CNS-W-2019

1. Answer ALL the questions:

a. Define attack? List the types of attack.

Ans: A cyber-attack is an exploitation of computer systems and networks. It uses malicious code to alter computer code, logic or data and lead to cybercrimes, such as information and identity theft. The various types of attacks in computer system are Interruption, Interception, Modification, Fabrication

b. What do you mean by plaintext and cipher text?

Ans: The original intelligible messages are plane text and the transformed messages are called cipher text.

c. List out some Transposition techniques.

Ans: rail fence, column transposition technique etc.

d. List down some functions of firewall.

Ans; A firewall works as a barrier, or a shield, between your computer network and internet

- Its purpose is to control what traffic is allowed to be transferred from one side to the other.
- firewalls blocks traffic/data/packet unintended for particular IP addresses or server ports.

e. What is VPN?

Ans: VPN is the virtual private network which makes use of cryptography (IPSec in tunnel mode) to perform private communication through insecure and public internet

f. What are the major threats to Data or Information?

Ans: malware, worms, trojan, virus.

g. What is the role of hash function in cryptography?

Ans: the hash function is used for assure integrity and Authentication.

h. What do you know about Vernam Cipher?

Ans: This uses a substitution technique and is based on the principle that each plaintext character from a message is 'mixed' with one character from a key stream. If a truly random key stream is used, the result will be a truly 'random' ciphertext which bears no relation to the original plaintext.

i. How authentications vary from authorization?

Ans: Authentication means confirming your own identity, whereas authorization means being allowed access to the system.that is authentication is the process of verifying oneself, while authorization is the process of verifying what you have access to

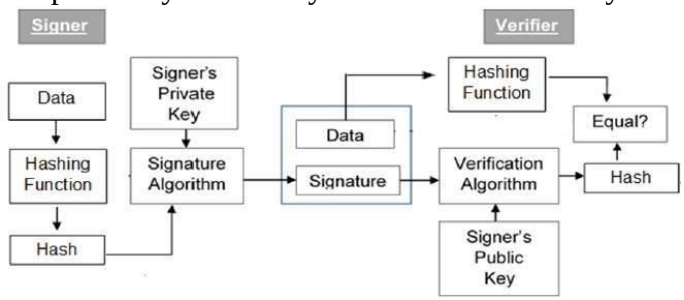
j. Define Encryption and Decryption.

Ans: Encryption is the process of translating plain text data (plaintext) into something that appears to be random and meaningless (ciphertext). Decryption is the process of converting ciphertext back to plaintext.

2. Answer any SIX questions:

a. **Explain Digital Signature algorithm**.

Ans: 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. It is based on public key cryptography.



- 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.

b. Write the difference between block cipher and stream cipher.

Ans:

1. digits are combined with a pseudorandom cipher digit stream. On the other hand, a block cipher is an encryption method that applies a deterministic algorithm along with a symmetric key to encrypt a block of text.
2. Stream cipher uses a different key for each byte whereas; block cipher uses the same key to encrypt each block.
3. Stream cipher uses XOR function for converting the plain text into cipher text that is the reason why it is easy to reverse the XORed bits. In contrast, block cipher do not use XOR function.
4. Stream cipher uses confusion to encrypt plaint text whereas block ciphers use both confusion and diffusion to encrypt plaintext into ciphertext.
5. 1 byte (8 bits) at a time is converted in the stream cipher, this makes the process faster whereas, in block ciphers, the normal size of the block could be 64 or 128 bits in the block cipher and this makes block cipher slower than stream cipher.
6. Stream cipher uses CFB (Cipher Feedback) and OFB (Output Feedback) algorithm modes. On the other hand, block cipher uses ECB (Electronic Code Book) and CBC (Cipher Block Chaining) algorithm modes.
7. Stream Ciphers does not require large memory because they only work on small bits at a time unlike block ciphers that require a relatively large memory because they work on a large chunk of data.
8. Stream ciphers do not provide integrity protection or authentication. On the contrary, some block ciphers (depending on the mode) can provide integrity protection, in addition to confidentiality.

c. Write the procedure of DES algorithm.

Ans: The input to the encryption algorithm are a plaintext block of length 64bits and a key K. the plaintext block is divided into two halves L_0 and R_0 of 32 bits each. The key K of 56 bits is compressed into 48 bits by discarding the 8^{th} bit of each byte. The two halves of the data pass through 16 rounds of processing and then combine to produce the cipher text block. Each round "i" has inputs L_{i-1} and R_{i-1}, derived from the previous round, as well as the subkey K_i, derived from the overall key K. in general, the subkeys K_i 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 has the same general structure for each round but is parameterized by the round sub key K_i. 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.

d. Write short notes on

i.SHTTP

Ans: S-HTTP is a secure HTTP connections. S-HTTP provides a wide variety of mechanisms to provide for confidentiality, authentication, and integrity. S-HTTP is a superset of HTTP, which allows messages to be encapsulated in various ways. Encapsulations can include encryption, signing, or MAC based authentication. This encapsulation can be recursive, and a message can have several security transformations applied to it. S-HTTP also includes header definitions to provide key transfer, certificate transfer, and similar administrative functions. S-HTTP appears to be extremely flexible in what it will allow the programmer to do. S- HTTP also offers the potential for substantial user involvement in, and oversight of, the authentication & encryption activities.

ii.Secure Socket Layer

Ans: The SSL protocol provides

- Confidentiality − Information is exchanged in an encrypted form.
- Authentication − Communication entities identify each other through the use of digital certificates. Web-server authentication is mandatory whereas client authentication is kept optional.
- Reliability − Maintains message integrity checks.

SSL itself is not a single layer protocol rather it is composed of two sub-layers.

- Lower sub-layer comprises of the one component of SSL protocol called as SSL Record Protocol. This component provides integrity and confidentiality services.
- Upper sub-layer comprises of three SSL-related protocol components and an application protocol. Application component provides the information transfer service between client/server interactions.

Technically, it can operate on top of SSL layer as well. Three SSL related protocol components are −

- SSL Handshake Protocol
- Change Cipher Spec Protocol
- Alert Protocol

e. Describe the principle of security

Ans: Data Confidentiality, Data Integrity, Authentication, Availability and Non-repudiation are core principles of modern-day cryptography.

- Confidentiality refers to certain rules and guidelines usually executed under confidentiality agreements which ensure that the information is restricted to certain people or places.
- Data integrity refers to maintaining and making sure that the data stays accurate and consistent over its entire life cycle.
- Authentication is the process of making sure that the piece of data being claimed by the user belongs to it.
- Availability refers to the ability to access data of a resource when it is needed, as such the information has value only if the authorized people can access at right time. Denying access to data nowadays has become a common attack. Imagine a downtime of a live server how costly it can be.
- Non-repudiation refers to ability to make sure that a person or a party associated with a contract or a communication cannot deny the authenticity of their signature over their document or the sending of a message.

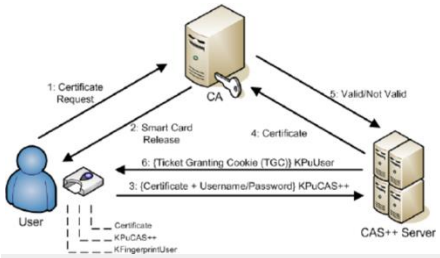
f. List down difference between substitution and transposition techniques.

Ans:

	Substitution techniques	Transposition techniques
Basic	Replaces the plaintext characters with other characters, numbers and symbols.	Rearranges the position of the characters of the plaintext.
Forms	Monoalphabetic and polyalphabetic substitution cipher.	Keyless and keyed transpositional cipher.
Alteration	The identity of the character is changed while its position remains unchanged.	The position of the character is changed in spite of its identity.
Demerits	The letter with the low frequency can discern the plaintext.	Keys near to the correct key can disclose the plaintext.
Example	Caesar Cipher	Reil Fence Cipher

g. Briefly describe the certificate based techniques of authentication.

Ans:



A certificate-based authentication scheme is a scheme that uses a public key cryptography and digital certificate to authenticate a user. A digital certificate is an electronic form that contains identification data, public key, and the digital signature of a certification authority derived from that certification authority's private key. When a user signs on to the server, he provides his digital certificate that has the public key and signature of the certification authority. The server then confirms the validity of the digital signature and if the certificate has been issued by a trusted certificate authority or not. The server then authenticates the user with public key cryptography to confirm the user is in possession of the private key associated with the certificate.

3. Describe Asymmetric key cryptography with RSA algorithm.

Ans: RSA cryptosystem is a public key cryptosystem which has two aspects. Firstly generation of key pair and secondly encryption-decryption algorithms.

1. Generation of RSA Key Pair

The process of generation of keys pair is described below −

a) Generate the RSA modulus (n)

- Select two large primes, p and q.
- Calculate n=p*q. For strong unbreakable encryption, let n be a large number, typically a minimum of 512 bits.

b) Find Derived Number (e)

- Number e must be greater than 1 and less than (p − 1)(q − 1).

- There must be no common factor for e and $(p - 1)(q - 1)$ except for 1. In other words two numbers e and $(p – 1)(q – 1)$ are co prime.

c) Form the public key

- The pair of numbers (n, e) form the RSA public key and is made public.

d) Generate the private key

- Private Key d is calculated from p, q, and e. For given n and e, there is unique number d.
- Number d is the inverse of e modulo $(p - 1)(q – 1)$. This means that d is the number less than $(p - 1)(q - 1)$ such that when multiplied by e, it is equal to 1 modulo $(p - 1)(q - 1)$.
- This can be written as : $ed = 1 \bmod (p - 1)(q - 1)$

The Extended Euclidean Algorithm takes p, q, and e as input and gives d as output.

Example

- Let two primes be p = 7 and q = 13. Thus, modulus $n = pq = 7 \times 13 = 91$.
- Select e = 5, which is a valid choice since there is no number that is common factor of 5 and $(p - 1)(q - 1) = 6 \times 12 = 72$, except for 1.
- The pair of numbers (n, e) = (91, 5) forms the public key.
- Input p = 7, q = 13, and e = 5 to the Extended Euclidean Algorithm. The output will be d = 29.
- Hence, public key is (91, 5) and private keys is (91, 29).

2. Encryption and Decryption

RSA Encryption :

- Suppose the sender wish to send some text message to someone whose public key is (n, e).
- The sender then represents the plaintext as a series of numbers less than n.
- To encrypt the first plaintext P=10 which is a number modulo n, the encryption process is $C = P^e \bmod n$
- plaintext P , we get cipher text $C = 10^5 \bmod 91 = 82$

RSA Decryption :

- Receiver after getting C, the plaintext $P = C^d \bmod n$
- Plaintext = $82^{29} \bmod 91 = 10$

4. What is the role of SET protocol in Internet Security? Describe in detail.

Ans: Secure Electronic Transaction (SET) is a standard protocol that is used for securing credit card transactions over insecure networks. SET itself is not a payment system. It is a a set of security protocols and formats that enables users to employ the existing credit card payment infrastructure on an open network in a secure fashion!

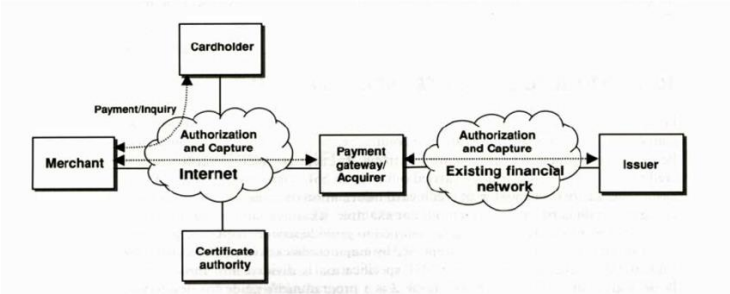
SET has following features:

- Maintains confidentiality of information: Information is provided only to the concerned recipient.
- SET takes care of Integrity of data.
- SET employs a particular subset of protocol for carrying out cardholder account authentication.
- SET employs a particular subset of protocol for carrying out Merchant authentication.

SET process: A SET system includes the following participants:

- Cardholder
- Merchant
- Issuer
- Acquirer
- Payment gateway

- Certification authority



Both cardholders and merchants must register with the CA (certificate authority) first, before they can buy or sell on the Internet. Once registration is done, cardholder and merchant can start to do transactions, which involve nine basic steps in this protocol, which is simplified.

- Customer browses the website and decides on what to purchase
- Customer sends order and payment information, which includes two parts in one message:

a. Purchase order – this part is for merchant
b. Card information – this part is for merchant's bank only.

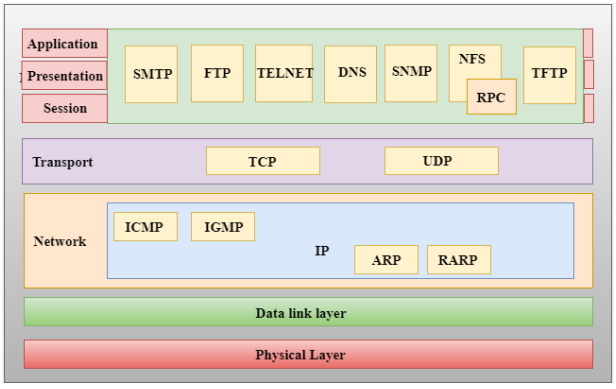
- Merchant forwards card information (part b) to their bank
- Merchant's bank checks with the issuer for payment authorization
- Issuer sends authorization to the merchant's bank
- Merchant's bank sends authorization to the merchant
- Merchant completes the order and sends confirmation to the customer
- Merchant captures the transaction from their bank
- Issuer prints credit card bill (invoice) to the customer

5. Explain the layering architecture of TCP/IP.

Ans:

The TCP/IP model consists of five layers: the application layer, transport layer, network layer, data link layer and physical layer.

The first four layers provide physical standards, network interface, internetworking, and transport functions that correspond to the first four layers of the OSI model and these four layers are represented in TCP/IP model by a single layer called the application layer.



Network Access Layer

- A network layer is the lowest layer of the TCP/IP model.
- A network layer is the combination of the Physical layer and Data Link layer defined in the OSI reference model.

- It defines how the data should be sent physically through the network.
- This layer is mainly responsible for the transmission of the data between two devices on the same network.
- The functions carried out by this layer are encapsulating the IP datagram into frames transmitted by the network and mapping of IP addresses into physical addresses.
- The protocols used by this layer are ethernet, token ring, FDDI, X.25, frame relay.

Internet Layer

- An internet layer is the second layer of the TCP/IP model.
- An internet layer is also known as the network layer.
- The main responsibility of the internet layer is to send the packets from any network, and they arrive at the destination irrespective of the route they take.

Transport Layer

The transport layer is responsible for the reliability, flow control, and correction of data which is being sent over the network.

The two protocols used in the transport layer are User Datagram protocol and Transmission control protocol.

User Datagram Protocol (UDP)

- It provides connectionless service and end-to-end delivery of transmission.
- It is an unreliable protocol as it discovers the errors but not specify the error.
- User Datagram Protocol discovers the error, and ICMP protocol reports the error to the sender that user datagram has been damaged.
- UDP consists of the following fields:

Source port address: The source port address is the address of the application program that has created the message.
Destination port address: The destination port address is the address of the application program that receives the message.
Total length: It defines the total number of bytes of the user datagram in bytes.
Checksum: The checksum is a 16-bit field used in error detection.

- UDP does not specify which packet is lost. UDP contains only checksum; it does not contain any ID of a data segment

Transmission Control Protocol (TCP)

- It provides a full transport layer services to applications.
- It creates a virtual circuit between the sender and receiver, and it is active for the duration of the transmission.
- TCP is a reliable protocol as it detects the error and retransmits the damaged frames. Therefore, it ensures all the segments must be received and acknowledged before the transmission is considered to be completed and a virtual circuit is discarded.

- At the sending end, TCP divides the whole message into smaller units known as segment, and each segment contains a sequence number which is required for reordering the frames to form an original message.
- At the receiving end, TCP collects all the segments and reorders them based on sequence numbers.

Application Layer

- An application layer is the topmost layer in the TCP/IP model.
- It is responsible for handling high-level protocols, issues of representation.
- This layer allows the user to interact with the application.
- When one application layer protocol wants to communicate with another application layer, it forwards its data to the transport layer.
- There is an ambiguity occurs in the application layer. Every application cannot be placed inside the application layer except those who interact with the communication system. For example: text editor cannot be considered in application layer while web browser using HTTP protocol to interact with the network where HTTP protocol is an application layer protocol.

6. What do you mean by secret key cryptography and Public Key Cryptography? How they are different from one another?

Ans: In Private or secret key cryptography the same key (secret key) is used for encryption and decryption. In this key is symmetric because the only key is copy or share by another party to decrypt the cipher text. It is faster than the public key cryptography.

In Public key cryptography two keys are used one key is used for encryption and another key is used for decryption. One key (public key) is used for encrypt the plain text to convert it into cipher text and another key (private key) is used by receiver to decrypt the cipher text to read the message.

SL. No.	Private key cryptography	Public key cryptography
1	Private key is faster than public key.	It is slower than private key.
2	In this, the same key (secret key) and algorithm is used to encrypt and decrypt the message.	In public key cryptography, two keys are used, one key is used for encryption and while the other is used for decryption.
3	In private key cryptography, the key is kept as a secret.	In public key cryptography, one of the two keys is kept as a secret.
4	Private key is Symmetrical because there is only one key that is called secret key.	Public key is Asymmetrical because there are two types of key: private and public key.
5	In this cryptography, sender and receiver need to share the same key.	In this cryptography, sender and receiver does not need to share the same key.
6	In this cryptography, the key is private.	In this cryptography, public key can be public and private key is private.

7. Write short notes on

i) PKIX Model

Ans: Public Key Infrastructure X.509 provides assurance of public key. It provides the identification of public keys and their distribution. PKIX has following components.

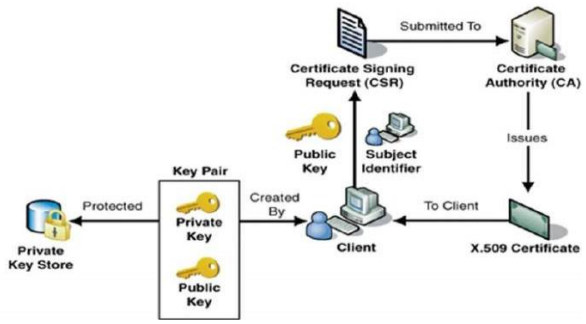
- Public Key Certificate, commonly referred to as 'digital certificate'.
- Private Key tokens.
- Certification Authority.
- Registration Authority.
- Certificate Management System.

o 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.

o 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.

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

o 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.



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.

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.

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.

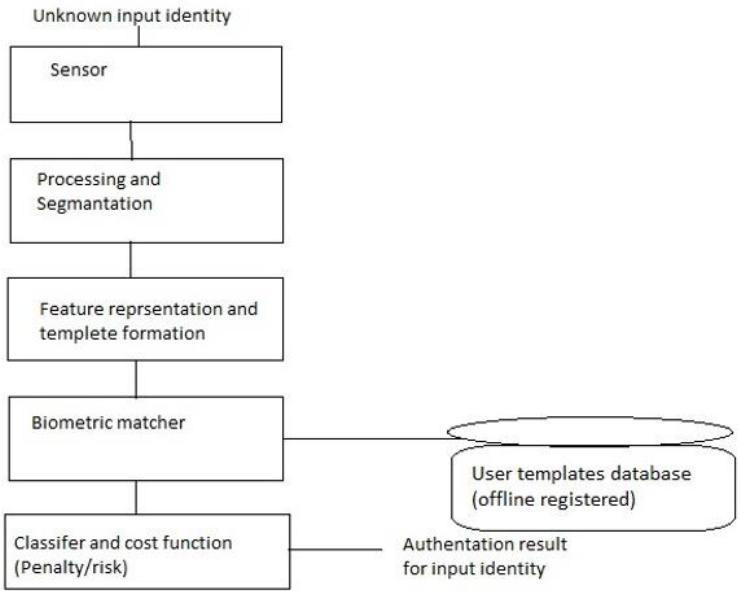
The procedure is given below

- A client whose authenticity is being verified supplies his certificate, generally along with the chain of certificates up to Root CA.
- Verifier takes the certificate and validates by using public key of issuer. The issuer's public key is found in the issuer's certificate which is in the chain next to client's certificate.
- Now if the higher CA who has signed the issuer's certificate, is trusted by the verifier, verification is successful and stops here.
- Else, the issuer's certificate is verified in a similar manner as done for client in above steps. This process continues till either trusted CA is found in between or else it continues till Root CA.

ii) Biometric Authentication

Ans: Biometric authentication is considered the automatic identification or identity verification of an individual using either a biological feature possesses physiological characteristics like a signature.
Biometric can be separated into two main categories:

- Physiological Characteristics: They are related to the shape of the body. The trait that has been used the longest, for over one hundred years, are fingerprints, other examples are face recognition, hand geometry and iris recognition.



- Behavioural Characteristics: They are related to the behaviour of a person. The first characteristics to be used that is still widely used today is the signature.

- Biometric samples are collected using an appropriate sensor. The samples are then processed to correct the deterministic variations like translational and rotational shifts due to interaction of a sensor with the external world. This leads to set of "discriminatory" attributes that are invariant to irrelevant transformation of the input at the sensor.
- Following this segmentation/identification is performed to extract/recognize the desired attributes from the biometric samples.
- Measurements performed on these attributes give features depending upon the representation method.
- The features so obtained are used to form a biometric template. The biometric template is stored in one of the many encrypted forms so as to avoid spoofing.
- Once the database is ready, a query template needs to be authenticated using a matcher so as to determine its similarity with templates in the database.

- The output of the matcher is a matching score which gives the degree of similarity of the query template with various templates. This is used to arrive at a decision using a classifier.