

Uka Tarsadia University (Diwaliba Polytechnic)
Diploma in Information Technology
Objective Type Questions (Web and Network Security-020070602)

Unit 1: Public key cryptosystem

- In public key cryptosystem _____ keys are used for encryption and decryption.
a) Same b) Different c) Encryption d) None of the above
- In public key cryptosystem which is kept as public?
a) Encryption keys b) Decryption keys
c) Encryption & Decryption keys d) None of the above
- In public key cryptosystem which is kept as private?
a) Encryption keys b) Decryption keys
c) Encryption & Decryption keys d) None of the above
- Input message in cryptography is called_____.
a) Plaintext b) Ciphertext c) Hash d) None of the above
- Encrypted message is known as_____.
a) Plaintext b) Ciphertext c) Plain and cipher (d) None of the above
- Asymmetric key is also called_____.
a) Secret key b) Public key c) Private key d) None of the above
- In a trapdoor function, the functions are easy to go in
a) One direction b) Two directions
c) All directions d) None of the above
- RSA stands for:

- a) Rivest Shamir and Adleman b) Rock Shane and Amozen
- c) Rivest Shane and Amozen d) Rock Shamir and Adleman

9. What are the inputs of encryption algorithm?

- a) Plaintext and ciphertext b) Ciphertext and key
- c) Plaintext and key d) Private and public key

10. What are the inputs of encryption algorithm?

- b) Plaintext and ciphertext b) Ciphertext and key
- c) Plaintext and key d) Private and public key

11. _____ is the valid pair of input to encryption algorithm.

- a) $E(\text{key}, \text{text})$ b) $E(\text{text}, \text{key})$ c) $D(\text{key}, \text{text})$ d) $D(\text{text}, \text{key})$

12. If A and B want to communicate with each other, B must not know_____.

- a) A's private key b) B's private key c) A's public key) d) B's public key

13. Which of the following is not ingredient of public key cryptosystem?

- a) Plaintext b) Hash function c) Ciphertext d) Key

14. To achieve confidentiality which pair of key is used?

- a) (P_{Ua}, P_{Rb}) b) (P_{Ra}, P_{Ub}) c) (P_{Ub}, P_{Rb}) d) (P_{Ra}, P_{Ua})

15. To achieve authentication which pair of key is used?

- a) (P_{Ua}, P_{Rb}) b) (P_{Ra}, P_{Ub}) c) (P_{Ub}, P_{Rb}) d) (P_{Ra}, P_{Ua})

16. User A encrypt message X using P_{Ub} then what will be the generated ciphertext Y?

- a) $Y = E(P_{Ub}, X)$ b) $Y = E(X, P_{Ub})$ c) $Y = X(P_{Ub}, E)$ d) $Y = P_{Ub}(E, X)$

17. User A decrypt message Y using P_{Ub} then what will be the generated plaintext X?

- a) $X = D(X, P_{Ub})$ b) $X = D(P_{Ub}, Y)$ c) $X = Y(P_{Ub}, E)$ d) $X = P_{Ub}(D, X)$

18. What will be the equation of plaintext X when ciphertext $Y=E(PR_a, X)$?

- a) $X=E(PR_a, Y)$ b) $Y=E(PU_a, Y)$ c) $X=D(PU_a, Y)$ d) $X=D(Y, PU_a)$

19. What will be the equation of plaintext X when ciphertext $Y=E(PU_b, X)$?

- a) $X=E(PU_a, Y)$ b) $X=D(PR_b, Y)$ c) $X=E(PR_b, Y)$ d) $X=D(Y, PR_b)$

20. In trap-door one way function calculation of $Y=f_k(x)$ is easy, if_____.

- a) K is known b) X is known c) K and X are known d) None of the above

21. In trap-door one way function calculation of $X=f_k^{-1}(Y)$ is infeasible, if_____

- b) K and Y are not known b) K is known but Y is not know

- c) K and Y are known d) Y is known but K is not known

22. Which of the followings are applications of public key crypto system?

- a) Encryption/Decryption b) Digital signature c) Key exchange d) All of above

23. What is the equation of euler's totient function?

- a) pq b) $(1-p)(1-q)$ c) $(p-1)(q-1)$ d) $p(p-q)$

24. If $n=35$ then what will be the value of euler's totient function?

- a) 7 b) 12 c) 35 d) 24

25. If $n=6$ then what will be the value of euler's totient function?

- a) 6 b) 2 c) 5 d) 8

26. _____ is gcd of 54 and 888.

- a) 5 b) 6 c) 4 d) 3

27. _____ is gcd of 55 and 22.

- a) 11 b) 12 c) 13 d) 14

28. _____ is gcd of 7120 and 150.

- a) 8 b) 9 c) 10 d) 11

29. _____ is gcd of 590 and 45.

- a) 2 b) 3 c) 4 d) 5

30. _____ is gcd of 270 and 192.

- a) 6 b) 7 c) 8 d) 9

31. In RSA algorithm, _____ is the equation of ciphertext C.

- a) $C = M^d \bmod n$ b) $C = M^e \bmod n$ c) $C = e^d \bmod n$ d) $C = M^d M^e \bmod n$

32. In RSA algorithm, _____ is the equation of plaintext M.

- b) $M = e^d \bmod n$ b) $M = d^e \bmod n$ c) $M = C^d \bmod n$ d) $M = C^{de} \bmod n$

33. In RSA algorithm, if $p=17$, $q=11$ then $n=$ _____.

- a) 17 b) 11 c) 160 d) 187

34. In RSA algorithm, if $p=17$, $q=31$ then $n=$ _____.

- a) 480 b) 840 c) 257 d) 527

35. In RSA algorithm, if $e=7$, $M=88$ and $n=187$ then ciphertext $C=$ _____.

- a) 10 b) 11 c) 12 d) 13

36. In RSA algorithm, if $C=3$, $d=5$ and $n=21$ then plaintext $M=$ _____.

- a) 10 b) 11 c) 12 d) 13

37. In RSA algorithm, if $M=12$, $e=5$ and $n=21$ then ciphertext $C=$ _____.

- a) 6 b) 5 c) 4 d) 3

38. If $n=21$ then what will be the value of euler's totient function?

- a) 21 b) 12 c) 13 d) 22

39. If $n=77$ then what will be the value of euler's totient function?

- a) 40 b) 50 c) 60 d) 77

40. In RSA algorithm, if $M=9$, $e=7$ and $n=143$ then ciphertext $C=$ _____.

- a) 45 b) 46 c) 47 d) 48

41. In RSA algorithm, if $M=10$, $e=5$ and $n=91$ then ciphertext $C= \underline{\hspace{2cm}}$.

- a) 80 b) 81 c) 82 d) 83

42. In RSA algorithm, if $C=20$, $d=3$ and $n=33$ then plaintext $M= \underline{\hspace{2cm}}$.

- a) 14 b) 15 c) 16 d) 17

43. In RSA algorithm, if $C=30$, $d=3$ and $n=33$ then plaintext $M= \underline{\hspace{2cm}}$.

- a) 4 b) 5 c) 6 d) 7

44. If $n=55$ then what will be the value of euler's totient function?

- a) 10 b) 20 c) 30 d) 40

45. In RSA algorithm, if $M=9$, $e=3$ and $n=55$ then ciphertext $C= \underline{\hspace{2cm}}$.

- a) 14 b) 15 c) 16 d) 17

46. In RSA algorithm, if $M=2$, $e=7$ and $n=527$ then ciphertext $C= \underline{\hspace{2cm}}$.

- a) 180 b) 182 c) 282 d) 128

47. In RSA algorithm, if $M=7$, $e=11$ and $n=143$ then ciphertext $C= \underline{\hspace{2cm}}$.

- a) 106 b) 100 c) 107 d) 108

48. Which of the followings are the attacks on RSA algorithm?

- a) Brute force b) Timing c) Mathematical d) All of the above

49. Counter measure of timing attack is .

- a) Random delay b) Blinding c) Constant exponential time d) All of the above

50. Trying of the possible combination of keys is known as .

- a) Brute force attack b) Timing attack c) Mathematical attack d) Hardware fault based attack

Unit 2: MAC and Hash function

1. When a hash function is used to provide message authentication, the hash function value is referred to as_____.

- a) Message field b) Message digest c) Message score d) Message Leap

2. Hash function provides _____ length output.

- a) Fixed b) Variable c) Both d) None of the above

3. Which of the following equation is used to calculate hash value?

- a) $H=h(M)$ b) $M=h(H)$ c) $h=H(M)$ d) $h=M(H)$

4. Another name for Message authentication codes is_____.

- a) cryptographic codebreak b) cryptographic codesum
c) cryptographic checksum d) cryptographic checkbreak

5. A hash function provides the integrity of a message that means message has not be_____.

- a) Copy b) Over view c) Changed d) Violates

6. MAC stands for

- a) Message authentication code b) Message arbitrary connection
c) Message authentication control d) Message authentication cipher

7. Message authentication is a service beyond

- a) Message confidentiality b) Message integrity
c) Message splashing d) Message sending

8. In message confidentiality, the transmitted message must make sense to only intended_____.

- a) Receiver b) Sender c) Modular d) Translator

9. In message authentication, the transmitted message must make sense to only intended_____.

- a) Receiver b) Sender c) Modular d) Translator

10. Encryption and decryption provide secrecy, or confidentiality, but not

- a) Authentication b) Integrity c) Privacy d) All of the above

11. When the data must arrive at the receiver exactly as they were sent, is called_____.

- a) Message confidentiality b) Message sending
c) Message splashing d) Message integrity

12. The message must be encrypted at the sender site and decrypted at the_____.

- a) Sender Site b) Site c) Receiver site d) Conferencing

13. If the sender encrypts the message with her private key, it achieves the purpose of _____.

- a) Confidentiality and digital signature
b) Confidentiality and authentication

c) Confidentiality but not authentication

d) Authentication and digital signature

14. If the sender encrypts the message with her public key, it achieves the purpose of _____.

a) Confidentiality

b) Confidentiality and authentication

c) Confidentiality and digital signature

d) Authentication and digital signature

15. If sender and receiver both are use same key then it is known as _____.

a) Public key b) Private key c) Symmetric key d) Asymmetric key

16. State the statement is true or false: A larger hash code cannot be decomposed into independent subcodes.

17. Which of the following is not possible through hash value?

a) Password check b) Data integrity check

c) Digital signatures d) Data retrieval in its original form

18. Which of the following options is not correct according to the definition of the Hash Function?

a) It mathematical functions

b) They compress the input values

c) Produce fixed length output

d) None of the above

19. Which of the following names can we use for denoting the output of the hash function?

a) Hash value b) Hash code c) Message digest d) All of the above

20. PRF stands for_____.

a) Public random function b) Pseudo random function

c) Pseudo random factor d) Private random function

21. PRNG stands for_____.

a) Pseudo random number generator

b) Pseudo random numeric generator

c) Public random number generator

d) Private random number generator

22. Pre-image resistant is also known as_____

a) Second pre-image resistant b) Weak collision resistant

c) One way property d) Two way property

23. Second pre-image resistant is also known as

a) Pre-image resistant b) Weak collision resistant

- c) One way property d) Two way property

24. Collision resistant is also known as

- a) Pre-image resistant b) Weak collision resistant
c) One way property d) Strong collision resistant

25. In collision resistant, it is computationally infeasible to find any pair x, y with $x \neq y$, such that _____

- a) $H(x)=H(y)$ b) $H(y)=H(x)$ c) $x(y)=y(x)$ d) $y(x)=x(y)$

26. Release of message content to any person not processing appropriate cryptography key is known as

- a) Traffic analysis b) Disclosure c) Masqueraded) Non repudiation

27. Discovery of the pattern of traffic between parties are known as

- a) Traffic analysis b) Disclosure c) Masqueraded) Non repudiation

27. Insertion of message into the network from fraudulent source is known as

- a) Traffic analysis b) Disclosure c) Masqueraded) Non repudiation

28. _____ means change the content of message.

- a) Traffic analysis b) Sequence modification c) Timing modification d) Content
modification

29. Delay or replayed message is known as _____

a) Traffic analysis b) Sequence modification c) Timing modification d) Content modification

30. In source repudiation, denial of transmission of message by _____.

a) Source b) Destination c) Moderator d) Translator

31. In destination repudiation, denial of transmission of message by _____.

a) Source b) Destination c) Moderator d) Translator

32. The ciphertext of the entire message serve as its authenticators known as

a) Message c) Message decryption c) Message authentication d) Message encryption

33. Which of the following function is used to calculate MAC?

a) $MAC = K(C, M)$ b) $MAC = M(K, C)$ c) $MAC = C(K, M)$ d) $MAC = MAC(C, M)$

34. _____ is the message digest algorithm.

a) DES b) IDEA c) MD5 d) RSA

35. MD5 has a message digest of

a) 160 bits b) 512 bits c) 128 bits d) 224 bits

36. What is the message digest size of SHA-1?

a) 160 bits b) 512 bits c) 128 bits d) 224 bits

37. What is the message digest size of SHA-256?

a) 160 bits b) 512 bits c) 128 bits d) 256 bits

38. What is the message digest size of SHA-512?

- a) 160 bits b) 512 bits c) 128 bits d) 224 bits

40. What is the block size of MD5?

- a) 512 bits b) 521 bits c) 1024 bits d) 1042 bits

41. In SHA-512, the message is divided into blocks of size ____ bits for the hash computation.

- a) 512 bits b) 521 bits c) 1024 bits d) 1042 bits

42. SHA stands for

- a) Secure hash album b) Secure high algorithm
c) Server hash algorithm d) Secure hash algorithm

43. The message in MD5 is padded so that it's length is

- a) 448 mod 512 b) 484 mod 512
c) 844 mod 512 d) 444 mod 512

44. What is the word size of MD5?

- a) 16 b) 32 c) 64 d) 48

45. What is the word size of SHA-1?

- a) 16 b) 32 c) 64 d) 48

45. What is the word size of SHA-512?

- a) 16 b) 32 c) 64 d) 48

46. MD5 stands for

- a) Mobile digest version 5 b) Message digest version 5
c) Message decryption version 5 d) Message digest violate 5

47. What is the message size of MD5?

- a) $<2^{46}$ b) $<2^{64}$ c) $<2^{128}$ d) $<2^{182}$

48. What is the message size of SHA-1?

- a) $<2^{46}$ b) $<2^{64}$ c) $<2^{128}$ d) $<2^{182}$

49. What is the message size of SHA-512?

- a) $<2^{46}$ b) $<2^{64}$ c) $<2^{128}$ d) $<2^{182}$

50. What is the message digest size of SHA-224?

- a) 160 bits b) 512 bits c) 128 bits d) 224 bits

Unit 3 Digital signature

1. A _____ is used to verify the authority of the digital message.
a) Digital signature b) Decryption algorithm c) Digital envelop d) None of the above
2. To verify digital signature, we need the _____.
a) Sender's private key b) Sender's public key
c) Receiver's private key d) Receiver's public key
3. To construct digital signature, we need the _____.
a) Sender's private key b) Sender's public key
c) Receiver's private key d) Receiver's public key
4. Digital signature cannot provide _____ for the message.
1. Integrity b) Confidentiality c) Nonrepudiation d) Authentication
5. Digital signature provides _____.
a) authentication b) nonrepudiation
c) both (a) and (b) d) neither (a) nor (b)
6. _____ can be used to preserve the integrity of a document or a message.
a) Message digest b) Message summary
c) Encrypted message d) None of the above
7. A digital signature needs _____ system.
a) symmetric-key b) asymmetric-key c) both (a) and (b) d) neither (a) nor (b)
8. Which of the following is the application of digital signature?
a) Electronic mail b) Data storage c) Smart card d) All of the above

9. A _____ signature is included in the document; a _____ signature is a separate entity.

- A) conventional; digital B) digital; digital
- C) digital, conventional d) None of the above

10. In digital signature relationship between signature and document is _____.

- a) Many-to-many b) Many-to-one c) One-to-many d) One-to-one

11. In conventional signature relationship between signature and document is _____.

- b) Many-to-many b) Many-to-one c) One-to-many d) One-to-one

ANs: c

12. DSS stands for

- a) Document signature standard b) Digital signature standard
- C) Digital standard signature d) Document standard signature

13. MIME stands for

- a) Multipurpose internet mail extensions
- b) Multipurpose internet message extensions
- c) Multipurpose internet mail encryption
- d) Multi internet mail extensions

14. Which of the following is an element of MIME?

- a) Header field b) Content-type c) Transfer encoding d) All of the above

15. _____ provide information about the body of message.

- a) Footer field b) Content-type c) Transfer encoding d) Header field

16. _____ define that enable the conversion of any content format.

- a) Footer field b) Content-type c) Transfer encoding d) Header field

17. _____ used to identify MIME entity uniquely in multiple content.
- a) Content-type b) Content-ID c) Content-description d) Content-transfer-encoding
18. Which of the following service provided by S/MIME?
- a) Authentication b) Confidentiality c) Compression d) All of the above
19. Which of the following algorithm used for compression?
- a) RSA b) DES c) ZIP d) MD5
20. Which of the following algorithm used for email compatibility?
- a) RSA b) DES c) ZIP d) Radix 64
21. _____ used to apply a digital signature to a message.
- a) SingedData b) EnvelopedData c) CompressedData d) SimpleData
22. _____ used to apply a compression to a message.
- a) SingedData b) EnvelopedData c) CompressedData d) SimpleData
23. _____ is consist of encryption key and encryption content.
- a) SingedData b) EnvelopedData c) CompressedData d) SimpleData
24. What is the PGP stand for?
- a) Permuted gap permission b) Permuted great privacy
- c) Pretty good permission d) Pretty good privacy
25. PGP makes use of which cryptographic algorithm?
- a) DES b) AES c) RSA d) Rabin
26. Data compression includes _____
- a) Removal of redundant character

b) Uniform distribution of characters

c) Both a and b

d) None of the mentioned

27. Which of the following is email security protocol?

a) WEP b) FTP c) PGP d) HTTPS

28. S/MIME is abbreviated as _____

a) Secure/Multimedia Internet Mailing Extensions

b) Secure/Multipurpose Internet Mailing Extensions

c) Secure/Multimedia Internet Mail Extensions

d) Secure/Multipurpose Internet Mail Extensions

29. Digital signature must be computationally infeasible to _____ digital signature.

a) Produce b) Recognize C) Verify d) forge

30. Digital signature must be relatively easy to _____ digital signature.

a) Produce b) Recognize C) Verify d) All of the above

31. In MIME _____ is used to encode data by mapping 6-bit blocks of input to 8-bit blocks of output.

a) binary b) base64 c) quoted-printable d) x-token

32. Which of the following is the MIME content-type?

a) Text b) Message c) Image d) All of the above

33. Which of the following is S/MIME message content-type?

a) SingedData b) EnvelopedData c) CompressedData d) All of the above

34. _____ algorithms used to achieve authentication in S/MIME.
- a) RSA b) IDEA c) SHA-256 d) Both a and c
35. Pretty good privacy program is used for
- a) Electronic mails b) File encryption
- c) Both a and b d) None of the mentioned
36. PGP system uses
- a) Private key system b) Public key system
- c) Private and public key system d) None of the mentioned
37. To achieve confidentiality in S/MIME _____ bit content encryption key is used.
- a) 125 b) 126 c) 127 d) 128
38. Which of the following is advantage of compression?
- a) Save space b) Save money c) Save time d) None of the above
39. Email compatibility provide_____.
- a) Space b) Storage c) Transparency d) Time
40. Which of the following is the use of PGP?
- a) Signing b) Encryption and decryption of content
- c) Email securities d) All of the above
41. In PGP message the date/time when the key pair was generated is called_____.
- a) Time b) Date c) TimeStamp d) DateTime
42. In PGP message the least significant 64-bit of public key is called_____.
- a) KeyID b) MessageID c) ContentID d) EmailID

43. In PGP message format MD stands for_____

- a) Mobile Data b) Message Digest c) Message Data d) Message Device

44. In which MIME transfer encoding the data is all represented by short lines of ASCII character?

- a) 7-bit b) 8-bit c) binary d) base64

45. In which MIME transfer encoding the line is short but there may be non-ASCII characters?

- a) 7-bit b) 8-bit c) binary d) base64

46. Which of the following is the not MIME content-type?

- a) Text b) SingedData c) Image d) Message

47. Which of the following is not S/MIME message content-type?

- a) SingedData b) EnvelopedData c) CompressedData d) Message

48. What are the properties of digital signature?

- a) It must be verify the author and date/time of signature.
b) It must be authenticate the content at the time of signature.
c) It must be available by third party to resolve disputes.
d) All of the above

49. Which of the following is the subtype of multipart in MIME content type?

- a) Parallel b) Image c) Message d) Video

50. Which of the following is the subtype of message in MIME content type?

- a) Rfc822 b) Partial c) Exeternal-body d) All of the above

Unit 4: IPSec

1. IPSec is designed to provide security at the _____.
 - a) transport layer
 - b) network layer
 - c) application layer
 - d) session layer
2. IPSec is protocols to provides security services during _____.
 - a) sending message
 - b) receiving message
 - c) communications between networks
 - d) none of above
3. What is the full form of IPSec?
 - a) IP security
 - b) IP server
 - c) IP secure
 - d) none of above
4. What is the full form of VPN?
 - a) Virtual Public Network
 - b) Virtual Private Number
 - c) Virtual Private Network
 - d) Virtual Path Number
5. What is the full form of ESP?
 - a) Encryption Security Payload

- b) Encryption Security Protocol
 - c) Encapsulation Security Protocol
 - d) Encapsulation Security Payload
6. IPSec configured on the networking devices like _____.
- a) routers
 - b) firewalls
 - c) gateways
 - d) all of above
7. Which protocols are used to secure the traffic or data flow in IPSec architecture?
- a) Encapsulation Security Payload
 - b) authentication header
 - c) A and B both
 - d) none of above
8. Which services are provided by IPSec?
- a) confidentiality
 - b) authentication
 - c) integrity
 - d) all of above
9. Which security service is not provided by IPSec?
- a) access control
 - b) non repudiation
 - c) confidentiality
 - d) connectionless integrity

10. What is the full form of IHL?

- a) Internet Header Length
- b) Integrity Header Length
- c) Internet Header Layer
- d) Integrity Header Layer

11. Which field gives the length of entire IP header?

- a) flags
- b) internet header length
- c) offset
- d) None of above

12. Which field gives the length of entire IP packet?

- a) flags
- b) internet header length
- c) offset
- d) total length

13. In IP header, “Total length” field stores which data?

- a) IP header length
- b) IP payload
- c) A and B both
- d) None of above

14. In IP header, “Version” field represents which data?

- a) the version of internet protocol
- b) the version of IP header

- c) the version of IPSec protocol
- d) none of above

15. What is the full form of TTL?

- a) Time to Live
- b) Time to leave
- c) Time to limit
- d) none of above

16. In which field address of sender is stored?

- a) destination address
- b) source address
- c) sender address
- d) header checksum

17. In which field address of receiver is stored?

- a) destination address
- b) source address
- c) receiver address
- d) header checksum

18. What size of sender's address is stored in source address field of IPv4?

- a) 16-bit
- b) 32-bit
- c) 16-byte
- d) 32-byte

19. What size of receiver's address is stored in destination address field of IPv4?

- a) 16-bit
- b) 32-bit
- c) 16-byte
- d) 32-byte

20. Which field is used if the value of IHL is greater than 5?

- a) option + password
- b) Option + total length
- c) Option + flags
- d) Option + padding

21. In IP header which field is optional?

- a) header checksum
- b) option + padding
- c) option + IHL
- d) IHL

22. What is the size of “version” field?

- a) 8 bits
- b) 16 bits
- c) 4 bits
- d) 2 bits

23. What is the size of “flow lable” field?

- a) 8 bits
- b) 16 bits
- c) 4 bits

- d) 20 bits
24. What is the size of “payload length” field?
- a) 8 bits
 - b) 16 bits
 - c) 4 bits
 - d) 20 bits
25. What is the size of “source address” field in IPv6?
- a) 8 bits
 - b) 16 bits
 - c) 42 bits
 - d) 128 bits
26. What is the size of “destination address” field?
- a) 16 bits
 - b) 4 bits
 - c) 128 bits
 - d) 48 bits
27. Traffic class is divided into _____ parts.
- a) Two
 - b) Three
 - c) Four
 - d) None of above
28. Which field of IPv6 is similar to TTL field of IPv4?
- a) flow label

- b) hop limit
 - c) payload length
 - d) traffic class
29. _____ used to maintain the sequential flow of the packets belonging to a communication.
- a) flow label
 - b) hop limit
 - c) payload length
 - d) traffic class
30. _____ is used to tell the routers how much information a particular packet contains in its payload.
- a) flow label
 - b) hop limit
 - c) payload length
 - d) traffic class
31. _____ is used to indicate the type of extension header.
- a) traffic class
 - b) hop limit
 - c) next header
 - d) none of above
32. What is the work of SPI?
- a) To identifies security association
 - b) To identify source

- c) To identify destination
- d) none of above

33. SPI stands for _____

- a) Standard Parameters Index
- b) Security Parameters Index
- c) Security Payload Index
- d) Standard Payload Index

34. Which is mode of IPSec?

- a) tunnel mode
- b) transport mode
- c) A and B both
- d) none of above

35. Which mode provides end-to-end security between two hosts?

- a) tunnel mode
- b) transport mode
- c) A and B both
- d) none of above

36. Which mode provides gateway-to-gateway security?

- a) tunnel mode
- b) transport mode
- c) A and B both
- d) none of above

37. Who provide security to the data that is transferred between web browser and server?

- a) IPsec
 - b) Secure Socket Layer (SSL)
 - c) A and B both
 - d) none of above
38. _____ useful to avoid expensive negotiations of security parameters for each connection.
- a) SSL connection
 - b) SSL session
 - c) A and B both
 - d) none of above
39. Which of the following is true for SSL session?
- a) single session has only one connections
 - b) single session has many connections
 - c) every connection has a different key
 - d) every connection has a same key
40. _____ an arbitrary byte sequence by the server to identify an active or resumable session state.
- a) sever identifier
 - b) session identifier
 - c) state identifier
 - d) none of above
41. What is peer certificate?
- a) it is an X509.v3 certificate of the peer

- b) it is an certificate of authentication
 - c) it is an X509 certificate of the peer
 - d) none of above
42. The secret key used in MAC operations on data sent by the server is known as _____.
- a) client write MAC secret
 - b) server write MAC secret
 - c) server write key
 - d) client write key
43. The conventional encryption key for data encrypted by the server and decrypted by the client is known as _____.
- a) client write MAC secret
 - b) server write MAC secret
 - c) server write key
 - d) client write key
44. Which services are provided to SSL connection by SSL Record?
- a) confidentiality, authentication
 - b) message integrity, confidentiality
 - c) message authentication, message integrity
 - d) none of above
45. Which protocol is used for establish the sessions?
- a) SSL record protocol
 - b) handshake protocol
 - c) change-cipher spec protocol

d) alert protocol

46. Who provides end-to-end communications security over networks?

a) Secure Socket Layer (SSL)

b) IPSec

c) Transport Layer Security (TLS)

d) both A and B

47. TLS is widely used for_____.

a) internet communications

b) online transactions

c) both A and B

d) none of above

48. TLS protocol_____ than SSL protocol.

a) faster

b) slower

c) less secure

d) complex

49. Which of the following is false for TLS session?

a) it can help to secure transmitted data using encryption

b) it provides Interoperability

c) it provides algorithm flexibility

d) none of above

50. Which protocol copies the pending state into current state?

a) SSL record protocol

- b) handshake protocol
- c) change-cipher protocol
- d) alert protocol

51. Which protocol is used to convey SSL-related alerts to the peer entity?

- a) SSL record protocol
- b) handshake protocol
- c) change-cipher protocol
- d) alert protocol

Unit 5: Web security

1. The process of securing confidential data stored online from unauthorized access and modification is known as _____.
 - a) authenticity
 - b) web security
 - c) data security
 - d) information security
2. Web security is also known as _____.
 - a) web reliability
 - b) information security
 - c) cyber Security
 - d) none of above
3. From following which tool is not used to provide web security?
 - a) Skipfish
 - b) Scrawlr
 - c) Wapiti
 - d) Router
4. Which threat violate integrity of web server?
 - a) eavesdropping on the net
 - b) modification of memory
 - c) filling up disk
 - d) none of above
5. Which threat violate confidentiality of web server?

- a) eavesdropping on the net
- b) modification of memory
- c) filling up disk
- d) none of above

6. Web proxies are used to provide _____.

- a) integrity
- b) authentication
- c) confidentiality
- d) none of above

7. What does the DoS attack involve?

- a) prevent user from getting work done
- b) misrepresentation of user
- c) modification of data
- d) none of above

8. _____ provides transparency to end users and applications.

- a) IPSec
- b) HTTP
- c) TCP
- d) FTP

9. Which protocol provides security at application layer?

- a) IPSec
- b) HTTP
- c) Secure Electronic Transaction

d) none of above

10. What is the full form of HTTPS?

a) Hypertext Transparent Protocol Secure

b) Hypertext Transport Protocol Secure

c) Hypertext Transfer Protocol Service

d) Hypertext Transfer Protocol Secure

11. Which protocol is used for secure communication over a computer network?

a) Secure Electronic Transaction

b) Transport layer protocol

c) Hypertext Transfer Protocol

d) all of above

12. HTTPs refers to the combination of _____ and _____.

a) HTTP + SSL

b) HTTP + SHA

c) HTTP + TCP

d) none of above

13. Which protocol is used to protect against man-in-the-middle attack?

a) HTTPS

b) FTP

c) TCP

d) none of above

14. Who initiates a connection?

a) client

- b) server
- c) browser
- d) URL

15. What message client sends to begin the TLS handshake?

- a) ServerHello
- b) HelloServer
- c) ClientHello
- d) HelloClient

16. At which level an HTTP client requests a connection to an HTTP server?

- a) HTTPS level
- b) HTTP level
- c) TCP level
- d) TLS level

17. At which level a session is established between a TLS client and a TLS server?

- a) TCP level
- b) HTTP level
- c) TLS level
- d) none of above

18. Who can perform HTTPS connection closure?

- a) client
- b) server
- c) A and B both
- d) none of above

19. URL of HTTPS is begin with _____.

- a) https//:
- b) http//:
- c) http://
- d) https://

20. On which layer HTTPS protocol is operated?

- a) application layer
- b) transport layer
- c) network layer
- d) data link layer

21. Which port number is used by HTTP for communication?

- a) 80
- b) 81
- c) 443
- d) 445

22. Which website uses HTTPS protocol?

- a) education sites
- b) internet forums
- c) banking website
- d) A and B both

23. Which system ensures security and integrity of electronic transactions done using credit cards?

- a) Secure Smart Card Transaction

- b) Ensure Smart Card Transaction
- c) Ensure Electronic Transaction
- d) Secure Electronic Transaction

24. _____ protocol was supported in development by major organizations like Visa and Mastercard.

- a) SET
- b) STE
- c) TLS
- d) TSL

25. Which service provides a secure communication channel in transaction?

- a) HTTP service
- b) SET service
- c) A and B both
- d) none of above

26. Who can use a payment card to purchase goods?

- a) merchant
- b) issuer
- c) certificate authority
- d) cardholder

27. Who provides the certificates to merchant, cardholder and payment gateway?

- a) merchant
- b) issuer
- c) certificate authority

d) cardholder

28. Which functionalities are provided by SET?

- a) provide authentication
- b) provide message confidentiality
- c) provide message integrity
- d) all of above

29. 3D Secure also known as _____

- a) a payer security
- b) a payer authentication
- c) a payer 3D secure
- d) a payer 3D authentication

30. Which protocol is used to prevent fraud in online credit and debit card transactions?

- a) D secure
- b) 3D secure
- c) transaction secure
- d) none of above

31. Which of the following are the domain of 3D secure protocol?

- a) issuer domain
- b) acquirer domain
- c) interoperability domain
- d) all of above

32. Which domain represents the bank that issued the card?

- a) issuer domain

- b) acquirer domain
- c) interoperability domain
- d) none of above

33. _____ acts as a way to transport messages between the Merchant Plug In and the Access Control Server.

- a) cardholder
- b) browser
- c) cardholder browser
- d) none of above

34. Which module provides a communication interface between the Visa/MasterCard servers and the merchant's servers?

- a) merchant
- b) merchant server plug in
- c) server plug in
- d) acquirer

35. Which component provides a proof for an attempted authentication, when authentication is not available?

- a) access control server
- b) visa directory server
- c) authentication control server
- d) none of above

36. _____ enables the communications between the software of the merchant and the issuer of the card.

- a) access control server
- b) visa directory server
- c) authentication control server
- d) none of above

37. Which are the advantages of 3D secure protocol?

- a) it reduces fraud
- b) it is easy to use
- c) it is easy to install
- d) all of above

38. Which of the following statement is false for 3D secure protocol?

- a) it provides less security
- b) it provides less privacy than SET
- c) it does restrict chargebacks to happen
- d) all of above

39. The merchant's system creates _____ request and sends it to the payment gateway.

- a) an XML payment
- b) a payment request
- c) a send request
- d) a gateway request

40. What is the full form of ACS?

- a) Authentication Control Server
- b) Access Control Server
- c) Access Control Security

d) Acquire Control Security

41. What is the full form of VDS?

- a) Visa Directory Server
- b) Virtual Directory Server
- c) Visa Directory Security
- d) Visa Dictionary Server

42. Which are the tasks of issuer?

- a) it issues the credit card
- b) it can determine the cardholder's eligibility to participate in the 3-D secure payment process
- c) it defines the card number ranges eligible to participate in the 3-D secure payment process
- d) all of above

43. Who checks the use of credit card is done by an authorized user?

- a) server
- b) merchant
- c) Secure Electronic Transaction
- d) X.509 v3 digital certificates

44. The customer who wants to shop an online product or a service is known as _____.

- a) cardholder
- b) merchant
- c) issuer
- d) acquirer

45. SET provides integrity using _____.

- a) RSA digital signatures with SHA-1
- b) HMAC with SHA-1
- c) A and B both
- d) none of above

46. Which institution work on be half of acquirer to process the merchant's payment messages?

- a) payment gateway
- b) merchant
- c) issuer
- d) acquirer

47. Who posts the payment authentication response?

- a) ACS
- b) merchant
- c) web browser
- d) payment gateway

48. Which of the following parameter is contained by XML payment authentication request in 3D secure protocol?

- a) PAREq
- b) AcsUrl
- c) both A and B
- d) none of above

49. What is the full form of PAP?

- a) Purchase Authentication Payment
- b) Purchase Acquirer Page
- c) Purchase Authentication Page
- d) Purchase Authentication Protocol

50. TLS implementations must initiate an exchange of _____before closing a connection.

- a) closure message
- b) closure alerts
- c) A and B both
- d) none of above

Unit 6: System security

1. Which activity is designed to compromise your data security?
 - a) intrusion
 - b) intruder
 - c) virus
 - d) none of above
2. A person who attempts to gain unauthorized access to a system is known as _____.
 - a) hacker
 - b) intruder
 - c) cracker
 - d) all of above
3. An individual who is not authorized to use computer system and gain access to system protection by way of legitimate user account is known as _____.
 - a) masquerader
 - b) misfeasor
 - c) clandestine user
 - d) none of above
4. The user is authorized for such access but misuses his or her privileges is known as _____.
 - a) masquerader
 - b) misfeasor
 - c) clandestine user
 - d) none of above

5. Clandestine user can be _____.
a) insider
b) outsider
c) A and B both
d) none of above
6. What is the full form of SAD?
a) Standard anomaly detection
b) Statistical anomaly detection
c) Statistical authorization detection
d) None of above
7. What is the full form of RBD?
a) Rapid based detection
b) Reliability based detection
c) Rule-based detection
d) None of above
8. Which detection technique involves the collection of data relating to the behavior of legitimate users over a period of time?
a) statistical anomaly detection
b) rule-based detection
c) A and B both
d) none of above
9. In which technique focuses on characterizing the past behavior of individual users then detecting significant deviations?

- a) threshold detection
- b) profile based
- c) A and B both
- d) none of above

10. What counts the number of logins by a single user during one hour?

- a) counter
- b) gauge
- c) interval timer
- d) none of above

11. A _____ is used to measure the current value of some entity.

- a) counter
- b) gauge
- c) A and B both
- d) none of above

12. Length of time between successive logins to an account is known as _____.

- a) interval
- b) timer
- c) interval timer
- d) none of above

13. Quantity of resources consumed during a specified period is known as _____.

- a) gauge
- b) counter
- c) interval timer

d) resource utilization

14. Which technique involves an attempt to define a set of rules that can be used to decide that a given behavior is that of an intruder?

a) statistical anomaly detection

b) profile based

c) rule-based detection

d) none of above

15. In which approach rules are generated by experts?

a) anomaly detection

b) penetration identification

c) A and B both

d) none of above

16. The_____ serves to authenticate the ID of the individual logging on to the system.

a) password

b) identification

c) A and B both

d) none of above

17. In UNIX Password Management Scheme, 8 character password is converted into _____.

a) 56-bit value and 12-bit “salt” value

b) 56-bit value and 8-bit “salt” value

c) 48-bit value and 12-bit “salt” value

d) none of above

18. On which algorithm based UNIX password management scheme is worked?

- a) DES
- b) AES
- c) SDES
- d) None of above

19. A user can log on the UNIX system by using _____.

- a) ID
- b) password
- c) A and B both
- d) none of above

20. What are the inputs to the encryption routine?

- a) salt and stored password
- b) id and stored password
- c) salt and user supplied password
- d) none of above

21. Which technique is used to protect a password file?

- a) one-way encryption
- b) access control
- c) A and B both
- d) all of above

22. What characters should you use in a password to make it strong?

- a) use of more than 6 characters
- b) use of upper case and lower case letters

- c) do not use dictionary words
 - d) all of above
23. _____ defines one of the best-designed automated password generators.
- a) FIPS PUB 181
 - b) FIPS
 - c) PUB 181
 - d) None of above
24. _____ produces a random stream of characters used to construct the syllables and words.
- a) A random password generator
 - b) A random stream generator
 - c) A random number generator
 - d) none of above
25. Which software is intentionally included or inserted in a system for a harmful purpose?
- a) anti virus software
 - b) malicious software
 - c) A and B both
 - d) none of above
26. _____ is a program or programming code that replicates itself into other executable code.
- a) Virus
 - b) Worm
 - c) Zombie

d) Trojan horse

27. In which phase virus is activated?

a) propagation phase

b) triggering phase

c) execution phase

d) none of above

28. In which phase virus places a copy of itself into other programs or into certain system areas on the disk?

a) dormant phase

b) propagation phase

c) triggering phase

d) execution phase

29. _____ infects files that the operating system or shell consider to be executable.

a) Boot sector infector

b) Macro virus

c) File infector

d) None of above

30. _____ infects files with macro code that is interpreted by an application.

a) Boot sector infector

b) Macro virus

c) File infector

d) None of above

31. _____ infects a master boot record or boot record and spreads when a system is booted from the disk containing the virus.

- a) Boot sector infector
- b) Macro virus
- c) File infector
- d) None of above

32. In which sequence virus removal process is performed?

- a) Detection => Identification => Removal
- b) Identification => Detection => Removal
- c) Detection => Removal=> Identification
- d) Identification => Removal => Detection

33. Which system is designed to prevent unauthorized access to or from a network?

- a) encryption
- b) firewall
- c) IDS
- d) none of above

34. Firewall can be implemented on

- a) hardware
- b) software
- c) combination of both hardware and software
- d) all of above

35. What is the full form of LAN?

- a) Local Area Network

- b) Line Area Network
- c) Lock Area Networking
- d) None of above

36. A firewall is a _____security system:

- a) network
- b) file
- c) program
- d) none of these

37. From following which is the design goal of firewall?

- a) all traffic from inside to outside must pass through the firewall
- b) only authorized traffic, as defined by the local security policy, will be allowed to pass
- c) the firewall itself is immune to penetration
- d) all of above

38. From following which is the limitation of firewall?

- a) it can not protect against attacks that bypass the firewall
- b) it do not protect against internal threats
- c) it can not protect against the transfer of virus-infected programs or files
- d) all of above

39. On which basis “packet filter firewall” filters the IP packets?

- a) source and destination IP addresses
- b) port number
- c) IP protocol field and interface

d) all of above

40. Which is the disadvantage of “packet filter firewall”?

a) difficult to setup the packet filter rules

b) does not support advanced user authentication scheme

c) vulnerable to attacks

d) all of above

41. Which application program runs on a firewall system between two networks?

a) packet filtering firewall

b) application proxy firewall

c) circuit-level proxy firewall

d) none of above

42. Using which application user can contact the gateway?

a) TCP/IP

b) Telnet

c) FTP

d) all of above

43. On which level Application proxy firewall controls the traffic?

a) Network layer

b) Application layer

c) Data link layer

d) Physical layer

44. A packet filter firewall filters at _____

a) physical layer

- b) data link layer
- c) network layer
- d) application layer

45. Which connection is setup by gateway?

- a) one between itself & TCP user on an inner host
- b) one between itself & TCP user on an outer host
- c) A and B both
- d) none of above

46. Which type of firewall hiding information about the private network?

- a) packet filtering firewall
- b) application proxy firewall
- c) circuit-level proxy firewall
- d) none of above

47. What is “salt” value?

- a) it is related to the time at which the password is assigned to the user
- b) it is computer generated password
- c) it is 56 bit value
- d) none of above

48. How operating system finds stored password?

- a) using ID
- b) using entered password
- c) A and B both
- d) none of above

49. Which is the type of intruder?

- a) masquerader
- b) misfeasor
- c) clandestine user
- d) all of above

50. Which technique enables the collection of information about intrusion techniques that can be used to strengthen the intrusion prevention facility?

- a) intrusion prevention
- b) intrusion detection
- c) A and B both
- d) none of above