CRYPTOGRAPHY & NETWORK SECURITY IMPORTANT QUESTIONS (CNS)

1. **Explain in detail about HMAC Algorithm. 6M**

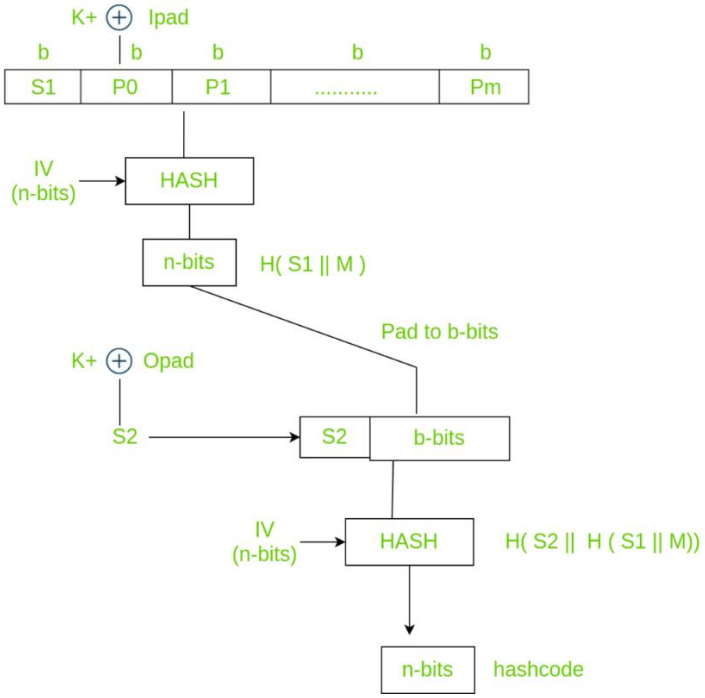
Ans

HMAC (Hash-Based Message Authentication Code) is a cryptographic technique that ensures data integrity and authenticity using a hash function and a secret key. Unlike approaches based on signatures and asymmetric cryptography. Checking data integrity is necessary for the parties involved in communication. HMAC uses a symmetric key(same copy) while Signatures uses an asymmetric (two different keys).

The formula **for HMAC:**

HMAC = hashFunc(secret key + message)

There are three types of authentication functions. They are message encryption, message authentication code, and hash functions.



Using key K (0 < K < b), K+ is generated by padding O's on left side of key K until length becomes b bits. The reason why it's not padded on right is change(increase) in the length of key. b bits because it is the block size of plain text. There are two predefined padding bits called ipad and opad. All this is done before applying hash function to the plain text message.

ipad - 00110110
opad - 01011100

Now we have to calculate S bits:

1. K+ is XORed with ipad and the result is S1 bits which is equivalent to b bits since both K+ and ipad are b bits. We have to append S1 with plain text messages. Let P be the plain text message.
2. S1, p0, p1 upto Pm each is b bits. m is the number of plain text blocks. P0 is plain text block and b is plain text block size. After appending S1 to Plain text we have to apply HASH algorithm (any variant). Simultaneously we have to apply initialization vector (IV) which is a buffer of size n-bits. The result produced is therefore n-bit hashcode i.e H(S1 || M).
3. Similarly, n-bits are padded to b-bits And K+ is EXORed with opad producing output S2 bits. S2 is appended to the b-bits and once again hash function is applied with IV to the block. This further results into n-bit hashcode which is H(S2 || H(S1 || M)).

2. **What are the Requirements of Message Authentication 6M**

Ans

Data is prone to various attacks. One of these attacks includes message authentication. This threat arises when the user does not have any information about the originator of the message. Message authentication can be achieved using cryptographic methods which further make use of keys.

Authentication Requirements:

- **Revelation:** It means releasing the content of the message to someone who does not have an appropriate cryptographic key.
- **Analysis of Traffic:** Determination of the pattern of traffic through the duration of connection and frequency of connections between different parties.
- **Deception:** Adding out of context messages from a fraudulent source into a communication network. This will lead to mistrust between the parties communicating and may also cause loss of critical data.
- **Modification in the Content:** Changing the content of a message. This includes inserting new information or deleting/changing the existing one.
- **Modification in the sequence:** Changing the order of messages between parties. This includes insertion, deletion, and reordering of messages.
- **Modification in the Timings:** This includes replay and delay of messages sent between different parties. This way session tracking is also disrupted.
- **Source Refusal:** When the source denies being the originator of a message.
- **Destination refusal:** When the receiver of the message denies the reception.

3. a) Explain about Web Security considerations 6M

Ans

Websites are always to prone to security risks. **Cyber crime** impacts your business by hacking your website. Your website is then used for hacking assaults that install malicious software or malware on your visitor's computer.

Hackers may also steal important customer data such as credit card information, destroy your business and propagate illegal content to your users.

Web Security deals with the security of data over the internet/network or web or while it is being transferred over the internet. Web security is crucial for protecting web applications, websites, and the underlying servers from malicious attacks and unauthorized access. In this article, we will discuss about web security.

Security Considerations

Updated Software

It is mandatory to keep you software updated. It plays vital role in keeping your website secure.

SQL Injection

It is an attempt by the hackers to manipulate your database. It is easy to insert rogue code into your query that can be used to manipulate your database such as change tables, get information or delete data.

Cross Site Scripting (XSS)

It allows the attackers to inject client side script into web pages. Therefore, while creating a form It is good to endure that you check the data being submitted and encode or strip out any HTML.

Error Messages

You need to be careful about how much information to be given in the error messages. For example, if the user fails to log in the error message should not let the user know which field is incorrect: username or password.

Validation of Data

The validation should be performed on both server side and client side.

Passwords

It is good to enforce password requirements such as of minimum of eight characters, including upper case, lower case and special character. It will help to protect user's information in long run.

Upload files

The file uploaded by the user may contain a script that when executed on the server opens up your website.

SSL

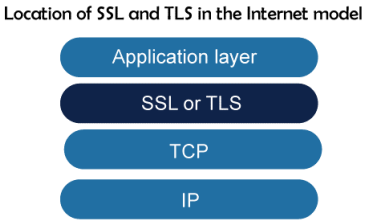
It is good practice to use SSL protocol while passing personal information between website and web server or database.

b) What is Secure Socket Layer and explain briefly 6M

Ans

Secure Socket Layer (SSL) provides security to the data that is transferred between web browser and server. SSL encrypts the link between a web server and a browser which ensures that all data passed between them remain private and free from attack. In this article, we are going to discuss SSL in detail, its protocols, the silent features of SSL, and the version of SSL.
SSL is the older version of what we now call TLS (Transport Layer Security).
Websites using SSL/TLS have "HTTPS" in their URL instead of "HTTP."
How does SSL work?

- **Encryption**: SSL encrypts data transmitted over the web, ensuring privacy. If someone intercepts the data, they will see only a jumble of characters that is nearly impossible to decode.
- **Authentication**: SSL starts an authentication process called a handshake between two devices to confirm their identities, making sure both parties are who they claim to be.
- **Data Integrity**: SSL digitally signs data to ensure it hasn't been tampered with, verifying that the data received is exactly what was sent by the sender.



Services Offered by SSL:

On data that has been received from the application layer, SSL offers a number of services:

- ***Fragmentation*** - The data is first divided into blocks by SSL that are 214 bytes or shorter.
- ***Compression*** - One of the lossless compression techniques agreed upon by the client and server is used to compress every data fragment. This service is not required.
- ***Message Integrity*** - A keyed-hash function is used by SSL to generate a MAC in order to protect the integrity of the data.
- ***Confidentiality*** - Strictly speaking, symmetric-key cryptography is used to encrypt both the original data and the MAC in order to maintain confidentiality.
- ***Framing*** - The encrypted payload receives a header. After that, a dependable transport-layer protocol receives the payload.

4. Explain different Principles of Mobile Device Security 12M

Ans

Mobile device security is a comprehensive approach to protecting mobile devices, ensuring they remain secure and prevent unauthorized access to corporate data.

The Importance of Mobile Device Security

1. Data Protection: Mobile devices often store and access sensitive information, including personal data, financial records, and corporate information. Protecting this data from unauthorized access and breaches is critical.
2. Privacy Preservation: With the increasing amount of personal data stored on mobile devices, ensuring user privacy is essential to maintain trust and comply with regulatory requirements.
3. Business Continuity: Mobile devices are integral to business operations. Securing these endpoints helps prevent disruptions caused by cyberattacks, ensuring business continuity.
4. Compliance: Many industries are subject to regulatory requirements concerning data protection and privacy. Effective mobile device security helps organizations comply with these regulations.

Common Threats to Mobile Devices

Mobile devices are susceptible to a variety of security threats, including:

1. Malware: Malicious software designed to infect mobile devices, steal data, or cause damage. Common types of mobile malware include trojans, spyware, and ransomware.
2. Phishing Attacks: Attempts to trick users into revealing sensitive information, such as login credentials or financial details, through deceptive emails, messages, or websites.

3. Network Attacks: Exploiting vulnerabilities in wireless networks to intercept data or gain unauthorized access to devices. This includes man-in-the-middle attacks and rogue Wi-Fi hotspots.
4. Device Theft and Loss: Physical theft or loss of a mobile device can result in unauthorized access to sensitive information.
5. App-Based Threats: Malicious or poorly secured applications that can compromise device security and data privacy.
6. OS and Software Vulnerabilities: Exploiting weaknesses in the operating system or installed software to gain unauthorized access or control over the device.

Mobile device security is essential for protecting sensitive information and ensuring the integrity of mobile systems. Here are some key principles of mobile device security:

1. **Authentication**:
   - Ensure that users are who they claim to be through strong authentication methods (e.g., biometrics, passwords, PINs).
2. **Access Control**:
   - Implement strict access controls to limit who can access specific applications and data based on user roles and permissions.
3. **Data Encryption**:
   - Encrypt sensitive data stored on the device and during transmission to protect it from unauthorized access.
4. **Regular Updates and Patch Management**:
   - Keep the operating system and applications updated to protect against vulnerabilities and security flaws.
5. **Application Security**:
   - Use secure coding practices for mobile applications and regularly assess third-party apps for security risks.
6. **Remote Wipe and Lock**:
   - Implement features that allow remote wiping or locking of devices if they are lost or stolen, ensuring that data remains secure.
7. **Network Security**:
   - Use secure connections (like VPNs) when accessing public Wi-Fi networks to protect data from interception.
8. **User Education and Awareness**:
   - Train users on security best practices, such as recognizing phishing attempts and managing app permissions responsibly.
9. **Secure Backup**:
   - Regularly back up data in a secure manner to ensure recovery in case of loss or damage.
10. **Device Management**:
    - Utilize Mobile Device Management (MDM) solutions to enforce security policies, monitor device compliance, and manage updates.
11. **Threat Detection and Response**:
    - Implement tools to detect and respond to security threats in real time, such as malware detection and anomaly monitoring.

By adhering to these principles, organizations can significantly enhance the security of their mobile devices and protect sensitive information from various threats.

5. Briefly explain about Pretty Good Privacy in Email Security 12M

Ans

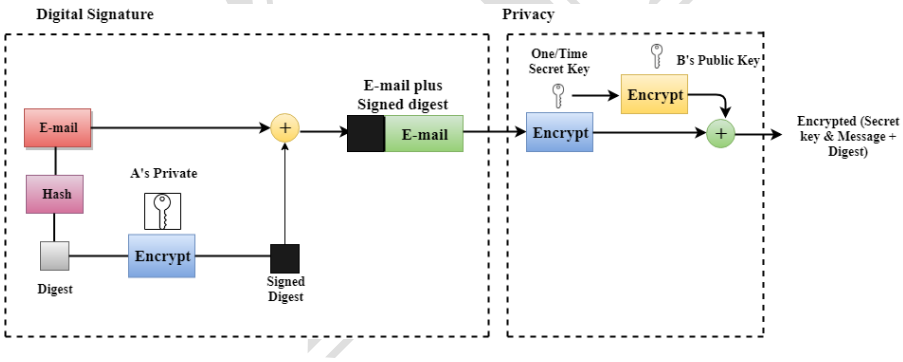
PGP

- PGP stands for Pretty Good Privacy (PGP) which is invented by Phil Zimmermann.
- PGP was designed to provide all four aspects of security, i.e., privacy, integrity, authentication, and non-repudiation in the sending of email.
- PGP uses a digital signature (a combination of hashing and public key encryption) to provide integrity, authentication, and non-repudiation. PGP uses a combination of secret key encryption and public key encryption to provide privacy. Therefore, we can say that the digital signature uses one hash function, one secret key, and two private-public key pairs.
- PGP is an open source and freely available software package for email security.
- PGP provides authentication through the use of Digital Signature.
- It provides confidentiality through the use of symmetric block encryption.
- It provides compression by using the ZIP algorithm, and EMAIL compatibility using the radix-64 encoding scheme.

Following are the steps taken by PGP to create secure e-mail at the sender site:

- The e-mail message is hashed by using a hashing function to create a digest.
- The digest is then encrypted to form a signed digest by using the sender's private key, and then signed digest is added to the original email message.
- The original message and signed digest are encrypted by using a one-time secret key created by the sender.
- The secret key is encrypted by using a receiver's public key.
- Both the encrypted secret key and the encrypted combination of message and digest are sent together.

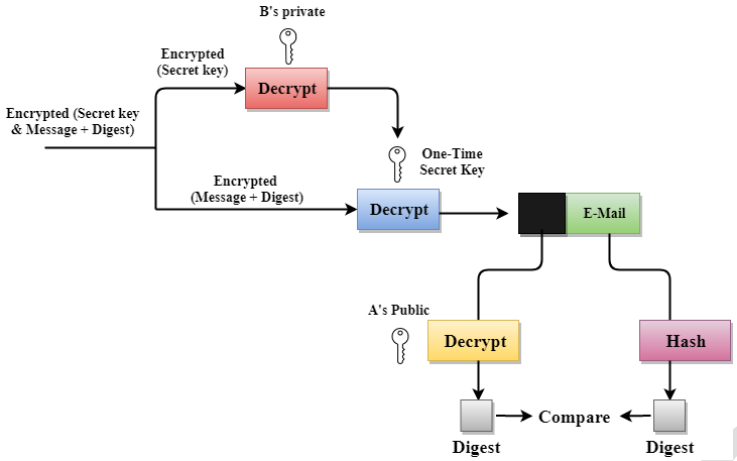
PGP at the Sender site (A)



Following are the steps taken to show how PGP uses hashing and a combination of three keys to generate the original message:

- The receiver receives the combination of encrypted secret key and message digest is received.
- The encrypted secret key is decrypted by using the receiver's private key to get the one-time secret key.
- The secret key is then used to decrypt the combination of message and digest.
- The digest is decrypted by using the sender's public key, and the original message is hashed by using a hash function to create a digest.
- Both the digests are compared if both of them are equal means that all the aspects of security are preserved.

PGP at the Receiver site (B)



6. a) Explain about Authentication Header with neat diagram 6M

AnsAuthentication Header (AH) is used to provide integrity and authentication to IP datagrams. Replay protection is also possible. The services are connectionless, that means they work on a per-packet basis.

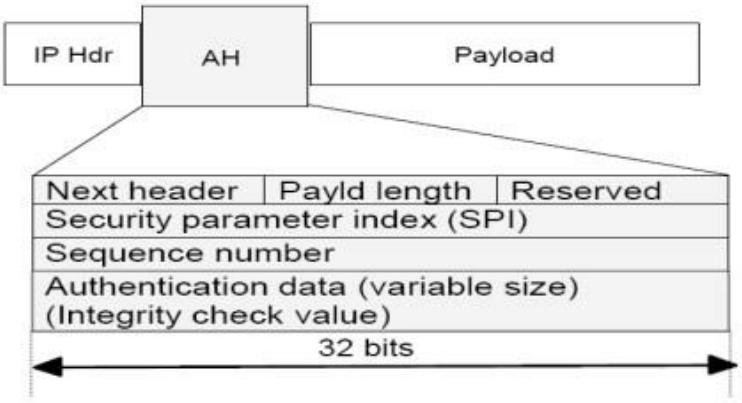
AH is used in two modes as follows −

- Transport mode
- Tunnel mode

AH authenticates are the same as IP datagram. In transport mode, some fields in the IP header change en-route and their value cannot be predicted by the receiver. These fields are called mutable and they are not protected by AH.

AH format

The AH format is described in RFC 2402. The below shows the position of the Authentication Header fields in the IP packet.



The fields are as follows −

Next header

It is an 8-bit field which identifies the type of what follows. The value of this field is chosen from the set of IP header protocol fields, which is set to 51, and the value that would have gone in the protocol field goes in the AH next header field.

Payload length

It is an 8 bits long field and contains the length of the AH header expressed in 32-bit words, minus 2. It does not relate to the actual payload length of the IP packet. Suppose if default options are used, the value is 4 (three 32-bit fixed words plus three 32-bit words of authentication data minus two).

Reserved

It is reserved for future use. Its length is 16 bits and it is set to zero.

Security parameter index (SPI)

It is 32 bits in length.

Sequence number

This 32-bit field is a monotonically increasing counter, which is used for replay protection. It is an optional field. The sender always includes this field, and it is at the discretion of the receiver to process it or not. Starting the sequence number is initialized to zero. The first packet transmitted using the SA has a sequence number of 1. Sequence numbers are not allowed to repeat.

Authentication data

This is a variable-length field containing the Integrity Check Value (ICV), and is padded to 32 bits for IPv4 or 64 bits for IPv6.

b) What is the process behind Virtual Elections explain briefly 6M

Ans

The Important Uses of Cryptography in Electronic Voting and Counting

Cryptography offers a number of benefits to electronic voting and counting solutions. It may be used to perform tasks such as encrypting votes and digital ballot boxes, ensuring votes and software are unmodified, verifying the identity of a voter before he or she casts a ballot, and assisting in auditing and tallying the results of an election.. Considering the paramount importance of ballot secrecy and fraud detection, cryptography has proved a useful tool for countries employing election technologies.

Encryption and Decryption

Encryption and decryption are among the most common uses of cryptography. Encryption is the process of obscuring information, and decryption reverses this process. Keys are the secret piece of information necessary to encrypt and decrypt data. Encrypted data is unintelligible; and without the correct decryption key, it cannot be recreated in its original form. An example of a very simple encryption key is to increment each letter in a block of text by one letter (i.e., "a" becomes "b," "b" becomes "c," etc.), so "Election Day" would become "Fmfdujpo Ebz". Decryption of the text requires that each letter be decremented by one.

For electoral purposes, encryption is often used to obscure the contents of a voter's ballot selections and the contents of a digital ballot box. The voter's encrypted ballot selections may be stored on a voting machine or sent over an insecure channel like the Internet or the telephone network. When casting an electronic vote, the value of the vote will be encrypted using an encryption key produced by the EMB and available at all electronic voting locations. However, only the EMB will have the key that is needed to decrypt encrypted data.

Hash Functions

Another cryptographic function is the hash (often called cryptographic hashes). Hashes are mathematical functions or equations that "read in" a piece of information (e.g., a file) and output a set of numbers and letters that are unique to the input. Just as with encryption, there are different hashing algorithms with unique characteristics. Using the SHA-256 hashing algorithm, the word "election" hashes to: c7a19845b9e9de079260094d79525957. But when using the same algorithm and inputting the word "elections" (notice there is only a one-letter difference), the output is completely different: b9dd4e28c0fe5673909bb6c0615f5f22. This is the point of hashes – detecting changes. A file of any size can be passed through the hashing algorithm, even large and complex computer programs. Hashes can identify a one-character modification to a vote stored on a computer, the software running on a voting machine, or even an entire operating system.

Digital Signatures

Digital signatures are mathematical functions that work in a similar manner to cryptographic hashes and also help identify who sent a message or file. Digital signatures are not analogous to physical handwritten signatures as they provide much stronger proof of who "signed" a message. A digital signature is different for every message, making it much more difficult to forge another person's signature. In elections, digital signatures are used to "sign" the contents of a digital ballot box or a

voter's ballot selections, thus helping ensure the ballot box or vote was not altered. If tampering occurred and the digital signature was forged, the attacker would need to know another person's, or the EMB's, secret key.

Mix-Nets

The order in which data is stored on electronic voting or counting systems can be used to link the identity of the voter to the value of the vote, if the order in which voters cast their ballots is also observed. Cryptographic schemes have been developed to protect the secrecy of stored votes. A mix-net takes encrypted, stored data and then re-encrypts it and mixes the order in which it is stored. Only then are the data decrypted and the values of the votes revealed. As the order of the original vote data has been changed and the encrypted value of the stored vote data has also been changed (it was re-encrypted as it passed through the mix-net), there is no way that decrypted vote values can be linked back to either the original data received or the identity of voters.

Homomorphic Cryptography

Another solution used to protect the secrecy of stored votes is homomorphic cryptography, which allows the votes in the electronic ballot box to be tabulated while still encrypted. As individual votes are never decrypted, there is no possibility of linking voters to the way that they voted. Votes may even be posted to a public bulletin board for independent tabulation by anyone to verify the outcome of the election.

SET-2

1. Explain about Digital Signatures in detail 6M

Ans

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.

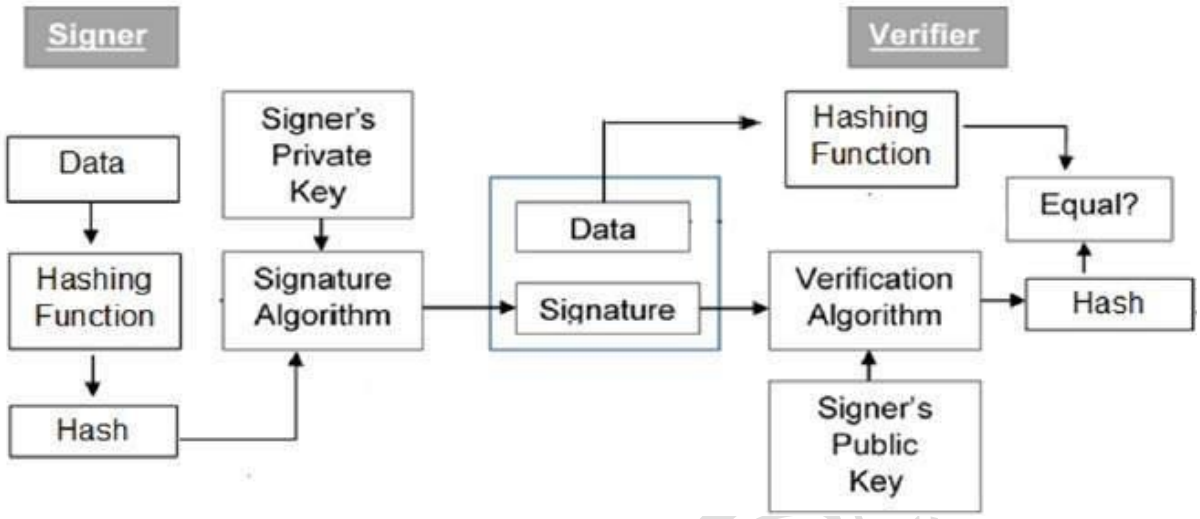
Similarly, a digital signature is a technique that binds a person/entity to the digital data. This binding can be independently verified by receiver as well as any third party.

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.

2 Briefly discuss about public key Infrastructure 6M

Ans

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.

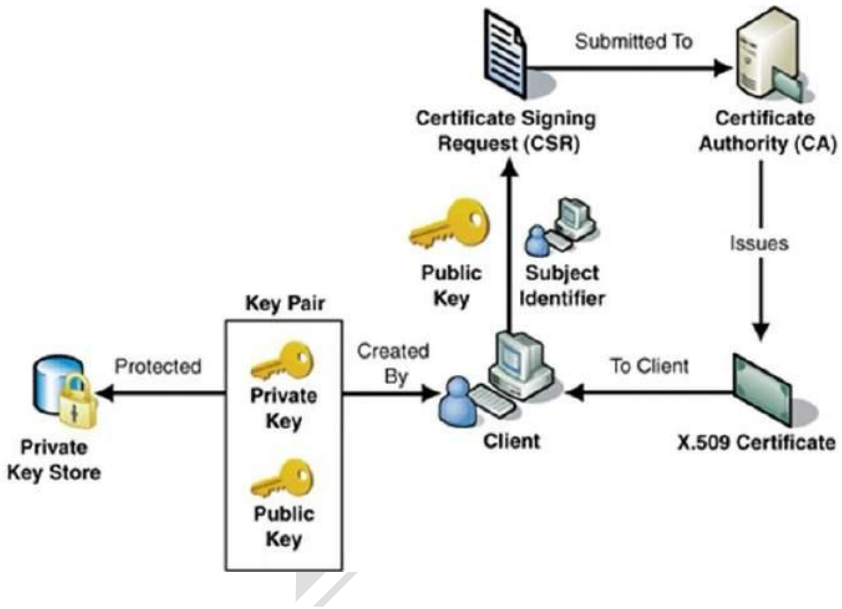
Digital Certificate

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.



3. a) Explain what is Transport Layer Security (TLS) 6M

Ans

TRANSPORT LAYER SECURITY

Transport layer security protocol is one of the security protocols which are designed to facilitate privacy and data security for communications over the Internet. The main use of TLS is to encrypt the communication between web applications and servers, like web browsers loading a website.

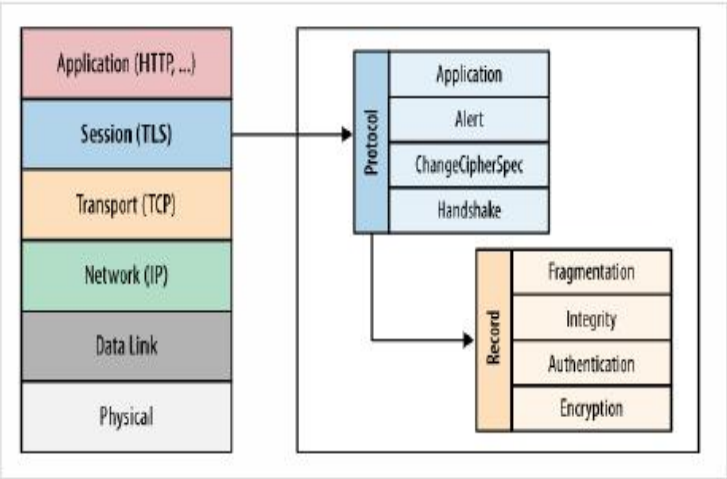
TLS is used to encrypt other communications like email, messaging, and voice over IP (VoIP). TLS was proposed by the Internet Engineering Task Force (IETF), which is an international standards organization.

Components

The three main components that TLS accomplishes are as follows −

- **Encryption** − It is used to hide the data being transferred from third parties.
- **Authentication** − It always ensures that the parties exchanging information are who they claim to be.
- **Integrity** − Integrity verifies that the data has not been tampered with.

Given below is the pictorial representation of the **Transport layer security protocol**



Transport Layer Securities (TLS) are designed to provide security at the transport layer. TLS was derived from a security protocol called Secure Socket Layer (SSL). TLS ensures that no third party may eavesdrop or tampers with any message.
There are several benefits of TLS:

- **Encryption:**
  TLS/SSL can help to secure transmitted data using encryption.
- **Interoperability:**
  TLS/SSL works with most web browsers, including Microsoft Internet Explorer and on most operating systems and web servers.
- **Algorithm flexibility:**
  TLS/SSL provides operations for authentication mechanism, encryption algorithms and hashing algorithm that are used during the secure session.
- **Ease of Deployment:**
  Many applications TLS/SSL temporarily on a windows server 2003 operating systems.

- **Ease of Use:**
  Because we implement TLS/SSL beneath the application layer, most of its operations are completely invisible to client.

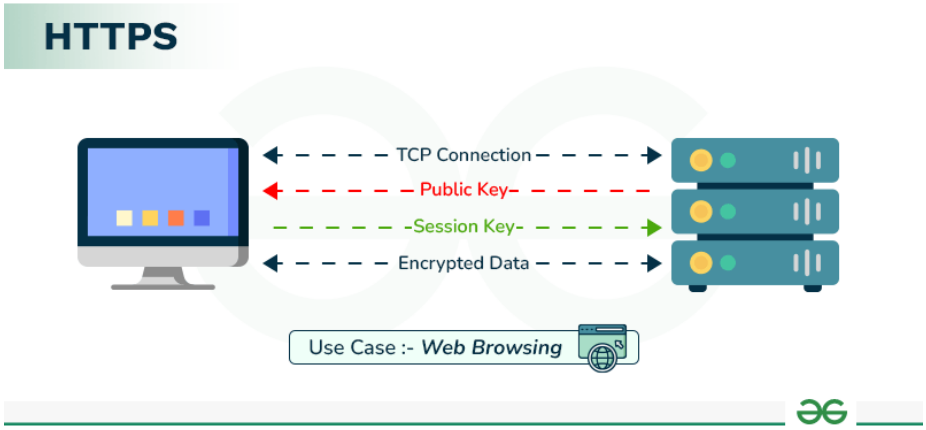
b. Explain about HTTPS in detail 6M

Ans

HTTPS stands for **HyperText Transfer Protocol Secure**. It is the most common protocol for sending data between a web browser and a website. In this article, we will discuss HTTPS, the Working of HTTPS, advantages of HTTPS. We will also discuss SSL (Secure Socket Layer) in this article.

What is Hypertext Transfer Protocol Secure?

Hypertext Transfer Protocol Secure is a protocol that is used to communicate between the user browser and the website. It also helps in the transfer of data. It is the secure variant of HTTP. To make the data transfer more secure, it is encrypted. Encryption is required to ensure security while transmitting sensitive information like passwords, contact information, etc.



HTTP vs HTTPS

Below are the basic differences between the HTTP and HTTPS.

HTTP	HTTPS
HTTP stands for HyperText Transfer Protocol.	HTTPS stands for HyperText Transfer Protocol Secure.
URL begins with “http://”.	URL starts with “https://”.
HTTP Works at the Application Layer.	HTTPS works at Transport Layer.
HTTP speed is faster than HTTPS.	HTTPS speed is slower than HTTP.

For more differences between these two, refer to the article Difference between http:// and https://.

HTTPS establishes the communication between the browser and the web server. It uses the **Secure Socket Layer** (SSL) and **Transport Layer Security** (TLS) protocol for establishing communication. The new version of SSL is

4. Explain IEEE802.11 frame structure in detail. 12M

Ans

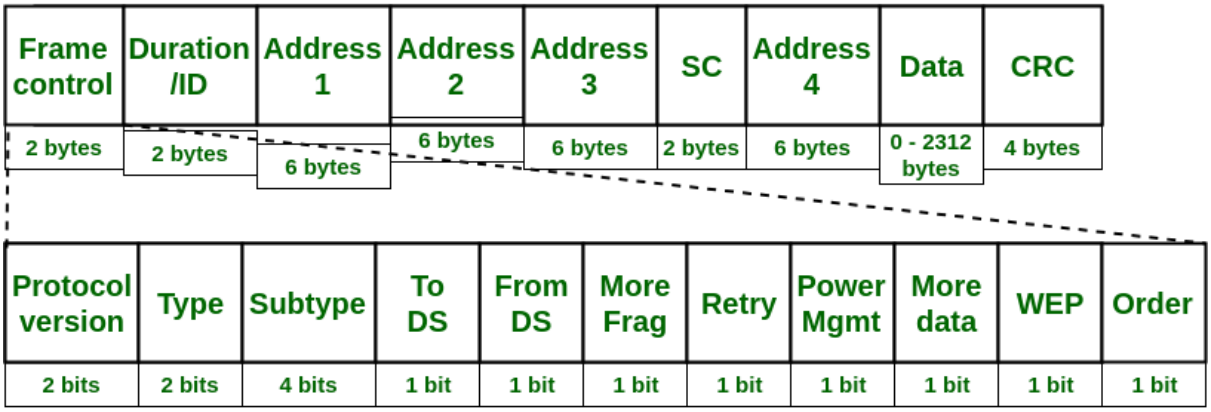
The IEEE 802.11 standard, lays down the architecture and specifications of wireless local area networks (WLANs). WLAN or WiFi uses high frequency radio waves instead of cables for connecting the devices in LAN. Users connected by WLANs can move around within the area of network coverage.

The 802.11 MAC sublayer provides an abstraction of the physical layer to the logical link control sublayer and upper layers of the OSI network. It is responsible for encapsulating frames and describing frame formats.

MAC Sublayer Frame Structure of IEEE 802.11

The main fields of a frame in WLANs as laid down by IEEE 802.11 are as depicted in the following diagram −

control field.



IEEE 802.11 MAC Frame Structure

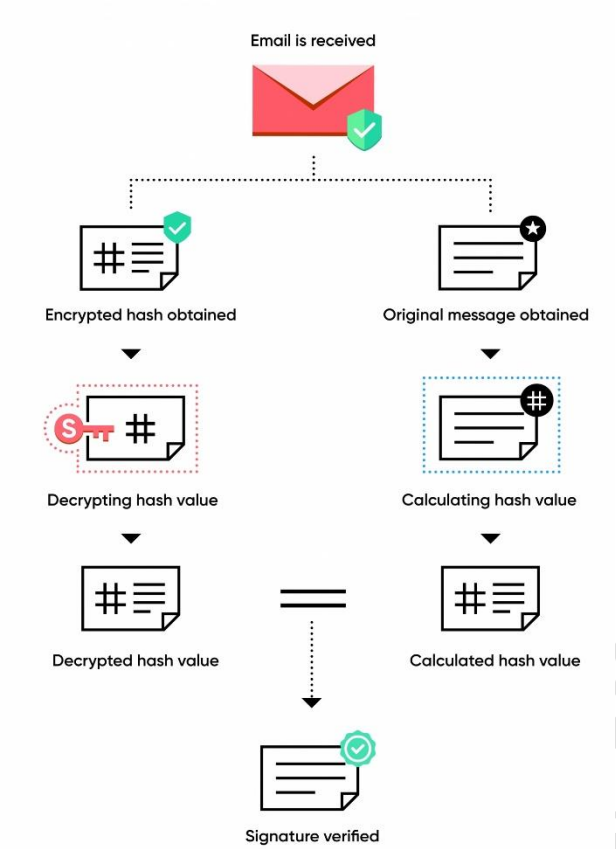
- **Frame Control(FC) –** It is 2 bytes long field which defines type of frame and some control information. Various fields present in FC are:
    1. **Version:** It is a 2 bit long field which indicates the current protocol version which is fixed to be 0 for now.
    2. **Type:** It is a 2 bit long field which determines the function of frame i.e management(00), control(01) or data(10). The value 11 is reserved.
    3. **Subtype:** It is a 4 bit long field which indicates sub-type of the frame like 0000 for association request, 1000 for beacon.
    4. **To DS:** It is a 1 bit long field which when set indicates that destination frame is for DS(distribution system).
    5. **From DS:** It is a 1 bit long field which when set indicates frame coming from DS.
    6. **More frag (More fragments):** It is 1 bit long field which when set to 1 means frame is followed by other fragments.

7. **Retry:** It is 1-bit long field, if the current frame is a retransmission of an earlier frame, this bit is set to 1.
8. **Power Mgmt (Power management):** It is 1-bit long field that indicates the mode of a station after successful transmission of a frame. Set to 1 the field indicates that the station goes into power-save mode. If the field is set to 0, the station stays active.
9. **More data:** It is 1-bit long field that is used to indicate receiver that a sender has more data to send than the current frame. This can be used by an access point to indicate to a station in power-save mode that more packets are buffered or it can be used by a station to indicate to an access point after being polled that more polling is necessary as the station has more data ready to transmit.
10. **WEP:** It is 1 bit long field which indicates that the standard security mechanism of 802.11 is applied.
11. **Order:** It is 1 bit long field, if this bit is set to 1 the received frames must be processed in strict order.

- **Duration/ID –** It is 4 bytes long field which contains the value indicating the period of time in which the medium is occupied(in μs).
- **Address 1 to 4 –** These are 6 bytes long fields which contain standard IEEE 802 MAC addresses (48 bit each). The meaning of each address depends on the DS bits in the frame control field.
- **SC (Sequence control) –** It is 16 bits long field which consists of 2 sub-fields, i.e., Sequence number (12 bits) and Fragment number (4 bits). Since acknowledgement mechanism frames may be duplicated hence, a sequence number is used to filter duplicate frames.
- **Data –** It is a variable length field which contain information specific to individual frames which is transferred transparently from a sender to the receiver(s).
- **CRC (Cyclic redundancy check) –** It is 4 bytes long field which contains a 32 bit CRC error detection sequence to ensure error free frame.

5. a) Explain S/MIME architecture in detail. 6M

Ans



S/MIME

Email is probably the most used mode of communication today not only for casual chat purposes but for the transmission of very sensitive information. It could be business plans, personal information, or other important documents, all of which you would want to be sure are safe in your email.

S/MIME can do both symmetric encryption and digital signatures, which are two very important functions for securing emails in the best possible way.

Symmetric encryption guarantees that only the addressee will be able to read your email, and digital signatures identify who it came from and show that it wasn't changed on its way to your inbox. With S/MIME, you will be able to protect your communication against unwanted readers and establish trust with those receiving your emails.

What is S/MIME

S/MIME stands for Secure/Multipurpose Internet Mail Extensions. Through encryption, S/MIME offers protection for business emails.

S/MIME comes under the concept of Cryptography. S/MIME is a protocol used for encrypting or decrypting digitally signed E-mails. This means that users can digitally sign their emails as the owner(sender) of the e-mail.

Emails could only be sent in NVT 7-bit format in the past, due to which images, videos, or audio were not a part of e-mail attachments. Bell Communications launched the MIME standard protocol in 1991 to increase the email's restricted functionality.

S/MIME is an upgrade of MIME(Multipurpose Internet Mail Extensions). Due to the limitations of MIME, S/MIME came into play. S/MIME is based on asymmetric cryptography which means that communications can be encrypted or decrypted using a pair of related keys namely public and private keys.
How S/MIME Works?

S/MIME enables non-ASCII data to be sent using Secure Mail Transfer Protocol (SMTP) via email. Moreover, many data files are sent, including music, video, and image files. This data is securely sent using the encryption method.

The data which is encrypted using a public key is then decrypted using a private key which is only present with the receiver of the E-mail. The receiver then decrypts the message and then the message is used.

In this way, data is shared using e-mails providing an end-to-end security service using the cryptography method.

Advantages of S/MIME

1. It offers verification.
2. It offers integrity to the message.
3. By the use of digital signatures, it facilitates non-repudiation of origin.
4. It offers seclusion.
5. Data security is ensured by the utilization of encryption.
6. Transfer of data files like images, audio, videos, documents, etc. in a secure manner.

Services of S/MIME

1. Digital Signature, which can maintain data integrity.
2. S/MIME can be used in encrypting messages.
3. By using this we can transfer our data using an e-mail without any problem

b) Explain Combining Security Associations. 6M

Ans

COMBINING SECURITY ASSOCIATIONS

An individual SA can implement either the AH or ESP protocol but not both. Sometimes a particular traffic flow will call for the services provided by both AH and ESP. Further, a particular traffic flow may require IPsec services between hosts and, for that same flow, separate services between security gateways, such as fire-walls. In all of these cases, multiple SAs must be employed for the same traffic flow to achieve the desired IPsec services. The term *security association bundle* refers to a sequence of SAs through which traffic must be processed to provide a desired set of IPsec services. The SAs in a bundle may terminate at different endpoints or at the same endpoints.

Security associations may be combined into bundles in two ways:

- **Transport adjacency:** Refers to applying more than one security protocol to the same IP packet without invoking tunneling. This approach to combining AH and ESP allows for only one level of combination; further nesting yields no added benefit since the processing is performed at one IPsec instance: the (ultimate) destination.

- **Iterated tunneling:** Refers to the application of multiple layers of security protocols effected through IP tunneling. This approach allows for multiple levels of nesting, since each tunnel can originate or terminate at a different IPsec site along the path.

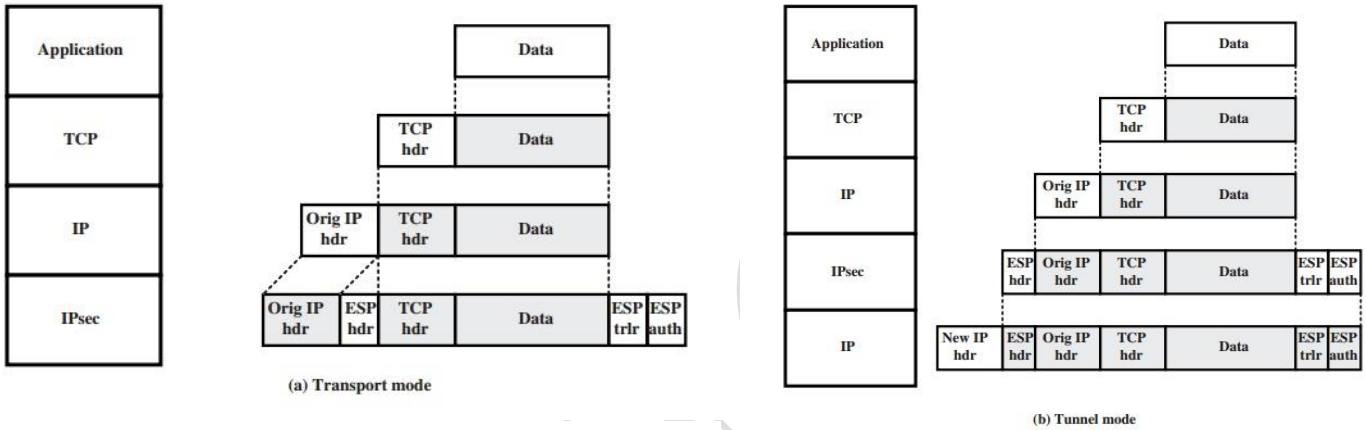


Figure 19.9 Protocol Operation for ESP

The two approaches can be combined, for example, by having a transport SA between hosts travel part of the way through a tunnel SA between security gateways. One interesting issue that arises when considering SA bundles is the order in which authentication and encryption may be applied between a given pair of endpoints and the ways of doing so. We examine that issue next. Then we look at combinations of SAs that involve at least one tunnel.

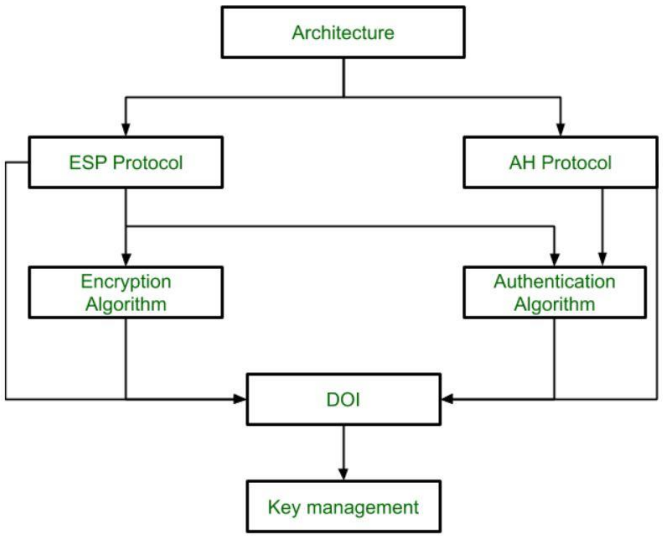
6. a) Explain IP Security Architecture. 6M

Ans

IPSec (IP Security) architecture uses two protocols to secure the traffic or data flow. These protocols are ESP (Encapsulation Security Payload) and AH (Authentication Header). IPSec Architecture includes protocols, algorithms, DOI, and Key Management. All these components are very important in order to provide the three main services:

- Confidentiality
- Authentication
- Integrity

IP Security Architecture:



1. Architecture: Architecture or IP Security Architecture covers the general concepts, definitions, protocols, algorithms, and security requirements of IP Security technology.
2. ESP Protocol: ESP(Encapsulation Security Payload) provides a confidentiality service. Encapsulation Security Payload is implemented in either two ways:

- ESP with optional Authentication.
- ESP with Authentication.

3. Encryption algorithm: The encryption algorithm is the document that describes various encryption algorithms used for Encapsulation Security Payload.
4. AH Protocol: AH (Authentication Header) Protocol provides both Authentication and Integrity service. Authentication Header is implemented in one way only: Authentication along with Integrity.
Authentication Header covers the packet format and general issues related to the use of AH for packet authentication and integrity.
5. Authentication Algorithm: The authentication Algorithm contains the set of documents that describe the authentication algorithm used for AH and for the authentication option of ESP.
6. DOI (Domain of Interpretation): DOI is the identifier that supports both AH and ESP protocols. It contains values needed for documentation related to each other.
7. Key Management: Key Management contains the document that describes how the keys are exchanged between sender and receiver.

b)What are steps involved in secure Inter-branch Payment Transactions. 6M

Ans

Secure inter-branch payment transactions involve the secure transfer of funds between different branches of a financial institution or bank. The following steps are typically involved in performing secure inter-branch payment transactions:

1. Authentication

- The customer initiating the transaction must be authenticated before any transaction can take place.

- This is typically done using some form of multi-factor authentication, such as a password, PIN, or biometric authentication.

2. Authorization

- Once the customer is authenticated, the transaction must be authorized by the appropriate parties.
- This typically involves verifying that the customer has sufficient funds to cover the transaction and that the recipient account is valid.

3. Encryption

- The transaction details, including the amount and recipient account information, are encrypted to protect against unauthorized access or interception during transmission.

4. Transmission

- The encrypted transaction details are transmitted securely to the recipient branch using a secure communication channel, such as SSL/TLS.

5. Decryption

- Upon receiving the transaction details, the recipient branch decrypts the information to access the transaction details.

6. Verification

- The recipient branch verifies the transaction details to ensure that the transaction is valid and authorized.
- This includes verifying the account information and the availability of sufficient funds.

7. Processing

- If the transaction is valid and authorized, the recipient branch processes the transaction by transferring funds from the sender's account to the recipient's account.
- This typically involves updating the account balances and transaction records.

8. Confirmation

- Both the sender and recipient are provided with a confirmation of the transaction, typically in the form of a receipt or confirmation number.
- This allows both parties to verify that the transaction was completed successfully.