SYED AMMAL ENGINEERING COLLEGE
(An ISO 9001: 2008 Certified Institution &
NBA Accredited : MECH, ECE, CSE & EEE)
Dr. E.M.Abdullah Campus, Ramanathapuram – 623 502
Department of Computer Science and Engineering

Objective Type Questions with Answers

Domain Name: Cryptography and Network Security

Prepared By: Sharmila.G, Asst.Prof / CSE

1. A sender S sends a message *m* to receiver R, which is digitally signed by S with its private key. In this scenario, one or more of the following security violations can take place.

(I) S can launch a birthday attack to replace *m* with a fraudulent message.

(II) A third party attacker can launch a birthday attack to replace *m* with a fraudulent message.

(III) R can launch a birthday attack to replace *m* with a fraudulent message.

Which of the following are possible security violations?

A. (I) and (II) only B. (I) only C. (II) only D. (II) and (III) only

Answer: (B) (I) only

2. In a RSA cryptosystem, a participant A uses two prime numbers p=13 and q=17 to generate her public and private keys. If the public key of A is 35, then the private key of A is _____.

Answer: 11.0

3. Anarkali digitally signs a message and sends it to Salim. Verification of the signature by Salim requires

A. Anarkali's Public Key B. Salim's Public Key

C. Salim's Private Key D. Anarkali's Private Key

Answer: A. Anarkali's Public Key

4. Suppose that everyone in a group of N people wants to communicate secretly with the N-1 others using symmetric key cryptographic system. The communication between any two persons should not be decode able by the others in the group. The number of keys required in the system as a whole to satisfy the confidentiality requirement is

A. 2N B. N(N-1) C. N(N-1)/2 D. $(N-1)^2$

Answer: N(N-1)/2

5. Which of the following are used to generate a message digest by the network security protocols?
(P) RSA (Q) SHA-1 (R) DES (S) MD5

A. P and R only B. Q and R only
C. Q and S only D. R and S only
Answer: C. Q and S only

6. Using public key cryptography, X adds a digital signature σ to message M, encrypts <M, σ>, and sends it to Y, where it is decrypted. Which one of the following sequences of keys is used for the operations?

(A) Encryption: X's private key followed by Y's private key; Decryption: Y's public key followed by X's public key

(B) Encryption: X's private key followed by Y's public key; Decryption: Y's public key followed by X's private key

(C) Encryption: X's public key followed by Y's private key; Decryption: Y's public key followed by X's private key

(D) Encryption: X's private key followed by Y's public key; Decryption: Y's private key followed by X's public key
Answer: (D) Encryption: X's private key followed by Y's public key; Decryption: Y's private key followed by X's public key

7. In the RSA public key cryptosystem, the private and public keys are (*e*,*n*) and (*d*,*n*) respectively, where $n=p*q$ and p and q are large primes. Besides, n is public and p and q are private. Let M be an integer such that $0<M<n$ and $\Phi(n) = (p-1)(q-1)$. Now consider the following equations.

I. $M' = M^e \bmod n$
$M = (M')^d \bmod n$
II. $ed \equiv 1 \bmod n$
III. $ed \equiv 1 \bmod \Phi(n)$
IV. $M' = M^e \bmod \Phi(n)$
$M = (M')^d \bmod \Phi(n)$

Which of the above equations correctly represent RSA cryptosystem?

A.(I) and (II) B. (I) and (III) C. (II) and (IV) D. (III) and (IV)

Answer: B. (I) and (III)

8. AES uses a _____ bit block size and a key size of _____ bits.

A. 128; 128 or 256 B. 64; 128 or 192

C. 256; 128, 192, or 256 D. 128; 128, 192, or 256

Answer: D. 128; 128, 192, or 256

9. Like DES, AES also uses Feistel Structure.

A. True B.False C. Maybe D. Can't say

Answer: B.False

10. Which one of the following is not a cryptographic algorithm?

A. Jupiter B. Blowfish C. Serpent D. Rijndael

Answer: A. Jupiter

11. Which algorithm among was chosen as the AES algorithm?

A. MARS B. Blowfish C.RC6 D. Rijndael

Answer: A. MARS

12. How many rounds does the AES-192 perform?

A. 10 B.12 C.14 D. 16

Answer: B.12

13. How many rounds does the AES-256 perform?

A. 10 B.12 C.14 D. 16

Answer: C.14

14. What is the expanded key size of AES-192?

A. 44 words B. 60 words

C. 52 words D. 36 words

Answer: C. 52 words

15. For the AES-128 algorithm there are _____ similar rounds and _____ round is different.

A. 2 pair of 5 similar rounds ; every alternate B. 9 ; the last

C. 8 ; the first and last D. 10 ; no

Answer: B. 9 ; the last

16. Which of the 4 operations are false for each round in the AES algorithm?

i) Substitute Bytes

ii) Shift Columns

iii) Mix Rows

iv) XOR Round Key

A. i) only B. ii) iii) and iv)

C. ii) and iii) D. only iv)

Answer: B. ii) iii) and iv)

17. On comparing AES with DES, which of the following functions from DES does not have an equivalent AES function?

A. f function B. permutation p

C. swapping of halves D. XOR of subkey with function f

Answer: C. swapping of halves

18. What is the block size in the Simplified AES algorithm?

A. 8 bits B. 40 bits

C. 16 bits D. 56 bits

Answer: 40 bits

19. What is the key size in the S-AES algorithm?

A. 16 bits B. 32 bits

C. 24 bits D. None of the above

Answer: A. 16 bits

20. Which of the following is a faulty S-AES step function?

A. Add round key B. Byte substitution

C. Shift rows D. Mix Columns

Answer: B. Byte substitution

21. How many step function do Round 1 and 2 each have in S-AES?

A. 4 and 3 B. Both 4 and 2

C. 1 and 4 D. 3 and 4

Answer: A. 4 and 3

22. Which one of the following modes of operation in DES is used for operating short data?

A. Cipher Feedback Mode (CFB) B. Cipher Block chaining (CBC)

C. Electronic code book (ECB) D. Output Feedback Modes (OFB)

Answer: C. Electronic code book (ECB)

23. Which of the following is false for ECB mode of operation?

i) The Plain text is broken into blocks of size 128 bytes

ii) Blocks can be swapped, repeated, replaced without recipient noticing

iii) Good for short data

iv) Encryption of each block is done separately using a randomly generated key for each block

A. i) only B. ii) and iii)

C. i) and iv) D. i) ii) and iv)

Answer: C. i) and iv)

24. Which of the following statements are true?

i) In the CBC mode, the plaintext block is XORed with previous ciphertext block before encryption

ii) The CTR mode does not require an Initialization Vector

iii) The last block in the CBC mode uses an Initialization Vector

iv) In CBC mode repetitions in plaintext do not show up in ciphertext

a. iii) b. ii) and iv)

c. All the Statements are true d. i) ii) and iv)

Answer: d. i) ii) and iv)

25. There is a dependency on the previous ‘s’ bits in every stage in CFB mode. Here ‘s’ can range from ___

a. 8-16 bits b. 8-32 bits c. 4-16 bits d. 8-48 bits

Answer: (b). 8-32 bits

26. Which of the following can be classified under advantages and disadvantages of OFB mode?

i) Transmission errors

ii) A bit error in a ciphertext segment

iii) Cannot recover from lost ciphertext segments

iv) Ciphertext or segment loss

a.Advantages: None; Disadvantages: All

b.Advantages: All; Disadvantages: None

c.Advantages: i); Disadvantages: ii) iii) iv)

d.Advantages: i); ii) Disadvantages: iii) iv)

Answer: a)

27. In OFB Transmission errors do not propagate: only the current ciphertext is affected, since keys are generated “locally”

a. True

b. False

c. May be

d. Can't say

Answer: (a). True

28. Which of the following modes does not implement chaining or “dependency on previous stage computations”?

a. CTR, ECB

b. CTR, CFB

c. CFB, OFB

d. ECB, OFB

Answer: (a). CTR, ECB

29. The counter value in CTR modes repeats are a regular interval.

a. True b. False c. May be d. Can't say

Answer: (b). False

30. Which mode of operation has the worst “error propagation” among the following?

a. OFB b. CFB c. CBC d. ECB

Answer: (d).ECB

31. Which block mode limits the maximum throughput of the algorithm to the reciprocal of the time for one execution?

a. OFB b. CTR c. CBC d. ECB

Answer: (b). CTR

32. Which mode requires the implementation of only the encryption algorithm?

a. ECB b. CBC c. CTR d. OFB

Answer: (c). CTR

33. Which of the following modes of operation does not involve feedback?

a. ECB b. CBC c. CTR d. OFB

Answer: (a). ECB

34. Which of the following is a natural candidates for stream ciphers?

a. OFB b. CFB c. CBC d. ECB

Answer: (a). OFB

35. A sender is employing public key cryptography to send a secret message to a receiver. Which one of the following statements is TRUE?

A. Sender encrypts using receiver's public key

B. Sender encrypts using his own public key

C. Receiver decrypts using sender's public key

D. Receiver decrypts using his own private key

Answer: A and D

36. The big-endian format is one in which

a) the least significant byte is stored in the low-address byte position

b) the least significant byte is stored in the high-address byte position

c) the most significant byte is stored in the high-address byte position

d) the most significant byte is stored in the low-address byte position

Answer: d

Explanation: The big-endian format is one in which the most significant byte is stored in the low-address byte position.

37. SHA-l has a message digest of

A.160 bits

B.512 bits

C.628 bits

D.820 bits

Answer: A. 160 bits

38. Message authentication is a service beyond

A. Message Confidentiality

B. Message Integrity

C. Message Splashing

D. Message Sending

Answer: B. Message Integrity

39. In Message Confidentiality, transmitted message must make sense to only intended

A. Receiver

B. Sender

C. Modulator

D. Translator

Answer: A. Receiver

40. A hash function guarantees integrity of a message. It guarantees that message has not be

A. Replaced

B. Over view

C. Changed

D. Violated

Answer: A. Replaced

41. To check integrity of a message, or document, receiver creates the

A. Hash-Table

B. Hash Tag

C. Hyper Text

D. Finger Print

Answer: B. Hash Tag

42. A digital signature needs a

A. Private-key system

B. Shared-key system

C. Public-key system

D. All of them

Answer: C. Public-key system

43. One way to preserve integrity of a document is through use of a

A. Eye-Rays

B. Finger Print

C. Biometric

D. X-Rays

Answer: B. Finger Print

44. A session symmetric key between two parties is used

A. Only once

B. Twice

C. Multiple times

D. Conditions dependant

Answer: A. Only once

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

A. Authentication

B. Integrity

C. Privacy

D. All of the above

Answer: B. Integrity

46. MAC stands for

A. Message authentication code

B. Message arbitrary connection

C. Message authentication control

D. Message authentication cipher

Answer: A. Message authentication code

47. Digest created by a hash function is normally called a

A. Modification detection code (MDC)

B. Modify authentication connection

C. Message authentication control

D. Message authentication cipher

Answer: A. Modification detection code (MDC)

48. Message confidentiality is using

A. Cipher Text

B. Cipher

C. Symmetric-Key

D. Asymmetric-Key

Answer: D. Asymmetric-Key

49. A sender must not be able to deny sending a message that was sent, is known as

A. Message Nonrepudiation

B. Message Integrity

C. Message Confidentiality

D. Message Sending

Answer: A. Message Nonrepudiation

50. To preserve integrity of a document, both document and fingerprint are

A. Not Used

B. Unimportant

C. Needed

D. Not Needed

Answer: C. Needed

51. When data must arrive at receiver exactly as they were sent, its called

A. Message Confidentiality

B. Message Integrity

C. Message Splashing

D. Message Sending

Answer: B. Message Integrity

52. In Message Integrity, message digest needs to be kept

A. Secret

B. Low

C. High

D. Constant 0

Answer: A. Secret

53. In Message Integrity, SHA-l hash algorithms create an N-bit message digest out of a message of

A. 512 Bit Blocks

B. 1001 Bit Blocks

C. 1510 Bit Blocks

D. 2020 Bit Blocks

Answer: A. 512 Bit Blocks

54. In brute force attack, on average half of all possible keys must be tried to achieve success.

a) True

b) False

Answer: a) True

Explanation: In brute force attack the attacker tries every possible key on a piece of cipher-text until an intelligible translation into plaintext is obtained.

55. If the sender and receiver use different keys, the system is referred to as conventional cipher system.

a) True

b) False

Answer: b) False

Explanation: Such a system is called asymmetric, two-key, or public-key cipher system.

56. An encryption scheme is unconditionally secure if the ciphertext generated does not contain enough information to determine uniquely the corresponding plaintext, no matter how much cipher text is available.

a) True

b) False

Answer: a

Explanation: The above statement is the definition for unconditionally secure cipher systems.

57. The estimated computations required to crack a password of 6 characters from the 26 letter alphabet is-

a) 308915776

b) 11881376

c) 456976

d) 8031810176

Answer: a) 308915776

Explanation: The required answer is 26^6 = 308915776.

58. Use Caesar's Cipher to decipher the following

HQFUBSWHG WHAW

a) ABANDONED LOCK

b) ENCRYPTED TEXT

c) ABANDONED TEXT

d) ENCRYPTED LOCK

Answer: b)

Explanation: Caesar Cipher uses C = (p+3) mod 26 to encrypt.

59. Caesar Cipher is an example of

a) Poly-alphabetic Cipher

b) Mono-alphabetic Cipher

c) Multi-alphabetic Cipher

d) Bi-alphabetic Cipher

Answer: b) Mono-alphabetic Cipher

Explanation: Caesar Cipher is an example of Mono-alphabetic cipher, as single alphabets are encrypted or decrypted at a time.

60. Monoalphabetic ciphers are stronger than Polyalphabetic ciphers because frequency analysis is tougher on the former.

a) True

b) False

Answer: b) False

Explanation: Monoalphabetic ciphers are easier to break because they reflect the frequency of the original alphabet.

61. Which are the most frequently found letters in the English language ?

a) e,a

b) e,o

c) e,t

d) e,i

Answer: c) e,t

Explanation: The relativity frequency of these letters in percent : e-12.702, a-8.167, t-9.056, i-6.996, o-7.507.

62. Choose from among the following cipher systems, from best to the worst, with respect to ease of decryption using frequency analysis.

a) Random Polyalphabetic, Plaintext, Playfair

b) Random Polyalphabetic, Playfair, Vignere

c) Random Polyalphabetic, Vignere, Playfair, Plaintext

d) Random Polyalphabetic, Plaintext, Beaufort, Playfair

Answer: c)

Explanation: Random Polyalphabetic is the most resistant to frequency analysis, followed by Vignere, Playfair and then Plaintext.

63. On Encrypting "thepepsiisintherefrigerator" using Vignere Cipher System using the keyword "HUMOR" we get cipher text-

a) abqdnwewuwjphfvrrtrfznsdokvl

b) abqdvmwuwjphfvvyyrfznydokvl

c) tbqyrvmwuwjphfvvyyrfznydokvl

d) baiuvmwuwjphfoeiyrfznydokvl

Answer: b)

Explanation: Cipher text:= Ci = Pi + ki mod m (mod 26).

64. On Encrypting "cryptography" using Vignere Cipher System using the keyword "LUCKY" we get cipher text

a) nlazeiibljji

b) nlazeiibljii

c) olaaeiibljki

d) mlaaeiibljki

Answer: a

Explanation: Cipher text:= Ci = Pi + ki mod m (mod 26).

65. The Index of Coincidence for English language is approximately

a) 0.068

b) 0.038

c) 0.065

d) 0.048

Answer: c

Explanation: The IC for the English language is approximately 0.065.

66) If all letters have the same chance of being chosen, the IC is approximately

a) 0.065

b) 0.035

c) 0.048

d) 0.038

Answer: d

Explanation: If all letters have the same chance of being chosen, the IC is approximately 0.038, about half of the IC for the English language.

67. Consider the cipher text message with relative frequencies:

4 0 10 25 5 32 24 15 6 11 5 5 1 2 6 6 15 19 0 0 6 28 8 2 3 2

The Index of Coincidence is

a) 0.065

b) 0.048

c) 0.067

d) 0.042

Answer: c

Explanation: Number of letters = 250. From this, IC=0.0676627. This is very strong evidence that the message came from a Monoalphabetic ciphering scheme.

68. Consider the cipher text message:

YJIHX RVHKK KSKHK IQQEV IFLRK QUZVA EVFYZ RVFBX UKGBP KYVVB QTAJK TGBQO ISGHU CWIKX QUXIH DUGIU LMWKG CHXJV WEKIH HEHGR EXXSF DMIIL UPSLW UPSLW AJKTR WTOWP IVXBW NPTGW EKBYU SBQWS

Relative Frequencies –

3 7 2 2 5 5 7 9 11 4 14 4 2 1 3 4 6 5 6 5 7 10 9 8 4 2

The Index of Coincidence is –

a) 0.065

b) 0.048

c) 0.067

d) 0.044

Answer: d

Explanation: Number of letters = 145.From this, IC=0.0438697 .This is very strong evidence that the message came from a polyalphabetic ciphering scheme.

69. A symmetric cipher system has an IC of 0.041. What is the length of the key ‘m’?

a) 1

b) 3

c) 2

d) 5

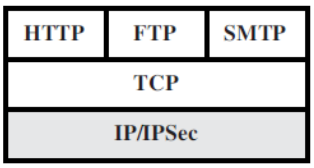
Answer: d

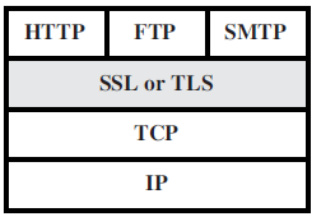
Explanation: Using the formula for calculating ‘m’ we get m=5, where

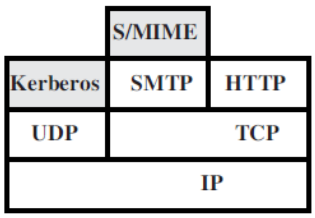
m≈0.027n/(I_c (n-1)-0.038n+0.065).

This set of Network Security Multiple Choice Questions & Answers (MCQs) focuses on “Secure Socket Layer”.

70. In the below figure from left to right, the correct order of the shaded levels are







a) Network level, Application level, Transport level

b) Application level, Network level, Transport level

c) Transport level, Application level, Network level

d) Network level, Transport level, Application level

Answer: d

Explanation: IP/IPSec is the Network level, SSL or TLS is the Transport Level, Kerberos and S/MIME are the Application level.

71. In the above figure, which of the above shaded block is transparent to end users and applications?

a) IP/IPSec

b) SSL

c) Kerberos

d) S/MIME

Answer: a

Explanation: IP/IPSec is the Network layer which is transparent to end users and applications.

72. In terms of Web Security Threats, "impersonation of another user" is a Passive Attack.

a) True

b) False

Answer: b

Explanation: Passive attacks include eavesdropping on network traffic between browser and server and gaining access to information on a website that is supposed to be restricted. Active attacks include impersonating another user, altering messages in transit between client and server, altering information on a website.

73. Which one of the following is not a higher –layer SSL protocol?

a) Alert Protocol

b) Handshake Protocol

c) Alarm Protocol

d) Change Cipher Spec Protocol

Answer: c

Explanation: Three higher –layer protocols are defined as part of SSL: The Handshake Protocol, The Change Cipher Spec Protocol and The Alert Protocol.

74. Which one of the following is not a session state parameter?

a) Master Secret

b) Cipher Spec

c) Peer Certificate

d) Server Write Key

Answer: d

Explanation: Session state is defined by the following parameters – Session identifier, Peer certificate, Compression method, Cipher spec, Master secret, Is resumable. Server Write Key falls under Connection State.

75. In the SSL Protocol, each upper layer message if fragmented into a maximum of _____ bytes.

a) 216

b) 232

c) 214

d) 212

Answer: c

Explanation: In the fragmentation process we obtain blocks of 2^14 bytes which is compressed in the next step.

76. The difference between HMAC algorithm and SSLv3 is that pad1 and pad2 are _____ in SSLv3 whereas _____ in HMAC.

a) NANDed, XORed

b) Concatenated, XORed

c) XORed, NANDed

d) XORed, Concatenated

Answer: b

Explanation: The pads are concatenated in SSLv3 and XORed in HMAC algorithm.

77. The full form of SSL is

a) Serial Session Layer

b) Secure Socket Layer

c) Session Secure Layer

d) Series Socket Layer

Answer: b

Explanation: SSL stands for Secure Sockets Layer.

78. After the encryption stage in SSL, the maximum length of each fragment is

a) 214+1028

b) 214+2048

c) 216+1028

d) 216+2048

Answer: b

Explanation: Encryption may not increase the content length by more than 1024 bytes, so the total length may not exceed 214+2048.

79. Consider the following example –

Size of Plaintext – 48 bytes.

Size of MAC – 20 bytes.

Block Length – 8 bytes.

How many bytes of padding need to be added to the system?

a) 1

b) 2

c) 3

d) 4

Answer: c

Explanation: 48 + 20 = 68 bytes. 72 is the next multiple of 8 (Block Length). 72 – 68 = 4. But we need to compensate 1 byte for length of the padding. Therefore, we require only 3 Bytes padding.

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

a) Alert Protocol

b) Handshake Protocol

c) Upper-Layer Protocol

d) Change Cipher Spec Protocol

Answer: a

Explanation: The Alert protocol is used to convey SSL related alerts to the peer entity.

81. Which protocol consists of only 1 bit?

a) Alert Protocol

b) Handshake Protocol

c) Upper-Layer Protocol

d) Change Cipher Spec Protocol

Answer: d

Explanation: The change cipher spec protocol is bit long.

82. Which protocol is used for the purpose of copying the pending state into the current state?

a) Alert Protocol

b) Handshake Protocol

c) Upper-Layer Protocol

d) Change Cipher Spec Protocol

Answer: d

Explanation: The Change Cipher Spec Protocol is used for this action.

83. Which of the following are possible sizes of MACs?

i) 12 Bytes

ii) 16 Bytes

iii) 20 Bytes

iv) 24 Bytes

a) i and iii

b) ii only

c) ii and iii

d) ii iii and iv

Answer: c

Explanation: MACs can be 0, 16 or 20 Bytes.

84. In the alert protocol the first byte takes the value 1 or 2 which corresponds to _____ and _____ respectively.

a) Select, Alarm

b) Alert, Alarm

c) Warning, Alarm

d) Warning, Fatal

Answer: d

Explanation: The first byte takes the value warning(1) or fatal(2) to convey the severity of the message.

This set of Network Security MCQs focuses on “Secure Socket Layer – II”.

85. Number of phases in the handshaking protocol?

a) 2

b) 3

c) 4

d) 5

Answer: c

Explanation: There are 4 phases in the handshaking protocol. These are –

Phase 1 : Establishing security capabilities

Phase 2 : Server Authentication and Key Exchange

Phase 3 : Client Authentication and Key Exchange

Phase 4 : Finish/ End.

86. In the SSL record protocol operation pad_2 is –

a) is the byte 0x36 repeated 40 times for MD5

b) is the byte 0x5C repeated 48 times for MD5

c) is the byte 0x5C repeated 48 times for SHA-1

d) is the byte 0x36 repeated 48 times for MD5

Answer: b

Explanation: pad_2 = is the byte 0x5C repeated 48 times for MD5.

87. In the SSL record protocol operation pad_1 is –

a) is the byte 0x36 repeated 40 times for MD5

b) is the byte 0x5C repeated 40 times for MD5

c) is the byte 0x5C repeated 48 times for SHA-1

d) is the byte 0x36 repeated 48 times for MD5

Answer: d

Explanation: pad_1 = is the byte 0x36 repeated 48 times for MD5.

88. In the Handshake protocol action, which is the last step of the Phase 2 : Server Authentication and Key Exchange?

a) server_done

b) server_key_exchange

c) certificate_request

d) certificate_verify

Answer: a

Explanation: The last step of the Phase 2 is the server_done step.

89. The certificate message is required for any agreed-on key exchange method except _____

a) Ephemeral Diffie-Hellman

b) Anonymous Diffie-Hellman

c) Fixed Diffie-Hellman

d) RSA

Answer: b

Explanation: The certificate message is required for any agreed-on key exchange method except Anonymous Diffie-Hellman.

90. In the Phase 2 of the Handshake Protocol Action, the step server_key_exchange is not needed for which of the following cipher systems?

a) Fortezza

b) Anonymous Diffie-Hellman

c) Fixed Diffie-Hellman

d) RSA

Answer: c

Explanation: The Fixed Diffie-Helmann does not require the server_key_exchange step in the handshake protocol.

91. The DSS signature uses which hash algorithm?

a) MD5

b) SHA-2

c) SHA-1

d) Does not use hash algorithm

Answer: c

Explanation: The DSS signature uses SHA-1.

92. The RSA signature uses which hash algorithm?

a) MD5

b) SHA-1

c) MD5 and SHA-1

d) None of the mentioned.

Answer: c

Explanation: The MD5 and SHA-1 hash is concatenated together and the then encrypted with the server's private key.

93. What is the size of the RSA signature hash after the MD5 and SHA-1 processing?

a) 42 bytes

b) 32 bytes

c) 36 bytes

d) 48 bytes

Answer: c

Explanation: The size is 36 bytes after MD5 and SHA-1 processing.

94. The certificate_request massage includes two parameters, one of which is-

a) certificate_extension

b) certificate_creation

c) certificate_exchange

d) certificate_type

Answer: d

Explanation: The certificate_request massage includes two parameters : certificate_type and certificate_authorities.

95. The client_key_exchange message uses a pre master key of size –

a) 48 bytes

b) 56 bytes

c) 64 bytes

d) 32 bytes

Answer: a

Explanation: The client_key_exchange message uses a pre master key of size 48 bytes.

96. The certificate_verify message involves the process defined by the pseudo-code (in terms of MD5) –

CertificateVerify.signature.md5_hash = MD5(master_secret || pad_2 || MD5(handshake_messages || master_secret || pad_1));

Is there any error? If so, what is it?

a) Yes. pad_1 and pad_2 should be interchanged

b) Yes. pad's should be present towards the end

c) Yes. master_key should not be used, the pre_master key should be used

d) No Error

Answer: d

Explanation: The code is correct with no errors.

97. In the handshake protocol which is the message type first sent between client and server ?

a) server_hello

b) client_hello

c) hello_request

d) certificate_request

Answer: b

Explanation: Interaction between the client and server starts via the client_hello message.

This set of Network Security Multiple Choice Questions & Answers focuses on "Transport Layer Security and HTTPS".

98. In the SSLv3 the padding bits are _____ with the secret key.

a) Padded

b) XORed

c) Concatenated

d) ANDed

Answer: c

Explanation: The padding bits are concatenated with the secret key.

99. Which of the following is not a valid input to the PRF in SSLv3?

a) secret value

b) identifying label

c) initialization vector

d) secret value

Answer: c

Explanation: The PRF does not require an initialization vector.

100. Which of the following alert codes is not supported by SSLv3?

a) record_overflow

b) no_certificate

c) internal_error

d) decode_error

Answer: b

Explanation: no_certificate is not supported by the SSLv3.

101. We encounter the record_overflow error when the payload length exceeds –

a) 214 + 1024

b) 216 + 1024

c) 214 + 2048

d) 216 + 2048

Answer: c

Explanation: The overflow error is encountered when the length exceeds 214 + 2048.

102. Which key exchange technique is not supported by SSLv3?

a) Anonymous Diffie-Hellman

b) Fixed Diffie-Hellman

c) RSA

d) Fortezza

Answer: d

Explanation: Fortezza is not supported in SSLv3.

103. Calculation of the certificate verify in TLS involves the use of a finished_label. The finished_label is the string-

a) client finished for the client

b) client finished for the client, server finished for the server

c) server finished for the server

d) client finished for the server, server finished for the client

Answer: b

Explanation: The finished_label is the string client finished for the client, server finished for the server.

104. In TLS padding cann be upto a maximum of –

a) 79 bytes

b) 127 bytes

c) 255 bytes

d) none of the mentioned

Answer: c

Explanation: Padding can be upto a maximum of 255 bytes.

105. URL stands for –

a) Universal Remote Locator

b) Universal Resource Language

c) Uniform Resource Locator

d) Uniform Resource Language

Answer: c

Explanation: URL stands for Uniform Resource Locator.

106. HTTPS stands for Hypertext Transfer Protocol over TLS.

a) True

b) False

Answer: a

Explanation: The statement is true. HTTPS is HTTP invoked over SSL/TLS.

107. An HTTP connection uses port _____ whereas HTTPS uses port _____ and invokes SSL.

a) 40; 80

b) 60; 620

c) 80; 443

d) 620; 80

Answer: c

Explanation: HTTP uses 80 ports, whereas HTTPS uses 443 ports.

108. For a 150-bit message and a 10-bit MAC, how many values are the MAC value dependent on?

a) 2140

b) 2150

c) 215

d) 210

Answer: a

Explanation: 2150/210 = 2140.

109. Confidentiality can only be provided if we perform message encryption before the MAC generation.

a) True

b) False

Answer: b

Explanation: Confidentiality can be provided even if we perform message encryption after the MAC generation.

110. MACs are also called

a) testword

b) checkword

c) testbits

d) none of the mentioned

Answer: d

Explanation: Another term for MACs are tags(or check sum).

111. For a 100 bit key and a 32 bit tag, how many possible keys can be produced in the 3rd round?

a) 24

b) 232

c) 216

d) 264

Answer: a

Explanation: First round: 100 – 32 = 68

Second round: 68 – 32 = 36.

Third round: 36 – 32 = 4.

Therefore 24 keys can be produced by the third round.

112. MAC is a

a) one-to-one mapping

b) many-to-one mapping

c) onto mapping

d) none of the mentioned

Answer: b

Explanation: MACs are many to one mapping, which makes it tougher for the intruder for cryptanalysis.

113. For an n-bit tag and a k-bit key, the level of effort required for brute force attack on a MAC algorithm is

a) 2k

b) 2n

c) min(2k,2n)

d) 2k/2n

Answer: c

Explanation: The level of effort required for brute force attack on a MAC algorithm is min(2k,2n).

This set of Cryptography Multiple Choice Questions & Answers (MCQs) focuses on "HMAC, DAA and CMAC".

114. Cryptographic hash functions execute faster in software than block ciphers.

a) Statement is correct

b) Statement is incorrect

c) Depends on the hash function

d) Depends on the processor

Answer: d

Explanation: The execution time varies from processor to processor for different cryptographic systems.

115. What is the value of ipad in the HMAC structure?

a) 00111110

b) 00110010

c) 10110110

d) 01110110

Answer: b

Explanation: ipad is 36 in hexadecimal.

116. What is the value of opad in the HMAC structure?

a) 00111110

b) 00110010

c) 10110110

d) 01011100

Answer: d

Explanation: opad is 5C in hexadecimal.

117. Data Authentication Algorithm (DAA) is based on

a) DES

b) AES

c) MD-5

d) SHA-1

Answer: a

Explanation: The DAA is an algorithm based on the DES cipher block chaining mode.

118. Which mode of operation is used in the DAA?

a) output feedback mode

b) electronic code block mode

c) cipher block chaining mode

d) cipher feedback mode

Answer: c

Explanation: The DAA is an algorithm based on the DES cipher block chaining mode.

119. What is the full-form of CMAC?

a) Code-based MAC

b) Cipher-based MAC

c) Construct-based MAC

d) Collective-based MAC

Answer: b

Explanation: CMAC stands for cipher-based message authentication code.

120. Which cryptographic algorithm is used in CMAC?

a) Triple DES and AES

b) DES

c) RC-4

d) AES

Answer: a

Explanation: The CMAC algorithm uses triple DES and AES.

121. In CMAC, which scenario is a different key K2 is used instead of K1?

a) If the tag is larger than the key length

b) If the tag is shorter than the key length

c) In the last step of the algorithm

d) If the plaintext/message is not an integer multiple of the cipher clock length

Answer: d

Explanation: If the plaintext/message is not an integer multiple of the cipher clock length, then K2 is used.

122. K2 is derived by left shifting L by 2 bits. What is L defined as?

a) E(K , 0b)

b) E(K , 10*b)

c) E(K , 1b)

d) E(K , 10*1b)

Answer: a

Explanation: L is defined as encrypting b-bits of 0s with the key K through the same algorithm.

This set of Cryptography Multiple Choice Questions & Answers (MCQs) focuses on "Public Keys and X.509 Certificates".

123. Public key encryption/decryption is not preferred because

a) it is slow

b) it is hardware/software intensive

c) it has a high computational load

d) all of the mentioned

Answer: d

Explanation: Due to high computational load (thus being slow) public key systems are not preferred for large cryptosystems and large networks.

124. Which one of the following is not a public key distribution means?

a) Public-Key Certificates

b) Hashing Certificates

c) Publicly available directories

d) Public-Key authority

Answer: b

Explanation: Hashing certificates is some I just made up. It doesn't exist noob.

125. What is the PGP stand for?

a) Permuted Gap Permission

b) Permuted Great Privacy

c) Pretty Good Permission

d) None of the mentioned

Answer: d

Explanation: PGP stands for Pretty Good Privacy.

126. PGP makes use of which cryptographic algorithm?

a) DES

b) AES

c) RSA

d) Rabin

Answer: c

Explanation: PGP recommends the use of RSA.

127. Which of the following public key distribution systems is most secure?

a) Public-Key Certificates

b) Public announcements

c) Publicly available directories

d) Public-Key authority

Answer: a

Explanation: Public certificates are the most secure key distribution/management systems right now.

128. Which systems use a timestamp?

i) Public-Key Certificates

ii) Public announcements

iii) Publicly available directories

iv) Public-Key authority

a) i) and ii)

b) iii) and iv)

c) i) and iv)

d) iv) only

Answer: c

Explanation: Public announcements and Public Certificates involve the use of timestamps.

129. Which of these systems use timestamps as an expiration date?

a) Public-Key Certificates

b) Public announcements

c) Publicly available directories

d) Public-Key authority

Answer: a

Explanation: Public key certificates use timestamps as expiration dates.

130. Which system uses a trusted third party interface?

a) Public-Key Certificates

b) Public announcements

c) Publicly available directories

d) Public-Key authority

Answer: a

Explanation: Public-Key certificates use a trusted third party interface.

131. Publicly Available directory is more secure than which other system?

a) Public-Key Certificates

b) Public announcements

c) Public-Key authority

d) None of the mentioned

Answer: b

Explanation: Publicly Available directory is more secure than Public announcements.

This set of Cryptography Multiple Choice Questions & Answers (MCQs) focuses on "Public Keys and X.509 Certificates – 2".

132. Extensions were added in which version?

a) 1

b) 2

c) 3

d) 4

Answer: c

Explanation: Extensions to the X.509 certificates were added in version 3.

133. The subject unique identifier of the X.509 certificates was added in which version?

a) 1

b) 2

c) 3

d) 4

Answer: b

Explanation: The subject unique identifier was added in the 2nd version.

134. Which of the following is not an element/field of the X.509 certificates?

a) Issuer Name

b) Serial Modifier

c) Issuer unique Identifier

d) Signature

Answer: b

Explanation: Serial Modifier is not an element/field of the X.509 certificates.

135. Suppose that A has obtained a certificate from certification authority X1 and B has obtained certificate authority from CA X2. A can use a chain of certificates to obtain B's public key. In notation of X.509, this chain is represented in the correct order as –

a) X2 X1 X1 B

b) X1 X1 X2 A

c) X1 X2 X2 B

d) X1 X2 X2 A

Answer: c

Explanation: The correct representation would be X1 X2 X2 B.

136. Certificates generated by X that are the certificates of other CAs are Reverse Certificates.

a) True

b) False

Answer: a

Explanation: The statement is true. Certificates of X generated by other CAs are forward certificates.

137. It is desirable to revoke a certificate before it expires because

a) the user is no longer certified by this CA

b) the CA’s certificate is assumed to be compromised

c) the user’s private key is assumed to be compromised

d) all of the mentioned

Answer: d

Explanation: All of the options are true with regard to revocation of a certificate.

138. CRL stands for

a) Cipher Reusable List

b) Certificate Revocation Language

c) Certificate Revocation List

d) Certificate Resolution Language

Answer: c

Explanation: CRL stands for Certificate Revocation List.

139. Which of the following is not a part of an Extension?

a) Extension Identifier

b) Extension value

c) Criticality Indicator

d) All of the mentioned constitute the Extension

Answer: d

Explanation: Extension Identifier, Extension value and the Criticality Indicator all constitue the Extension header.

140. The criticality indicator indicates whether an extension can be safely ignored.

a) True

b) False

Answer: a

Explanation: The statement is true.

141. “Conveys any desired X.500 directory attribute values for the subject of this certificate.”

Which Extension among the following does this refer to?

a) Subject alternative name

b) Issuer Alternative name

c) Subject directory attributes

d) None of the mentioned

Answer: c

Explanation: The Subject directory attributes has the function of conveying any desired X.500 directory attribute values for the subject of this certificate.”

This set of Cryptography Problems focuses on “Public Keys and X.509 Certificates”.

142. How many handshake rounds are required in the Public-Key Distribution Scenario?

a) 7

b) 5

c) 3

d) 4

Answer: a

Explanation: A total of seven messages are required in the Public-Key distribution scenario.

143. A total of seven messages are required in the Public-Key distribution scenario. However, the initial five messages need to be used only infrequently because both A and B can save the other’s public key for future – a technique known as ____

a) time stamping

b) polling

c) caching

d) squeezing

Answer: c

Explanation: This technique is known as caching.

144. X.509 certificate recommends which cryptographic algorithm?

a) RSA

b) DES

c) AES

d) Rabin

Answer: a

Explanation: RSA is the recommended cryptographic algorithm for X.509 certificates.

145. The issuer unique identifier of the X.509 certificates was added in which version?

a) 1

b) 2

c) 3

d) 4

Answer: b

Explanation: The issuer unique identifier was added in the 2nd version.

146. The period of validity consists of the date on which the certificate expires.

a) True

b) False

Answer: b

Explanation: The Period of validity consists of 2 dates: the first and last date on which the certificate is valid.

147. Certificate extensions fall into 3 categories. Which one of the following is not a Certificate extensions category?

a) Subject and Issuer attributes

b) Key and Policy information

c) Certification path constraints

d) All of the above are Certificate extensions categories

Answer: d

Explanation: Subject and Issuer attributes, Key and Policy information and Certification path constraints are the three categories of Certificate extensions.

148. CMP stands for

a) cipher message protocol

b) cipher management protocol

c) certificate message protocol

d) none of the mentioned

Answer: d

Explanation: CMP stands for certificate management protocol.

149. CMS stands for

a) cipher message syntax

b) certificate message session

c) cryptographic message syntax

d) none of the mentioned

Answer: c

Explanation: CMS stands for cryptographic message syntax.

This set of Cryptography Multiple Choice Questions & Answers (MCQs) focuses on "Elliptic Curve Arithmetic/Cryptography".

150. What is the general equation for elliptic curve systems?

a) y3+b_1 xy+b_2 y=x33+a_1 x2+a_2 x+a_3

b) y3+b_1 x+b_2 y=x2+a_1 x2+a_2 x+a_3

c) y2+b_1 xy+b_2 y=x3+a_1 x2+a_2

d) y2+b_1 xy+b_2 y=x3+a_1 x2+a_2 x+a_3

Answer: d

Explanation: The general equations for an elliptic curve system is y2+b_1 xy+b_2 y=x3+a_1 x2+a_2 x+a_3.

151. In Singular elliptic curve, the equation x^3+ax+b=0 does ____ roots.

a) does not have three distinct

b) has three distinct

c) has three unique

d) has three distinct unique

Answer: a

Explanation: In Singular elliptic curve, the equation x^3+ax+b=0 does not have three distinct roots.

152. How many real and imaginary roots does the equation y2=x3-1 have

a) 2 real, 1 imaginary

b) all real

c) all imaginary

d) 2 imaginary, 1 real

Answer: d

Explanation: On solving the equation we get 2 imaginary and 1 real root.

153. How many real and imaginary roots does the equation y2=x3-4x have

a) 2 real, 1 imaginary

b) all real

c) all imaginary

d) 2 imaginary, 1 real

Answer: b

Explanation: On solving the equation we get all real roots.

154. In the elliptic curve group defined by y2= x3- 17x + 16 over real numbers, what is P + Q if P = (0,-4) and Q = (1, 0)?

a) (15, -56)

b) (-23, -43)

c) (69, 26)

d) (12, -86)

Answer: a

Explanation: P=(x1, y1)= (0,-4)

Q=(x2, y2)= (1,0)

From the Addition formulae:

λ= (0-(-4)) / (1-0) = 4

x3= = 16 – 0 – 1 = 15 and

y3= 4(0 – 15) –(-4) = -56

Thus R=P + Q = (15, -56).

155. In the elliptic curve group defined by y2= x3- 17x + 16 over real numbers, what is 2P if P = (4, 3.464)?

a) (12.022, -39.362)

b) (32.022, 42.249)

c) (11.694, -43.723)

d) (43.022, 39.362)

Answer: a

Explanation: From the Doubling formulae:

λ = (3*(4)2+ (-17)) / 2*(3.464) = 31 / 6.928 = 4.475

x3= (4.475)2- 2(4) = 20.022 – 8 = 12.022 and

y3= -3.464 + 4.475(4 – 12.022) = – 3.464 – 35.898 = -39.362

Thus 2P = (12.022, -39.362).

156. “Elliptic curve cryptography follows the associative property.”

a) True

b) False

Answer: a

Explanation: ECC does follow associative property.

157. “In ECC, the inverse of point P =(x1, y1) is Q = (-x1, y1). “

a) True

b) False

Answer: b

Explanation: The inverse of point P =(x1, y1) is Q =(x1, -y1).

This set of Cryptography online quiz focuses on “Elliptic Curve Arithmetic/Cryptography”.

158. On adding the two points P (4,3) and Q (10, 6) in the elliptic curve E11(1,1) we get

a) (9,3)

b) (6,4)

c) (7,5)

d) (2,8)

Answer: b

Explanation: Apply ECC to obtain P+Q=(6,4).

159. If P = (1,4) in the elliptic curve E13(1, 1) , then 4P is

a) (4, 2)

b) (7, 0)

c) (5, 1)

d) (8, 1)

Answer: d

Explanation: Apply ECC via adding P+P=2P then, 4P=2P+2P.

160. Multiply the point P=(8, 1) by a constant 3, thus find 3P, in the elliptic curve E13(1, 1)

a) (10,7)

b) (12,6)

c) (11,1)

d) (9,8)

Answer: a

Explanation: P+P=2P then, 3P=2P+P

Thus we get Q=3P = (10, 7).

161. Bob selects E67(2, 3) as the elliptic curve over GF(p). He selects e1 = (2, 22) and d = 4.

Then he calculates e2 = d × e1 .What is the value of e2?

a) (23,49)

b) (16,55)

c) (12,19)

d) (13,45)

Answer: d

Explanation: e2 = d × e1 ; e2 =(13, 45).

162. Bob selects E67(2, 3) as the elliptic curve over GF(p). He selects e1 = (2, 22) and d = 4.

Then he calculates e2 = d × e1 and the publicly announces the tuple (E, e1, e2). Now, Alice wants to send the plaintext P = (24, 26) to Bob and she selects r = 2. What are C1 and C2?

a) C1=(35,1) ; C2 =(21,44)

b) C1=(44,21) ; C2 =(1,35)

c) C1=(44,21) ; C2 =(44,21)

d) C1=(21,44); C2 =(35,1)

Answer: a

Explanation: Alice finds the points C1= r × e1 ; C1= (35, 1),

C2=P + r × e2 ; C2= (21, 44).

163. P = C1 – (d x C2)

Is this above stated formula true with respect to ECC?

a) True

b) False

Answer: b

Explanation: P = C2 – (d x C1).

164. For the point P (11, 2) defined in the curve E13(1, 1). What is –P?

a) (12,4)

b) (10,7)

c) (11,11)

d) (11,12)

Answer: c

Explanation: The inverse of P(11,2) is (11,11) or (11,-2).

165. For the point P (7, 0) defined in the curve E13(1, 1). What is –P?

a) (7,1)

b) (8,12)

c) (8,1)

d) (7,0)

Answer: d

Explanation: The inverse of P(11,2) is (11,11) or (11,-2).

This set of Cryptography Multiple Choice Questions & Answers (MCQs) focuses on "Hash Functions and Its Applications".

166. 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

Answer: b

Explanation: A hash function providing message authentication is referred to as massage digest.

167. Message authentication code is also known as

a) key code

b) hash code

c) keyed hash function

d) message key hash function

Answer: c

Explanation: Message authentication code is also known as keyed hash function.

168. The main difference in MACs and digital signatures is that, in digital signatures the hash value of the message is encrypted with a user's public key.

a) True

b) False

Answer: b

Explanation: The main difference in MACs and digital signatures is that, in digital signatures the hash value of the message is encrypted with a user's private key.

169. What is a one-way password file?

a) A scheme in which the password is jumbled and stored

b) A scheme in which the password is XOR with a key and stored

c) A scheme in which the hash of the password is stored

d) A scheme in which the password is passed through a PRF, which is then stored

Answer: c

Explanation: A scheme in which the hash of the password is stored by an operating system rather than the password itself is the one-way password file system.

170. Which one of the following is not an application hash functions?

a) One-way password file

b) Key wrapping

c) Virus Detection

d) Intrusion detection

Answer: b

Explanation: Key wrapping is a separate algorithm and not an application of hash fuctions.

171. If the compression function is collision resistant, then so is the resultant iterated hash function.

a) True

b) False

Answer: a

Explanation: The statement is true. The problem of designing a secure hash function reduces to that of designing a collision resistant compression function.

172. A larger hash code cannot be decomposed into independent subcodes.

a) True

b) False

Answer: b

Explanation: Hash codes can be decomposed into independent subcodes and this was the logic behind the meet in the middle attack.

This set of Cryptography Multiple Choice Questions & Answers (MCQs) focuses on "Hash Functions Based on Cipher Block Chaining".

173. What is the effectiveness of an n-bit hash value?

a) 2n

b) 2-n

c) 22n

d) 2-2n

Answer: b

Explanation: When an n-bit hash value is used its effectiveness is 2^-n, that is, the probability that a data error will result in an unchanged hash value is 2-n.

174. What is the effectiveness of a 128 bit hash value?

a) 2-64

b) 264

c) 2-112

d) 2-128

Answer: c

Explanation: In most normal text files, the high order bit of each octet is always zero. So if a 128 bit hash value is used, instead of an effectiveness of 2-128, the hash function will have an effectiveness of 2-112.

175. We define collision as: A collision occurs if we have x=y and H(x) = H(y).

a) True

b) False

Answer: b

Explanation: A collision occurs if we have x not equal to y and H(x) = H(y).

176. Consider the following properties

Variable Input size

Fixed Output size

Efficiency

Pre image resistant

Second Pre image Resistant

Collision resistant

Pseudo randomness

A hash function that satisfies the first _____ properties in the above table is referred to as a weak hash function.

a) 5

b) 4

c) 3

d) 2

Answer: a

Explanation: If the sixth property is also satisfied it is referred to as a strong hash function.

177. The second pre-image resistant property is

a) It is computationally infeasible to find any pair (x, y) such that H(x) = H(y)

b) For any given block x, it is computationally infeasible to find y not equal to x, with H(y) = H(x)

c) For any given hash value h it is computationally infeasible to find y such that H(y) = h

d) None of the mentioned

Answer: b

Explanation: The second pre-image property is defined by: For any given block x, it is computationally infeasible to find y not equal to x, with H(y) = H(x).

178. A function that is second pre-image resistant is also collision resistant.

a) True

b) False

Answer: b

Explanation: The statement is false. A function that is collision resistant is also second image resistant.

179. For an m-bit value, the adversary would have to try _____ values to generates a given hash value h.

a) 2m

b) 2(m-1)

c) 2(m/2)

d) (2m) – 1

Answer: b

Explanation: The adversary would have to try 2(m-1) values to generates a given hash value h.

180. For an m bit hash value, if we pick data blocks at random we can expect to find two data blocks with the same hash value within ____ attempts.

a) 2m

b) 2(m-1)

c) 2(m/2)

d) (2m) – 1

Answer: c

Explanation: This is known as the birthday paradox. If we choose random variables from a uniform distribution in the range 0 through N-1, then the probability that a repeated element is encountered exceeds 0.5 after root (N) choices have been made.

181. Which attack requires the least effort/computations?

a) Pre-image

b) Second Pre-image

c) Collision

d) All required the same effort

Answer: c

Explanation: Due to the birthday paradox it requires 2(m/2) computations only.

This set of Cryptography Multiple Choice Questions & Answers (MCQs) focuses on "Secure Hash Algorithms (SHA) – 1".

182. SHA-1 produces a hash value of

a) 256 bits

b) 160 bits

c) 180 bits

d) 128 bits

Answer: b

Explanation: SHA-1 produces a hash value of 160 bits.

183. What is the number of round computation steps in the SHA-256 algorithm?

a) 80

b) 76

c) 64

d) 70

Answer: c

Explanation: The number of round computation steps in the SHA-256 algorithm is 64.

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

a) 1024

b) 512

c) 256

d) 1248

Answer: a

Explanation: The message is divided into blocks of size 1024 bits, and the output produced is a 512-bit message digest.

185. What is the maximum length of the message (in bits) that can be taken by SHA-512?

a) 2128

b) 2256

c) 264

d) 2192

Answer: a

Explanation: The maximum length of the message is 2128.

186. The message in SHA-512 is padded so that it's length is

a) 832 mod 1024

b) 768 mod 1024

c) 960 mod 1024

d) 896 mod 1024

Answer: d

Explanation: Padding is done so that the length is 896 mod 1024.

187. In SHA-512, the registers 'a' to 'h' are obtained by taking the first 64 bits of the fractional parts of the cube roots of the first 8 prime numbers.

a) True

b) False

Answer: b

Explanation: The registers 'a' to 'h' are obtained by taking the first 64 bits of the fractional parts of the square roots of the first 8 prime numbers.

188. What is the size of W (in bits) in the SHA-512 processing of a single 1024- bit block?

a) 64

b) 128

c) 512

d) 256

Answer: a

Explanation: The 1024 bit message blocks are compressed to form 64 bit values(W).

189. In the SHA-512 processing of a single 1024- bit block, the round constants are obtained

a) by taking the first 64 bits of the fractional parts of the cube roots of the first 80 prime numbers

b) by taking the first 64 bits of the fractional parts of the cube roots of the first 64 prime numbers

c) by taking the first 64 bits of the fractional parts of the square roots of the first 80 prime numbers

d) by taking the first 64 bits of the non-fractional parts of the first 80 prime numbers

Answer: a

Explanation: The round constants (K) is obtained by taking the first 64 bits of the fractional parts of the cube roots of the first 80 prime numbers.

190. The output of the N 1024-bit blocks from the Nth stage is

a) 512 bits

b) 1024 bits

c) N x 1024bits

d) N x 512 bits

Answer: a

Explanation: The message digest output is 512-bits.

191. Among the registers ‘a’ to ‘h’ how many involve permutation in each round?

a) 4

b) 5

c) 6

d) 3

Answer: c

Explanation: (b, c, d, f, g, and h) undergo permutations.