ROEVER ENGINEERING COLLEGE

ELAMBALUR, PERAMBALUR- 621 212
DEPARTMENT OF INFORMATION TECHNOLOGY

CRYPTOGRAPHY AND NETWORK SECURITY

UnitI

1. Specify the four categories of security threads?

- Ø Interruption
- Ø Interception
- Ø Modification
- Ø Fabrication

2. Explain active and passive attack with example?

Passive attack:
Monitoring the message during transmission.
Eg: Interception

Active attack:
It involves the modification of data stream or creation of false data stream.
E.g.: Fabrication, Modification, and Interruption

3. Define integrity and nonrepudiation?

Integrity:
Service that ensures that only authorized person able to modify the message.

Nonrepudiation:
This service helps to prove that the person who denies the transaction is true or false.

4. Differentiate symmetric and asymmetric encryption?
Symmetric
It is a form of cryptosystem in which encryption and decryption performed using the same key. Eg: DES, AES
Asymmetric
It is a form of cryptosystem in which encryption and decryption performed using two keys.
Eg: RSA, ECC

5. Define cryptanalysis?
It is a process of attempting to discover the key or plaintext or both.

6. Compare stream cipher with block cipher with example.

Stream cipher:
Processes the input stream continuously and producing one element at a time.
Example: caeser cipher.

Block cipher:
Processes the input one block of elements at a time producing an output block for each input block.
Example: DES.

7. Define security mechanism

It is process that is designed to detect prevent, recover from a security attack.
Example: Encryption algorithm, Digital signature, Authentication protocols.

8. Differentiate unconditionally secured and computationally secured

An Encryption algorithm is unconditionally secured means, the condition is if the cipher text generated by the encryption scheme doesn't contain enough information to determine corresponding plaintext.

Encryption is computationally secured means,
1. The cost of breaking the cipher exceed the value of enough information.
2. Time required to break the cipher exceed the useful lifetime of information.

9. Define steganography

Hiding the message into some cover media. It conceals the existence of a message.

10. Why network need security?

When systems are connected through the network, attacks are possible during transmission time.

11. Define Encryption

The process of converting from plaintext to cipher text.

12. Specify the components of encryption algorithm.

1. Plaintext
2. Encryption algorithm
3. Secret key
4. Cipher text
5. Decryption algorithm

13. Define confidentiality and authentication

Confidentiality:
It means how to maintain the secrecy of message. It ensures that the information in a computer system and transmitted information are accessible only for reading by authorized person.

Authentication:
It helps to prove that the source entity only has involved the transaction.

14. Define cryptography.

It is a science of writing Secret code using mathematical techniques. The many schemes used for enciphering constitute the area of study known as cryptography.

15. Compare Substitution and Transposition techniques.

SUBSTITUTION	TRANSPOSITION
*A substitution techniques is one in which the letters of plaintext are replaced by other letter or by number or symbols.	It means,different kind of mapping is achieved by performing some sort of permutation on the plaintext letters.
*Eg: Caeser cipher.	*Eg: DES, AES.

16. What are the design parameters of Feistel cipher network?

- Ø Block size
- Ø Key size
- Ø Number of Rounds
- Ø Subkey generation algorithm
- Ø Round function
- Ø Fast software Encryption/Decryption
- Ø Ease of analysis

17. Define Product cipher.

It means two or more basic cipher are combined and it produce the resultant cipher is called the product cipher.

18. Explain Avalanche effect.

A desirable property of any encryption algorithm is that a small change in either the plaintext or the key produce a significant change in the ciphertext. In particular, a change in one bit of the plaintext or one bit of the key should produce a change in many bits of the ciphertext. If the change is small, this might provider a way to reduce the size of the plaintext or key space to be searched.

19. Give the five modes of operation of Block cipher.

1. Electronic Codebook(ECB)
2. Cipher Block Chaining(CBC)
3. Cipher Feedback(CFB)
4. Output Feedback(OFB)
5. Counter(CTR)

20. State advantages of counter mode.

- Hardware Efficiency
- Software Efficiency
- Preprocessing
- Random Access
- Provable Security
- Simplicity.

21. Define Diffusion & confusion.

Diffusion:
It means each plaintext digits affect the values of many ciphertext digits which is equivalent to each ciphertext digit is affected by many plaintext digits. It can be achieved by performing permutation on the data. It is the relationship between the plaintext and ciphertext.

Confusion:
It can be achieved by substitution algorithm. It is the relationship between ciphertext and key.

22. Define Multiple Encryption.

It is a technique in which the encryption is used multiple times.
Eg: Double DES, Triple DES

23. Specify the design criteria of block cipher.

- Ø Number of rounds
- Ø Design of the function F
- Ø Key scheduling

24. Define Reversible mapping.

Each plain text is maps with the unique cipher text. This transformation is called reversible mapping.

25. Specify the basic task for defining a security service.

A service that enhances the security of the data processing systems and the information transfer of an organization. The services are intended to counter security attack, and they make use of one or more security mechanism to provide the service.

26. List the evaluation criteria defined by NIST for AES?
The evaluation criteria for AES is as follows:

- ü Security
- ü Cost
- ü Algorithm and implementation characteristics

27.What is Triple Encryption? How many keys are used in triple encryption?
Triple Encryption is a technique in which encryption algorithm is performed three times using three keys.

UnitII

1. Define the meaning of relatively prime (or) co-prime?

Two integer a and b are relatively prime if gcd(a,b) = 1

Eg: gcd(20,7) = gcd(7,20 mod 7)

= gcd(7,6)

= gcd(6,7 mod 6)

= gcd(1,6 mod 1)

= gcd(1,0)

= 1

2. Define prime number and Divisibility?

Prime Number:

An integer p>1 is a prime number if and only if its divisor are ±1 & ±p

Eg: p= 13 then divisors are ±1 and ±3

Any integer a>1 can be factored in a way as a = p_1

a_1,p_2

a_2,…. p_t

a_t where p1<p2

… p_t , a_i are prime numbers, a' is a +ive integer then it can be written as a = Π_p

a_p. P Є p

where a_p > 0 . p represents set of prime numbers.

3. Using fermat theorem find 5_{14} mod13?

Fermats theorem is a_{p-1} Ξ 1modp

a=5, p=13

5^{13-1} Ξ 1mod13

5^{12} Ξ 1mod13=1

5 $_{14}$=5 $_{12}$.5 $_2$

5 $_2$ Ξ 25mod13

=12mod13=12

5 $_{14}$mod13=(5 $_{12}$.5 $_2$)mod13

=(1.12)mod13

=12mod13

=12

4. Find 27^{-1}mod41 using fermet theorem?

Fermet theorem a $_{p-1}$ Ξ 1modp

multiplicative inverse is a $_{-1}$modp=a $_{p-2}$modp

gn)27 $_{-1}$mod41

a=27,p=41

p-2=41-2=39

27 $_{-1}$mod41=27 $_{39}$mod41(multiple inverse)

27 $_{39}$=27*27 2*27 4*27 32

27 $_2$=729mod41=32

$27^{4} = (3^{2})^{2} \bmod 41$
$= 1024 \bmod 41$
$= 40$
$27^{32} = (27^{4})^{8}$
$= (20)^{8} \bmod 41$
$= 37 \bmod 41$
$= 37$
$27^{39} \bmod 41 = (27*32*20*37) \bmod 41$
$= 38$

5. Define Euler's theorem
Euler's theorem states that for every a and n that are relatively prime:
$a^{\Phi(n)} \equiv\equiv 1 \bmod n$

6. Define Euler's totient function
The Euler's totient function states that, it should be clear for a prime number p,
$\Phi(p) = p-1$

7. Determine Φ (27) using Euler's totient function?
$\Phi(p\ e) = p\ e - p\ e-1$
$\Phi(3\ 3) = 3^{3} - 3\ 2$
$= 27-9$
$= 18$
$\Phi(27) = 18$

8. Define Fermat Theorem?
Fermat Theorem states the following: If p is prime and a is a positive integer not divisible by p, then
$A^{p-1} \equiv 1 \bmod p$

9. Differentiate public key and conventional encryption?

Conventional Encryption	**Public key Encryption**
The same algorithm with the same Key is used for encryption	One algorithm is used for encryption and decryption and decryption with a pair of keys, one for encryption and another fordecryption
The sender and receiver must share the algorithm and the key	The sender and receiver must each have one of the matched pair of keys
The key must be secret	One of two keys must be kept Secret
. It must be impossible or atleast impractial decipher a message if no other information is available message	4. It must be impossible or to at least impractical to decipher a if no other information is available

Knowledge of the algorithm plus samples of cipher text must insufficient to determine the key	Knowledge of the algorithm plus one of key plus samples of ciphertext must be insufficient to determine the other key.

10.What are the principle elements of a public key cryptosystem?

The principle elements of a cryptosystem are:
1.plain text
2.Encryption algoritm
3.Public and private key
4.Cipher text
5.Decryption algorithm

11.What are roles of public and private key?

The two keys used for public-key encryption are referred to as the public key and the private key. Invariably, the private key is kept secret and the public key is known publicly. Usually the public key is used for encryption purpose and the private key is used in the decryption side.

12. Specify the applications of the public key cryptosystem?

The applications of the public-key cryptosystem can classified as follows
1. **Encryption/Decryption**: The sender encrypts a message with the recipient's public key.
2. **Digital signature:** The sender "signs" a message with its private key. Signing is achieved by a cryptographic algorithm applied to a message or to a small block of data that is a function of the message.
3. **Key Exchange:** Two sides cooperate to exchange a session key. Several different approaches are possible, involving the private key(s) of one or both parties.

13. What requirements must a public key cryptosystem to fulfill to a secured algorithm?

The requirements of public-key cryptosystem are as follows:
1. It is computationally easy for a party B to generate a pair(Public key KU_b, Private key KR_b)
2. It is computationally easy for a sender A, knowing the public key and the message to be encrypted , M, to generate the corresponding ciphertext:
$C=E_{KU_b}(M)$
3. It is computationally easy for the receiver B to decrypt the resulting ciphertext using the private key to recover the original message :
$M=D_{KR_b}(C)=D_{KR_b}[E_{KU_b}(M)]$
4. It is computationally infeasible for an opponent , knowing the public key,KU_b,to determine the private key,KR_b.

5. It is computationally infeasible for an opponent , knowing the public key, KU_b, and a ciphertext, C, to recover the original message,M.
6. The encryption and decryption functions can be applied in either order:
$M=E_{KUb}[D_{KRb}(M)]=D_{KUb}[E_{KRb}(M)]$

14. List four general characteristics of schema for the distribution of the public key?
The four general characteristics for the distribution of the public key are
1. Public announcement
2. Publicly available directory
3. Public-key authority
4. Public-key certificate

15. What is a public key certificate?

The public key certificate is that used by participants to exchange keys without contacting a public key authority, in a way that is as reliable as if the keys were obtained directly from the public-key authority. Each certificate contains a public key and other information, is created by a certificate authority, and is given to a participant with the matching private key.

16. What are essential ingredient of the public key directory?

The essential ingredient of the public key are as follows:
1. The authority maintains a directory with a {name, public key} entry for each Participant
2. Each participant registers a public key with the directory authority. Registration would have to be in person or by some form of secure authenticated communication.
3. A participant may replace the existing key with a new one at a time ,either because of the desire to replace a public key that has already been used for a large amount of data, or because the corresponding private key has been comprised in some way.
4. Periodically, the authority publishes the entire directory or updates to the directory. For example, a hard-copy version much like a telephone book could be published, or updates could be listed in a widely circulated newspaper.
5. Participants could also access the directory electronically. For this purpose, secure, authenticated communication from the authority to the participant is mandatory.

17. Perform encryption and decryption using RSA Alg. for the following.

P=7; q=11; e=17; M=8.
Soln:
n = pq
n = 7*11=77
$\varphi(n)=(p-1)(q-1)$
=6*10 = 60
e =17
d =27

$C = M^e \bmod n$
$C = 817 \bmod 77$
$= 57$
$M = C^d \bmod n$
$= 5727 \bmod 77$
$= 8$

18. Describe in general terms an efficient procedure for picking a prime number?
The procedure for picking a prime number is as follows:
1. Pick an odd integer n at random (eg., using a pseudorandom number generator).
2. Pick an integer a<n at random.
3. Perform the probabilistic primality test, such as Miller-Rabin. If n fails the test, reject the value n and go to step 1.
4. If n has passed a sufficient number of tests, accept n; otherwise , go to step 2.

19.What is the primitive root of a number?
We can define a primitive root of a number p as one whose powers generate all the integers from 1 to p-1. That is p, if a is a primitive root of the prime number p then the numbers.

20. User A and B exchange the key using Diffie-Hellman algorithm. Assume α=5 q=11 X_A=2 X_B=3. Find the value of Y_A,Y_B and k?
Soln:
$Y_A = \alpha^{X_A} \bmod q$
$= 25 \bmod 11$
$= 3$
$Y_B = \alpha^{X_B} \bmod q$
$= 125 \bmod 11$
$= 4$
$K = (Y_A)^{X_B} \bmod q$
$= 27 \bmod 11$
$= 5$
$K = (Y_B)^{X_A} \bmod q$
$= 16 \bmod 11$
$= 5$

UnitIII

1.What is a one way function?
One way function is one that map the domain into a range such that every function value has a unique inverse with a condition that the calculation of the function is easy where as the calculations of the inverse is infeasible.

2.What is a trapdoor one way function?
It is function which is easy to calculate in one direction and infeasible to calculate in other direction in the other direction unless certain additional information is known. With the additional information the inverse can be calculated in polynomial time. It can be summarized as: A trapdoor one way function is a family of invertible functions f_k, such that
$Y = f_k(X)$ easy, if k and X are known
$X = f_k^{-1}(Y)$ easy, if k and y are known
$X = f_k^{-1}(Y)$ infeasible, if Y is known but k is not known

3. What is message authentication?
It is a procedure that verifies whether the received message comes from assigned source has not been altered. It uses message authentication codes, hash algorithms to authenticate the message.

4. Define the classes of message authentication function.
- Message encryption: The entire cipher text would be used for authentication.
- Message Authentication Code: It is a function of message and secret key produce a fixed length value.
- Hash function: Some function that map a message of any length to fixed length which serves as authentication.

5.What are the requirements for message authentication?
1. Disclosure:Release of message contents to any person or process
2. Traffic Analysis: Discovery of the pattern of traffic between parties.
3. Masquerade: Insertion of messages into the network from a fraudulent source.
4. Content modification: Changes to the contents of a message.
5. Sequence modification: Any modification to a sequence of messages between parties, including insertion, deletion, and modification.
6. Timing modification: Delay or replay of messages.
7. Source repudiation: Denial of transmission of message by source.
8. Destination repudiation: Denial of receipt of message by destination.

6. What you meant by hash function?
Hash function accept a variable size message M as input and produces a fixed size hash code H(M) called as message digest as output. It is the variation on the message authentication code.

7. Differentiate MAC and Hash function?
MAC: In Message Authentication Code, the secret key shared by sender and receiver. The MAC is appended to the message at the source at a time which the message is assumed or known to be correct.
Hash Function: The hash value is appended to the message at the source at time when the message is assumed or known to be correct. The hash function itself not considered to be secret.

8. Any three hash algorithm.
- MD5 (Message Digest version 5) algorithm.
- SHA_1 (Secure Hash Algorithm).
- RIPEMD_160 algorithm.

9. What are the requirements of the hash function?
- H can be applied to a block of data of any size.
- H produces a fixed length output.
- H(x) is relatively easy to compute for any given x, making both hardware and software implementations practical.

10.What you meant by MAC?
MAC is Message Authentication Code. It is a function of message and secret key which produce a fixed length value called as MAC.
MAC = $C_k(M)$
Where M = variable length message
K = secret key shared by sender and receiver.
$C_K(M)$ = fixed length authenticator.

11. Differentiate internal and external error control.
Internal error control:
In internal error control, an error detecting code also known as frame check sequence or checksum.
External error control:
In external error control, error detecting codes are appended after encryption.

12.What is the meet in the middle attack?
This is the cryptanalytic attack that attempts to find the value in each of the range and domain of the composition of two functions such that the forward mapping of one through the first function is the same as the inverse image of the other through the second function-quite literally meeting in the middle of the composed function.

13.What is the role of compression function in hash function?

The hash algorithm involves repeated use of a compression function f, that takes two inputs and produce a n-bit output. At the start of hashing the chaining variable has an initial value that is specified as part of the algorithm. The final value of the chaining variable is the hash value usually b>n; hence the term compression.

14. What is the difference between weak and strong collision resistance?

Weak collision resistance	Strong resistance collision
For any given block x, it is computationally infeasible to fine y≠x with H(y)=H(x).	It is computationally infeasible to find any pair (x,y) such that H(x)=H(y)
It is proportional to 2^n	It is proportional to $2^{n/2}$

15. Compare MD5, SHA1 and RIPEMD-160 algorithm.

	MD5	**SHA-1**	**RIPEMD160**
Digest length	128 bits	160 bits	160 bits
Basic unit of processing	512 bits	512 bits	512 bits
No of steps	64(4 rounds of 16)	80 (4 rounds of 20)	160 (5 paired rounds of 16)
Maximum message size	∞	2^{64}-1 bits	2^{64}-1 bits
Primitive logical function	4	4	5
Additive constants used	64	4	9
Endianess	Little Endian	Big Endian	Little Endian

16. Distinguish between direct and arbitrated digital signature?

Direct digital signature	**Arbitrated Digital Signature**
The direct digital signature involves only the communicating parties.	The arbiter plays a sensitive and crucial role in this digital signature.
This may be formed by encrypting the entire message with the sender's private key.	Every signed message from a sender x to a receiver y goes first to an arbiter A, who subjects the message and its signature to a number of tests to check its origin and content.

17. What are the properties a digital signature should have?

- Ø It must verify the author and the data and time of signature.
- Ø It must authenticate the contents at the time of signature.
- Ø It must be verifiable by third parties to resolve disputes.

18. What requirements should a digital signature scheme should satisfy?

- The signature must be bit pattern that depends on the message being signed.
- The signature must use some information unique to the sender, to prevent both forgery and denial.
- It must be relatively easy to produce the digital signature.
- It must be relatively easy to recognize and verify the digital signature.
- It must be computationally infeasible to forge a digital signature, either by constructing a new message for anexisting digital signature or by constructing a fraudulent digital signature for a given message.
- It must be practical to retain a copy of the digital signature in storage.

Unit IV

1. Define Kerberos.

Kerberos is an authentication service developed as part of project Athena at MIT. The problem that Kerberos address is, assume an open distributed environment in which users at work stations wish to access services on servers distributed throughout the network.

2. What are the uses of Kerberos?

Kerberos is an authentication service developed as a part of project Athena at MIT.Kerberos provide a centralized authentication server whose functions is to authenticate servers.

3. What 4 requirements were defined by Kerberos?

§ Secure
§ Reliable
§ Transparent
§ Scalable

4. In the content of Kerberos, what is realm?

A full service Kerberos environment consisting of a Kerberos server, a no. of clients, no.of application server requires the following:

§ The Kerberos server must have user ID and hashed password of all participating users in its database.

§ The Kerberos server must share a secret key with each server. Such an environment is referred to as "Realm".

5. Assume the client C wants to communicate server S using Kerberos procedure. How can it be achieved?

Dialogue between client 'C' , server 'S' and authentication server(AS) are given below

a) C → AS: [IDc|| Pc || IDs]

b) AS → C: Ticket

c) C → S: [IDc || ADc || IDs]

Ticket = E_{Ks} [IDc ||ADc || IDs]

Step 1: The user logon to workstation and request access to the server S. The client module C in the workstation request user password and sends message to AS that includes user ID(IDc), server ID(IDc) and its password.

Step 2: Now the AS verify users password against its password database, if it is valid. AS sends the ticket to C that includes user ID(IDc), server ID(IDs) and the address of the client workstation (ADc) are encrypted with key which is shared by both AS and server(S).

Step 3: Now the client use the ticket to server S, to send the message to S with IDc to access service.

6. What is the purpose of X.509 standard?
X.509 defines framework for authentication services by the X.500 directory to its users.X.509 defines authentication protocols based on public key certificates.

7.What are the services provided by PGP services
- Digital signature
- Message encryption
- Compression
- E-mail compatibility
- Segmentation

8. Explain the reasons for using PGP?
a) It is available free worldwide in versions that run on a variety of platforms, including DOS/windows, UNIX, Macintosh and many more.
b) It is based on algorithms that have survived extensive public review and are considered extremely secure.
E.g.) RSA, DSS and Diffie-Hellman for public key encryption, CAST-128, IDEA, 3DES for conventional encryption, SHA-1for hash coding.
c) It has a wide range of applicability from corporations that wish to select and enforce a standardized scheme for encrypting files and communication.
d) It was not developed by nor is it controlled by any governmental or standards organization.

9.Why E-mail compatibility function in PGP needed?

Electronic mail systems only permit the use of blocks consisting of ASCII text. To accommodate this restriction PGP provides the service converting the row 8-bit binary stream to a stream of printable ASCII characters. The scheme used for this purpose is Radix-64 conversion.

10. Name any cryptographic keys used in PGP?
a) One-time session conventional keys.
b) Public keys.
c) Private keys.
d) Pass phrase based conventional keys.

11. Define key Identifier?
PGP assigns a key ID to each public key that is very high probability unique with a user ID. It is also required for the PGP digital signature. The key ID associated with each public key consists of its least significant 64bits.

12. List the limitations of SMTP/RFC 822?
a) SMTP cannot transmit executable files or binary objects.
b) It cannot transmit text data containing national language characters.
c) SMTP servers may reject mail message over certain size.

d) SMTP gateways cause problems while transmitting ASCII and EBCDIC.
e) SMTP gateways to X.400 E-mail network cannot handle non textual data included in X.400 messages.

13. Define S/MIME?
Secure/Multipurpose Internet Mail Extension(S/MIME) is a security enhancement to the MIME Internet E-mail format standard, based on technology from RSA Data Security.

14. What are the elements of MIME?
- Five new message header fields are defined which may be included in an RFC 822 header.
- A number of content formats are defined.
- Transfer encodings are defined that enable the conversion of any content format into a form that is protected from alteration by the mail system.

15. What are the headers fields define in MIME?
- MIME version.
- Content type.
- Content transfer encoding.
- Content id.
- Content description.

16. What is MIME content type and explain?
It is used to declare general type of data. Subtype define particular format for that type of the data. It has 7 content type & 15 subtypes. They are,
1. Text type
- Plain text.

Enriched.
2. Multipart type
- Multipart/mixed.
- Multipart/parallel.
- Multipart/alternative.
- Multipart/digest.

3. Message type
- Message/RFC822.
- Message/partial.
- Message/external.

4. Image type
- JPEG.
- CIF.

5. Video type.
6. Audio type.
7. Application type
- Post script.

• Octet stream.

17. What are the key algorithms used in S/MIME?
• Digital signature standards.
• Diffi Hellman.
• RSA algorithm.

18. Give the steps for preparing envelope data MIME?
• Generate K_s.
• Encrypt K_s using recipient's public key.
• RSA algorithm used for encryption.
• Prepare the 'recipient info block'.
• Encrypt the message using K_s.

19. What you mean by Verisign certificate?
Mostly used issue X.509 certificate with the product name" Verisign digital id". Each digital id contains owner's public key, owner's name and serial number of the digital id.

20. What are the function areas of IP security?
• Authentication
• Confidentiality
• Key management.

21. Give the application of IP security?
• Provide secure communication across private & public LAN.
• Secure remote access over the Internet.
• Secure communication to other organization.

22. Give the benefits of IP security?
• Provide security when IP security implement in router or firewall.
• IP security is below the transport layer is transparent to the application.
• IP security transparent to end-user.
• IP security can provide security for individual user.

23. What are the protocols used to provide IP security?
• Authentication header (AH) protocol.
• Encapsulating Security Payload (ESP) protocol.

24. Specify the IP security services?
• Access control.
• Connectionless integrity.
• Data origin authentication
• Rejection of replayed packet.

• Confidentiality.
• Limited traffic for Confidentiality.

25. What do you mean by Security Association? Specify the parameters that identifies the Security Association?

• An association is a one-way relationship between a sender and receiver that affords security services to the traffic carried on.
• A key concept that appears in both the authentication and confidentiality mechanism for IP is the security association (SA).
A security Association is uniquely identified by 3 parameters:
• Security Parameter Index (SPI).
• IP Destination Address.
• Security Protocol Identifier.

26. What does you mean by Reply Attack?

• A replay attack is one in which an attacker obtains a copy of an authenticated packet and later transmits it to the intended destination.
• Each time a packet is send the sequence number is incremented in the counter by the sender.

27. General format of IPsec ESP Format?

Security Parameter Index(SPI)
Sequence Number(SN)
Payload Data (Variable)
Padding(0-255 bytes)
Authentication Data (variable)

28. Differentiate Transport and Tunnel mode in IPsec?

Transport mode	**Tunnel mode**
1. Provide the protection for upper layer protocol between two hosts.	1. Provide the protection for entire IP Packet.
2. ESP in this mode encrypts and optionally authenticates IP Payload but not IP Header.	2. ESP in this mode encrypt authenticate the entire IP packet.
3. AH in this mode authenticate the IP Payload and selected portion of IP Header.	3. AH in this mode authenticate the entire IP Packet plus selected portion of outer IP Header.

29 . What is Authentication Header? Give the format of the IPsec Authentication Header?

It provides the authentication of IP Packet, so authentication is based on the use of MAC.

FormatofIPsecAuthenticationHeader:

First Header	Payload	Length Reserved
Security Parameter Index(SPI)		
Sequence number(SN)		
Authentication Data(Variable)		

30. List the steps involved in SSL record protocol?

1. SSL record protocol takes application data as input and fragments it.
2. Apply lossless Compression algorithm.
3. Compute MAC for compressed data.
4. MAC and compression message is encrypted using conventional alg.

31. Give SSL record format?

Content type	Major Version	Minor Version	Compressed Length
Plain Text(Optionally Compressed)			
MAC 0, 16 or 20 bytes.			

32. What are the different between SSL version 3 and TLS?

SSL TLS

- In SSL the minor version is 0 and * In TLS, the major version is 3 and the

the major version is 3 minor version is 1.

* SSL use HMAC alg., except that * TLS makes use of the same alg.

the padding bytes concatenation.

* SSL supports 12 various alert * TLS supports all of the alert codes

codes. defined in SSL3 with the exception of

- no _ certificate.

33.What is mean by SET? What are the features of SET?

Secure Electronic Transaction (SET) is an open encryption and security specification designed to protect credit card transaction on the internet.

Features are:

1. Confidentiality of information

2. Integrity of data
3. Cardholder account authentication
4. Merchant authentication

34.What are the steps involved in SET Transaction?

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

35. What is dual signature? What it is purpose?

The purpose of the dual signature is to link two messages that intended for two different recipients.
To avoid misplacement of orders.

UnitV

1. List the 3 classes of intruder?

Classes of Intruders
1) Masquerader
2) Misfeasor
3) Clandestine user

2. Suggest any four password selection strategies and identify their advantages and disadvantages if any.

User education
Computed generated passwords
Reactive password checking
Proactive password checking

3. What is the Objective of intruder?

To gain access to a system

4. What are the schemes used in Password protection?

- One way encryption
  - Store the encrypted form of password
- Access control
  - Accessible only by the authorized user

5. What is the purpose of Salt?

Prevents duplicate password
Increases the length of password
Prevents hardware implementations

6. What is Intrusion Detection?

Detected based on the behavior

7. What is meant by statistical anomaly detection?

Collect the authorized user behavior over certain time.

Threshold detection
Counting the no of occurrences of a specific event
Profile based anomaly detection
Focusing on past behavior

8.What is meant by rule based detection?

Define the set of rules

anomaly detection
rules are developed from previous usage patterns
penetration identification
rules are developed by experts

9. What are the components of Distributed Intrusion Detection?
Host agent module
Collect the data on security related events
Host monitor agent module
Analyses LAN traffic
Central mgr module
Detect the intrusion

10. Define Firewall.
Firewall defines a single choke point that keeps unauthorized users out of the protected network.

11. List the design goals of firewalls?
1. All traffic from inside to outside, and vise versa, must pass through the firewall.
2. Only authorized traffic, as defined by the local security policy, will be allowed to pass.
3. The firewall itself is immune to penetration.

12. Give the different types of firewalls?
• Pack filtering router
• Application level gateway
• Circuit level gateway

13. What is the function of Pack filtering router?
Forward / discard the packet the packet based on IP address.

14. What is application level gateway?
An application level gateway also called a proxy server; act as a relay of application-level traffic. The user contacts the gateway using a TCP/IP application, such as Telnet or FTP, and the gateway asks the user for the name of the remote host to be accessed.

15. What is circuit level gateway?
• relays two TCP connections
• imposes security by limiting which such connections are allowed
• once created usually relays traffic without examining contents
• typically used when trust internal users by allowing general outbound connections

16. What are the configurations of firewall?
Screened host firewall single homed bastion
Use PFR and bastion host with single connection
Screened host firewall dual homed bastion
Use PFR and bastion host with dual connection

Screened subnet firewall
Use two PFR and bastion host

17. Define virus.
A virus is a program that can infect other program by modifying them the modification includes a copy of the virus program, which can then go on to infect other program.

18. Specify the types of viruses?
1) Parasitic virus
2) Memory-resident virus
3) Boot sector virus
4) Stealth virus
5) Polymorphic virus

19.What are the phases of viruses?
dormant – waiting on trigger event
propagation – replicating to programs/disks
triggering – by event to execute payload
execution – of payload

20. Specify some Antivirus Approaches
- Prevention
- Detection
  - Locate the virus
  - Identify the virus
  - Remove the virus

21. List the Generation of viruses?
- **first-generation**
  - scanner uses virus signature to identify virus
  - or change in length of programs
- **second-generation**
  - uses heuristic rules to spot viral infection
  - or uses program checksums to spot changes
- **third-generation**
  - memory-resident programs identify virus by actions
- **fourth-generation**
  - packages with a variety of antivirus techniques
  - eg scanning & activity traps, access-controls

22. Specify the Advanced antivirus approaches
- generic decryption
- digital immune system (IBM)
- Behavior blocking software