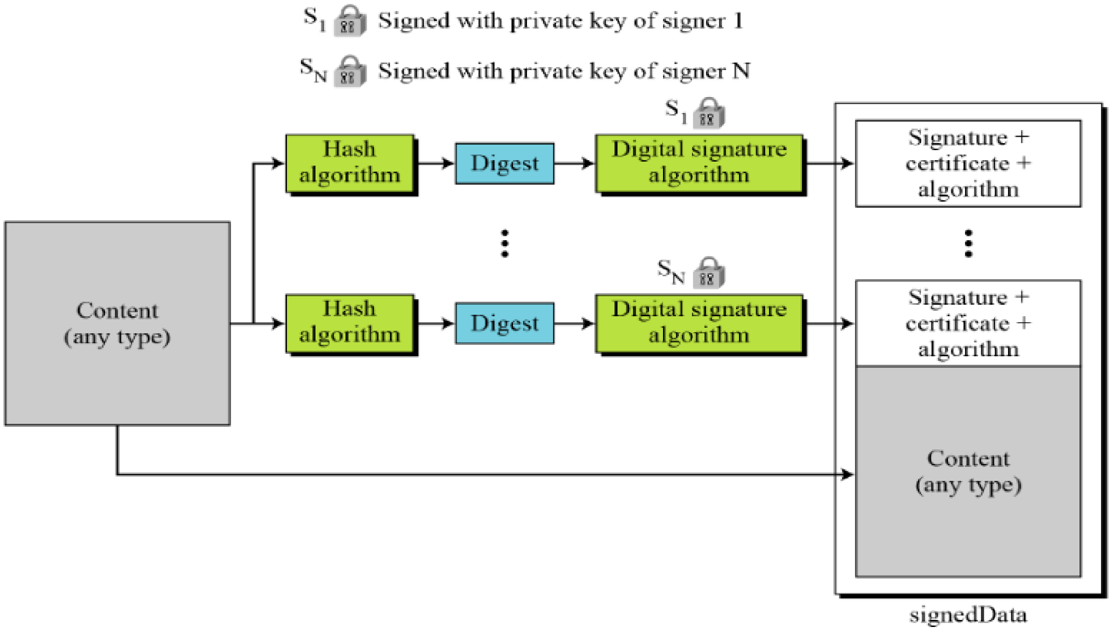
8. Explain about S/MIMIE in detail.

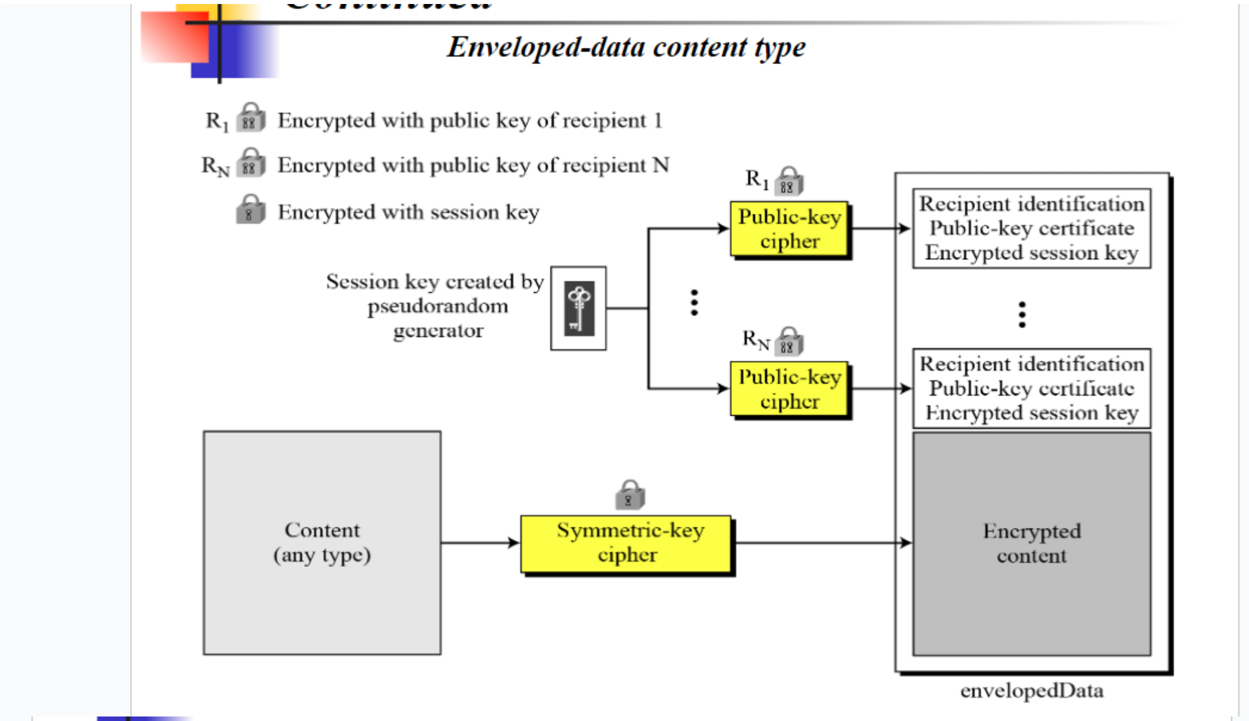
S/MIME adds some new content types to include security services to the MIME. All of these new types include the parameter “application/pkcs7-mime,” in which “pkcs” defines “Public Key Cryptography Specification.”

Cryptographic Message Syntax (CMS)

To define how security services, such as confidentiality or integrity, can be added to MIME content types, S/MIME has defined Cryptographic Message Syntax (CMS). The syntax in each case defines the exact encoding scheme for each content type. For details, the reader is referred to RFC 3369 and 3370.

Signed-data content type


S1 Signed with private key of signer 1
SN Signed with private key of signer N
Content (any type)
Hash algorithm
Digest
S1
Digital signature algorithm
Signature + certificate + algorithm
Hash algorithm
Digest
SN
Digital signature algorithm
Signature + certificate + algorithm
Content (any type)
signedData



Continued

Enveloped-data content type

R1 Encrypted with public key of recipient 1

RN Encrypted with public key of recipient N

Encrypted with session key

Session key created by pseudorandom generator

R1

Public-key cipher

RN

Public-key cipher

Recipient identification
Public-key certificate
Encrypted session key

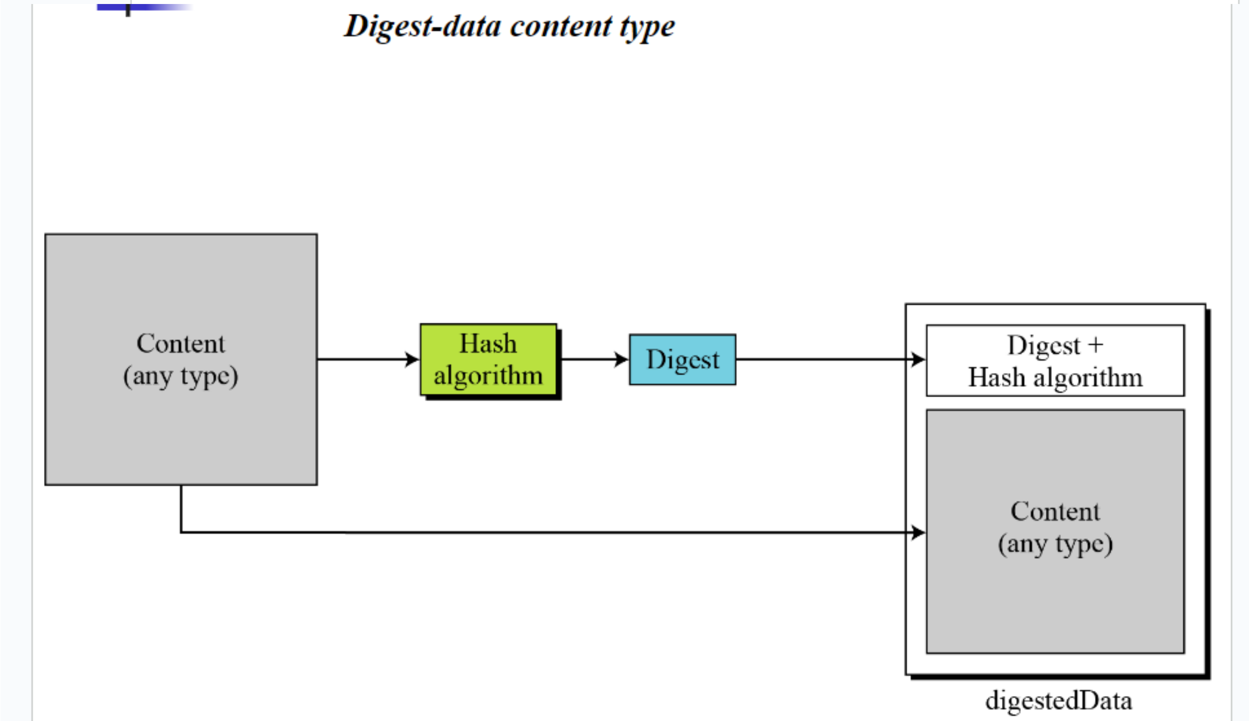
Recipient identification
Public-key certificate
Encrypted session key

Content (any type)

Symmetric-key cipher

Encrypted content

envelopedData



Digest-data content type

Content (any type)

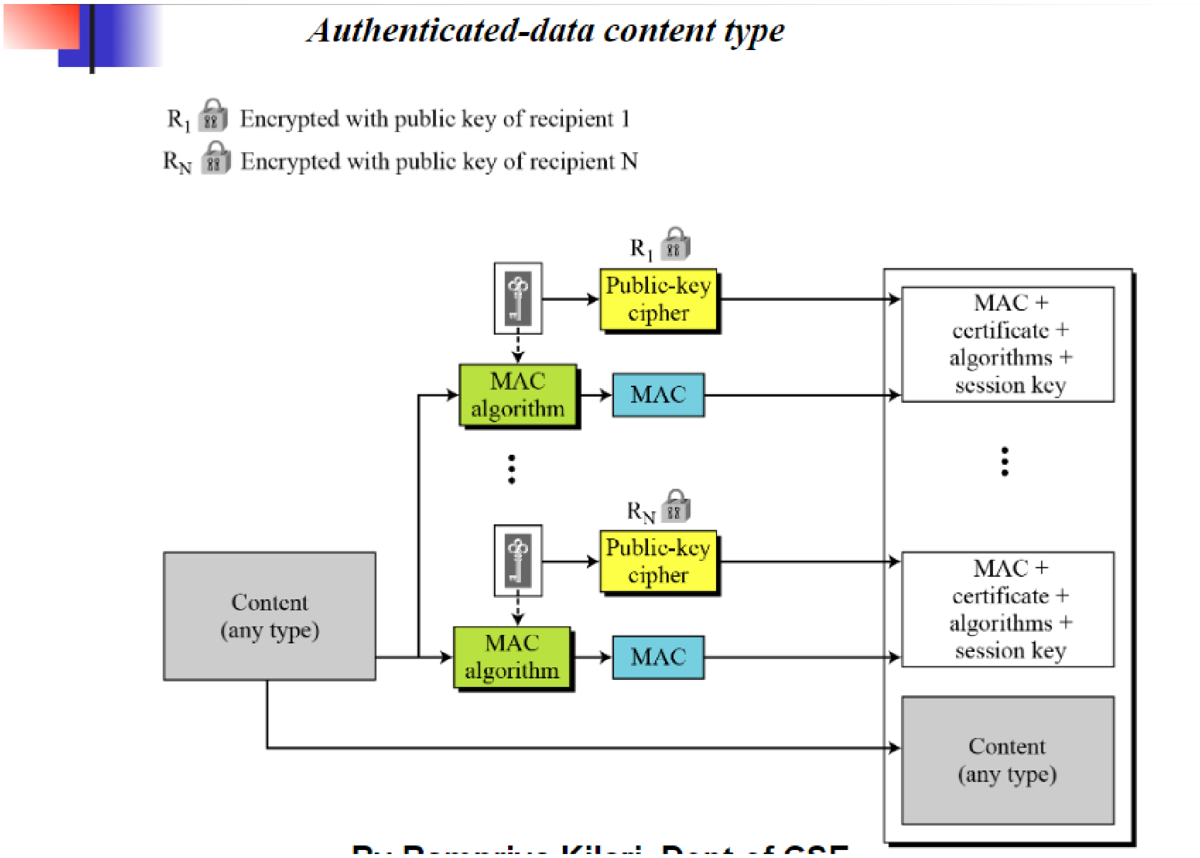
Hash algorithm

Digest

Digest +
Hash algorithm

Content (any type)

digestedData



Authenticated-data content type

R1 🔒 Encrypted with public key of recipient 1
RN 🔒 Encrypted with public key of recipient N

9. Describe various services provided by PGP in detail.

PGP includes the following services which are as follows −

Authentication − The hash function used is SHA-1 which makes a 160 bit message digest. EP (DP) defines public encryption (decryption) and the algorithm used can be RSA or DSS.

The set of SHA-1 and RSA supports an effective digital signature scheme. Because of the strength of RSA the recipient is guaranteed that only the possessor of the connecting private key can make the signature. Because of the strength of SHA-1 the recipient is guaranteed that no one else can create a new message that connects the hash code and therefore the signature of the original message.

Confidentiality − It is a service supported by PGP is confidentiality which is provided by encrypting messages to be transmitted or to be saved locally as files. In some cases, the user has a best of CAST-128, IDEA or 3DES in 64 bit cipher feedback (CFB) mode. The symmetric key is used only once and is generated as a random number with the required number of bits. It is acquired along with the message and is encrypted using the recipient's public key.

- The sender creates a message and a random number to be used as a session key for this message only.
- The message is encrypted utilizing CAST-128, IDEA or 3DES with the session key.
- The session key is encrypted with RSA utilizing the recipient's public key and is prepended to the message.
- The receiver uses RSA with its private key to decrypt and restore the session key.
- The session key can be used to decrypt the message.

Confidentiality and Authentication − The both services can be used for the same message. First, a signature is produced for the plaintext message and prepended to the message. Therefore the plaintext message plus signature is encrypted using CAST-128 (or IDEA or 3DES), and the session key is encrypted using RSA.

This sequence is desirable to the opposite encrypting the message and thus producing a signature of the encrypted message. It is usually more convenient to save a signature with a plaintext version of a message. Moreover, for the goals of third party verification, if the signature is implemented first, a third party need not be concerned with the symmetric key when testing the signature.

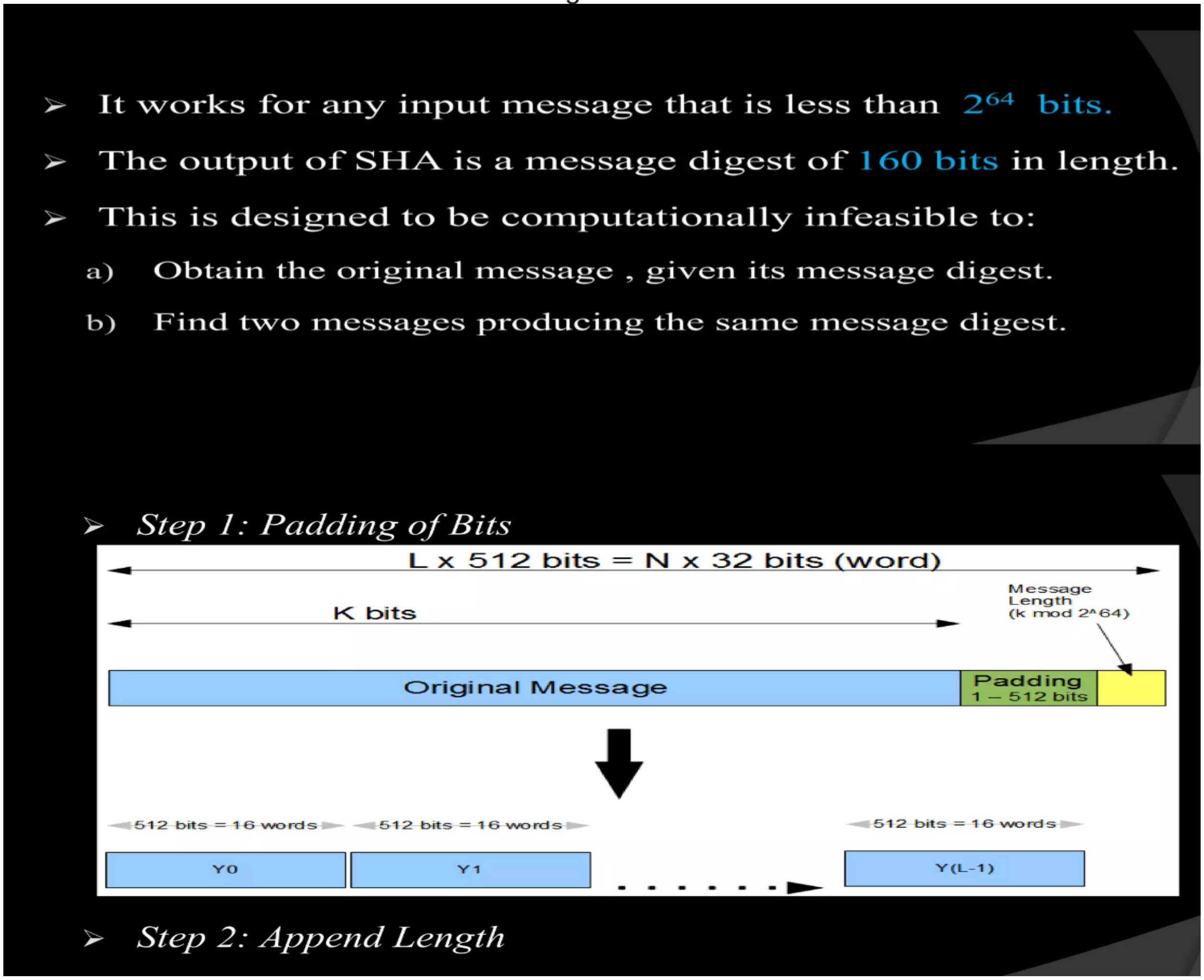
Compression − As a default, PGP restrict the message after using the signature but before encryption. This has the advantage of storing space both for e-mail transmission and for file storage.

E-mail compatibility − Some electronic mail systems only allows the use of blocks including ASCII text. When PGP is used, minimum part of the block to be transmitted is encrypted.

Segmentation − E-mail facilities are restricted to a maximum message length. For instance, some facilities accessible throughout the internet set a maximum length of 50,000 octets. Some message higher than that should be broken up into smaller segments, each of which is mailed independently.

10. State the function of SHA-1 ? State its important features.Explain the outlinr of its compression function?

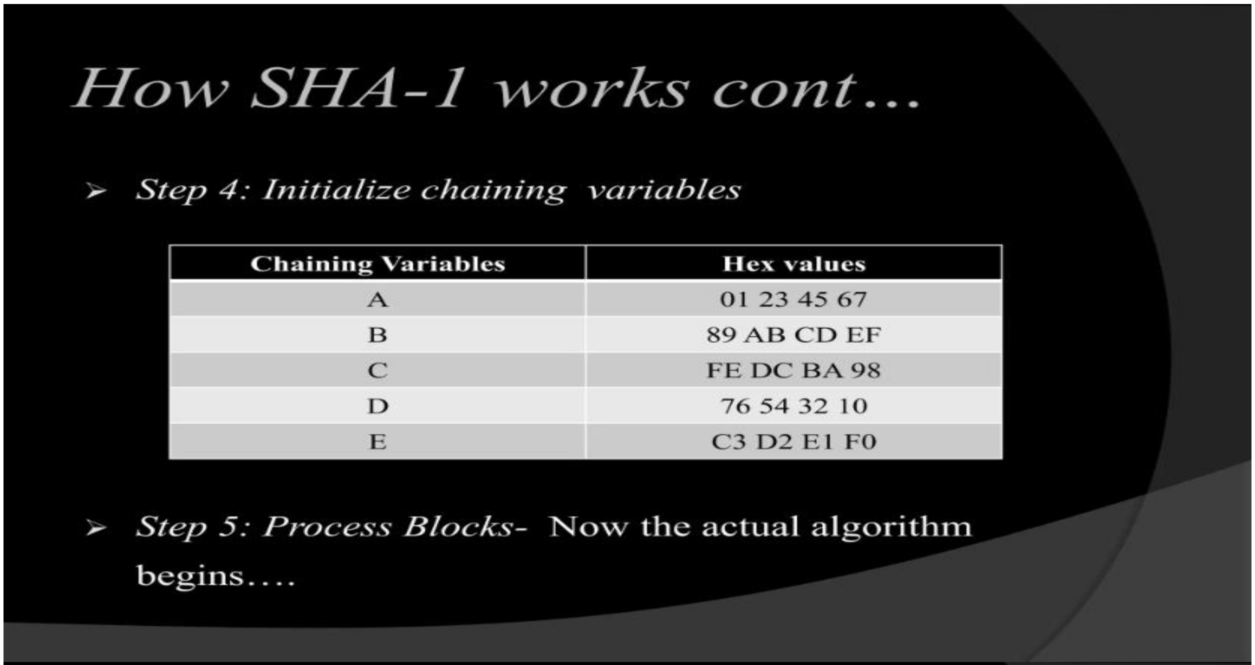
Secure Hashing Algorithm, or SHA. Data and certificates are hashed with SHA, a modified version of MD5. By using bitwise operations, modular additions, and compression functions, a hashing algorithm reduces the input data into a smaller form that is impossible to comprehend. Can hashing be cracked or decrypted, you may wonder? The main distinction between hashing and encryption is that hashing is one-way; once data has been hashed, the resultant hash digest cannot be decrypted unless a brute force assault is applied. See the illustration below to see how the SHA algorithm functions.



- It works for any input message that is less than 2^{64} bits.
- The output of SHA is a message digest of 160 bits in length.
- This is designed to be computationally infeasible to:
  a) Obtain the original message , given its message digest.
  b) Find two messages producing the same message digest.

- *Step 1: Padding of Bits*

- *Step 2: Append Length*

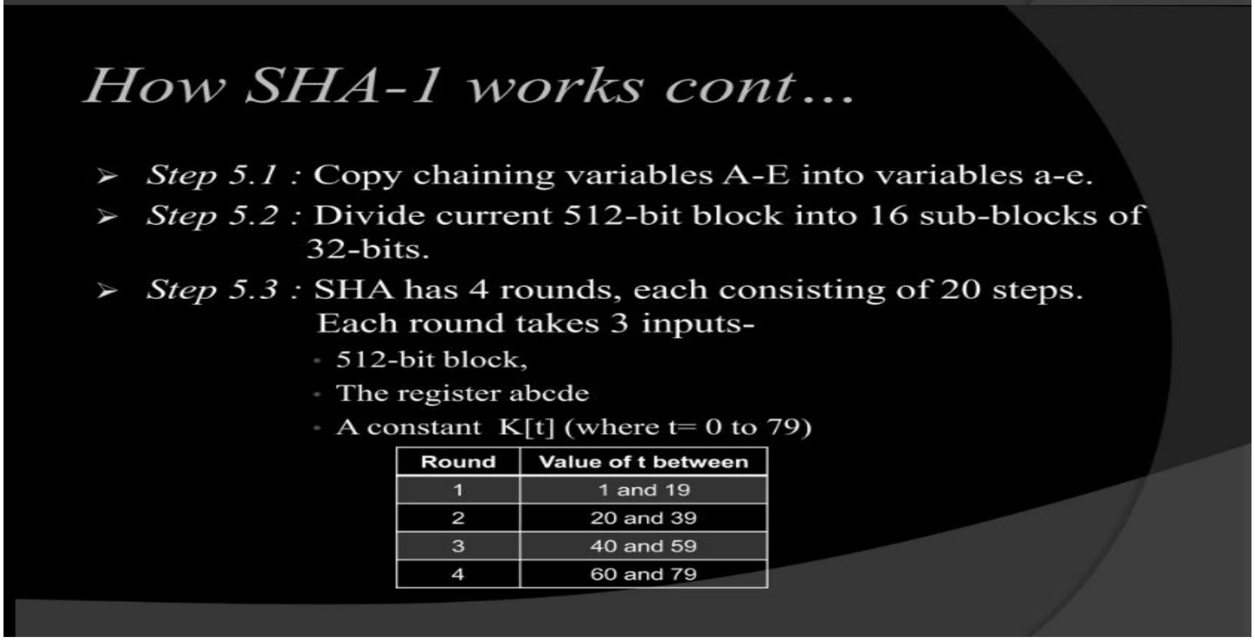


How SHA-1 works cont…

- *Step 4: Initialize chaining variables*

Chaining Variables	Hex values
A	01 23 45 67
B	89 AB CD EF
C	FE DC BA 98
D	76 54 32 10
E	C3 D2 E1 F0

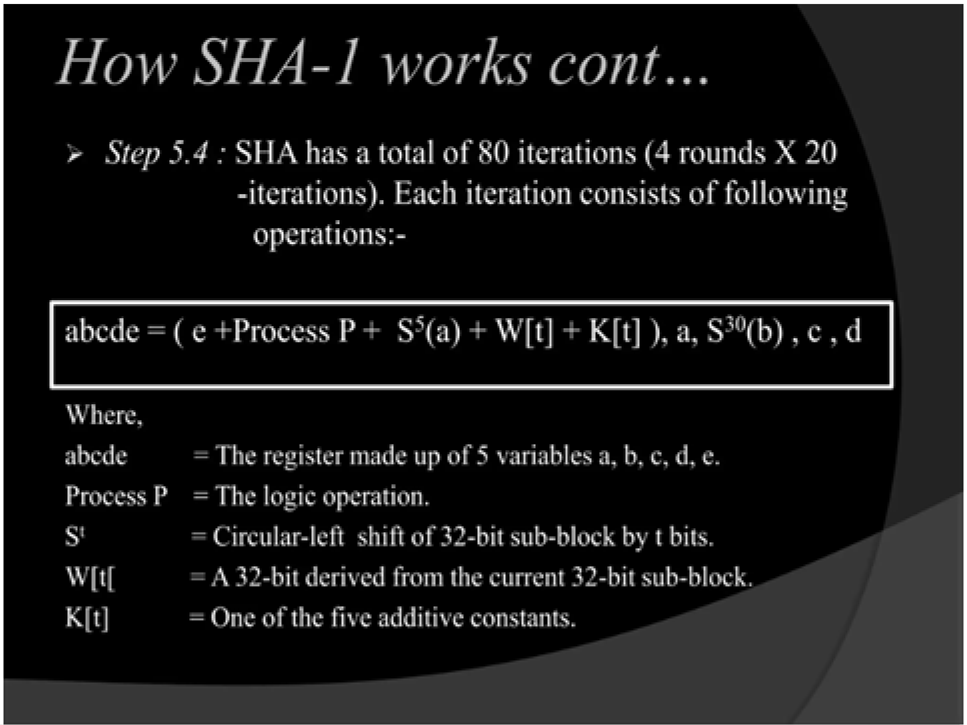
- *Step 5: Process Blocks-* Now the actual algorithm begins….



How SHA-1 works cont…

- *Step 5.1 :* Copy chaining variables A-E into variables a-e.
- *Step 5.2 :* Divide current 512-bit block into 16 sub-blocks of 32-bits.
- *Step 5.3 :* SHA has 4 rounds, each consisting of 20 steps. Each round takes 3 inputs-
  - 512-bit block,
  - The register abcde
  - A constant K[t] (where t= 0 to 79)

Round	Value of t between
1	1 and 19
2	20 and 39
3	40 and 59
4	60 and 79



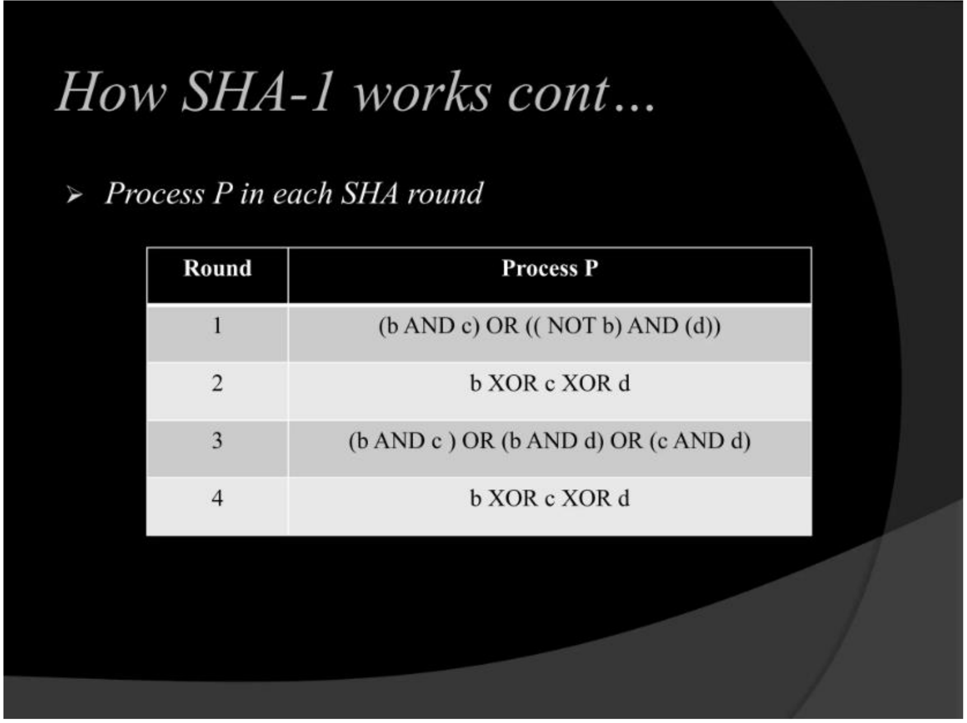
How SHA-1 works cont…

- *Step 5.4 :* SHA has a total of 80 iterations (4 rounds X 20 -iterations). Each iteration consists of following operations:-

abcde = (e +Process P + $S^5(a)$ + W[t] + K[t]), a, $S^{30}(b)$, c , d

Where,

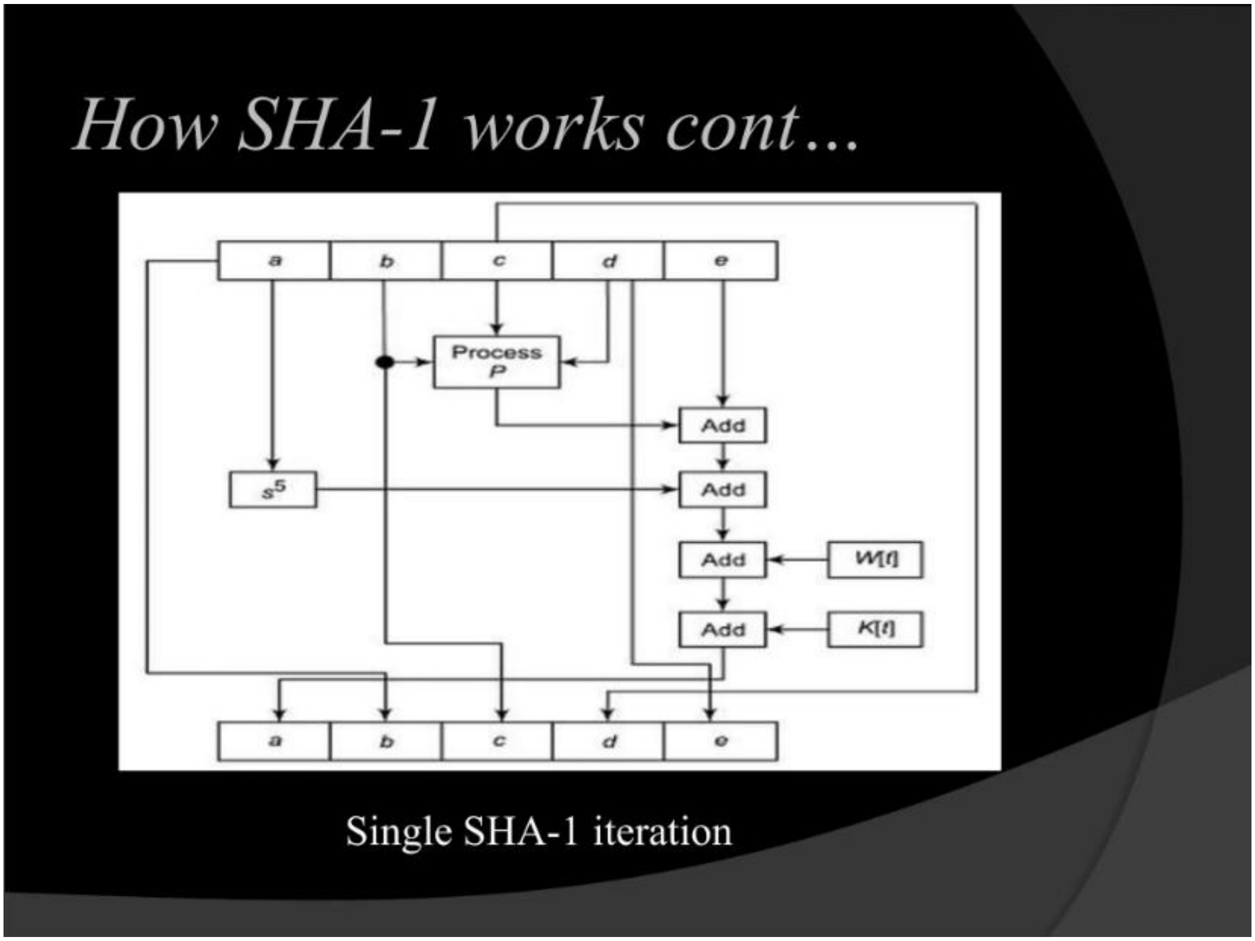
abcde	= The register made up of 5 variables a, b, c, d, e.
Process P	= The logic operation.
S^t	= Circular-left shift of 32-bit sub-block by t bits.
W[t[	= A 32-bit derived from the current 32-bit sub-block.
K[t]	= One of the five additive constants.



How SHA-1 works cont…

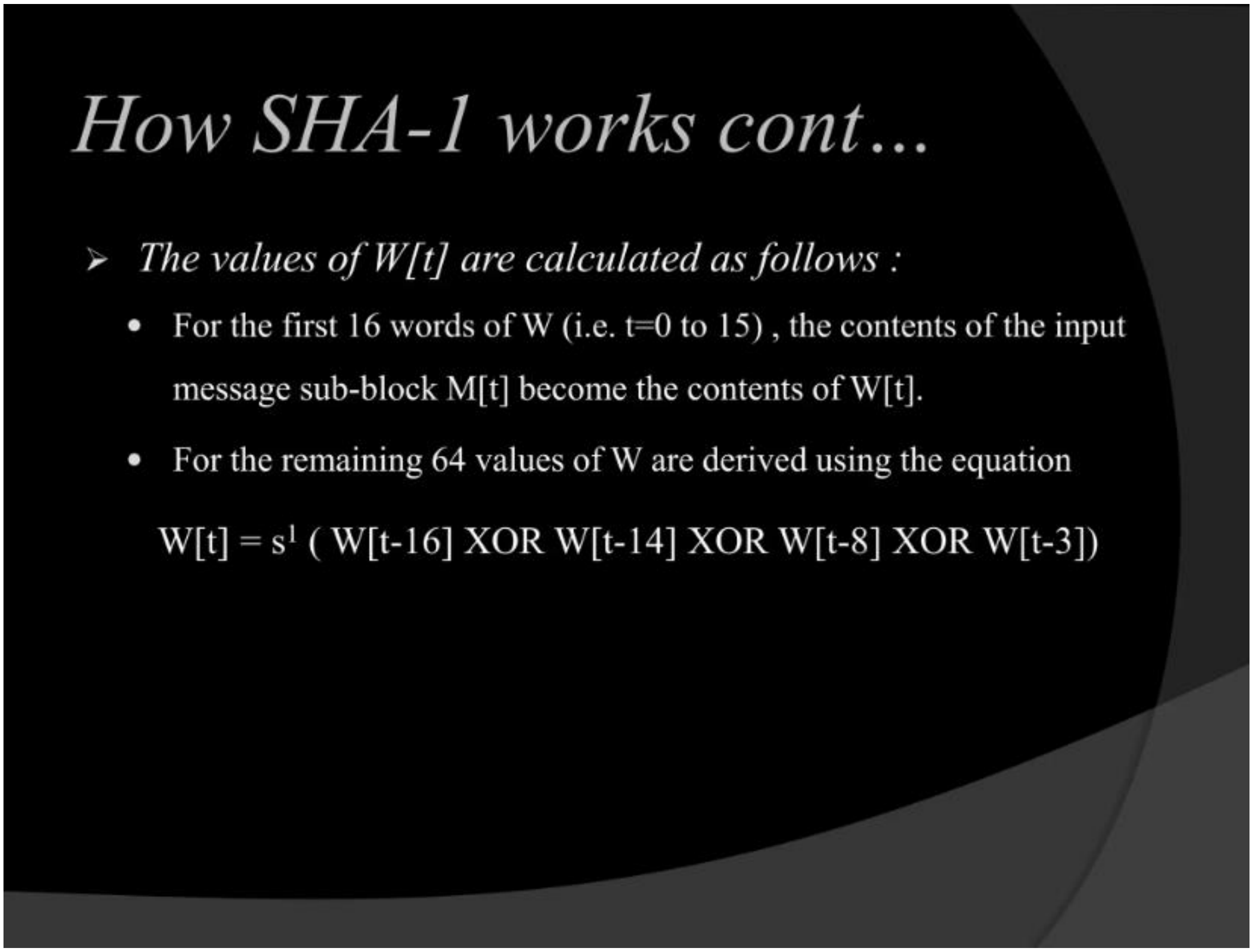
- *Process P in each SHA round*

Round	Process P
1	(b AND c) OR ((NOT b) AND (d))
2	b XOR c XOR d
3	(b AND c) OR (b AND d) OR (c AND d)
4	b XOR c XOR d



How SHA-1 works cont…

Single SHA-1 iteration



How SHA-1 works cont…

- *The values of W[t] are calculated as follows :*
  - For the first 16 words of W (i.e. t=0 to 15) , the contents of the input message sub-block M[t] become the contents of W[t].
  - For the remaining 64 values of W are derived using the equation

    $W[t] = s^1$ (W[t-16] XOR W[t-14] XOR W[t-8] XOR W[t-3])

11. Define Steganography.Explain its working principles.

Steganography is a method of hiding secret data, by embedding it into an audio, video, image, or text file. It is one of the methods working to protect secret or sensitive data from malicious attacks.

Cryptography and steganography are both methods used to hide or protect secret data. However, they differ in the respect that cryptography makes the data unreadable, or hides the meaning of the data, while steganography hides the existence of the data.

Image Steganography –

Image Steganography refers to the process of hiding data within an image file. The image selected for this purpose is called the **cover image** and the image obtained after steganography is called the **stego image**.

- An image is represented as an N*M (in case of grayscale images) or N*M*3 (in case of color images) matrix in memory, with each entry representing the intensity value of a pixel.
- In image steganography, a message is embedded into an image by altering the values of some pixels, which are chosen by an encryption algorithm.

- The recipient of the image must be aware of the same algorithm in order to know which pixels he or she must select to extract the message
- steganography approach involves cover a huge amount of data (picture, audio, and text) within a colour bitmap (bmp) image.
- The image will be filtered and segmented with bits replacement applied to the appropriate pixels. These pixels are chosen at random rather than in order.
- Detection of the message within the cover image is done by the process of steganalysis.
- This can be done through comparison with the cover image, histogram plotting, or noise detection.
- Efforts are being invested in developing new algorithms with a greater degree of immunity against such attacks,
- Efforts are also being dedicated towards improving existing algorithms for steganalysis, to detect the exchange of secret information between terrorists or criminal