Network Security Objectives

ICT 7th Sem

by

Mukesh Singh
(ICT Batch 2073)

Sukuna Multiple Campus
Sundarharaincha - 12, Morang

Objectives

Set-1

1. Message ___ means that the sender and the receiver expect privacy.
a) Confidentiality b) Integrity
c) Authentication d) none of the above

2. Message ___ means that the data must arrive at the receiver exactly sent...
a) Confidentiality b) Integrity
c) Authentication d) none of the above

3. Message ___ means that the receiver is ensured that the message is coming from the intended sender, not an imposter.
a) Confidentiality b) Integrity
c) Authentication d) none of the above

4. ___ means that a sender must not be able to deny sending a message that he sent.
a) Confidentiality b) Integrity
c) Authentication d) Non-repudiation

5. ___ means to improve the identity of the entity that tries to acces the system's resources.
a) Message authentication b) Entity authentication
c) Message Confidentiality d) none of the above

6. A(n) ___ can be used to preserve the integrity of a document or a message.

प्रश्न नं. उत्तर

a) message digest b) message summary
c) encrypted message d) non of the above

7. A(n) ___ function creates a message digest out of a message.
a) encryption b) decryption
c) hash d) none of the above

8. A hash function must meet ___ criteria.
a) two b) three
c) four d) none of the above

9. A ___ message digest is used as an MDC.
a) keyless b) keyed
c) either (a) or (b)
d) neither (a) nor (b)

10. A ___ signature is included in the document; a ___ signature is a separate entity.
a) Conventional; digital
b) digital; digital
c) either (a) or (b)
d) neither (a) nor (b)

11. To authenticate the data origin, one needs a(n) ___.
a) MDC b) MAC
c) either (a) or (b) d) neither (a) nor (b)

12. Digital signature provides ___.
a) authentication b) non-repudiation
c) both (a) and (b) d) neither (a) nor (b)

13. Digital signature cannot provide ___ for the message.
a) integrity b) confidentiality
c) non-repudiation d) authentication

14. If ___ is needed, a cryptosystem must be applied over the scheme.
a) integrity b) confidentiality
c) non-repudiation d) authentication

15. A digital signature needs a(n) ___ system.
a) symmetric-key b) asymmetric-key
c) either (a) or (b) d) neither (a) nor (b)

16. A witness used in entity authentication is ___.
a) something known b) something possessed
c) something inherent d) all of the above

17. In ___, a claimant proves her identity to the verifier by using one of the three kinds of witnesses.
a) message authentication b) entity authentication
c) message confidentiality d) message integrity

18. Password-based authentication can be divided into two broad categories: ___ and ___.
a) fixed; variable b) time-stamped; fixed
c) fixed; one-time d) none of the above

19. In ___ authentication, the claimant proves that she knows a secret without actually sending it.
a) Password base

a) password-based b) Challenge-response
c) either (a) or (b) d) neither (a) nor (b)

20. Challenge-response authentication can be done using ____.
a) symmetric-key ciphers b) asymmetric-key ciphers
c) keyed-hash functions d) all of the above

21. A(n) ____ is a trust third party that assigns a symmetric key to two parties.
a) KDC b) CA
c) KDD d) None of the above

22. A(n) ____ creates a secret key only between a member and the center.
a) CA b) KDC
c) KDD d) nine of the above

23. The secret key between member needs to be created as a ____ key when two members contact KDC.
a) public b) session
c) complimentary d) non of the above

24. ____ is a popular session key creator protocol that requires an authentication server and a ticket-granting server.
a) KDC b) Kerberos
c) CA d) none of the above

25. A(n) ___ is a federal or stage organization that binds a public key to an entity and issues a certificate.
a) KDC b) Kerberos
c) CA d) none of the above

26. A(n) ___ is a hierarchical system that answers queries about key certification.
a) KDC b) PKI
c) CA d) none of the above

27. The ___ criterion states that it must be extremely difficult or impossible to create the message if the message digest is given.
a) one-wayness b) weak-collision-resistance
c) strong-collision resistance d) none of the above

28. The ___ criterion ensures that a message cannot easily be forged.
a) one-wayness b) weak-collision-resistance
c) strong-collision resistance d) none of the above

29. The ___ criterion ensures that we cannot find two messages that holds that hash to the same digest.
a) one-wayness b) weak-collision-resistance
c) strong-collision resistance d) none of the above

Set-2

1. Confidentiality with asymmetric-key cryptosystem has its own ___.
   a) entities b) data
   c) problems d) translator

2. Secure Hash Algorithm 1 (SHA-1) has a message digest of ___.
   a) 160 bits b) 512 bits c) 628 bits d) 820 bits

3. Message authentication is a service beyond ___.
   a) message confidentiality b) message integrity
   c) message splashing d) message sending

4. In message confidentiality, the transmitted message must make sense to only intended ___.
   a) receiver b) sender
   c) modulor d) translator

5. A hash function guarantees the integrity of a message. It guarantees that the message has not been ___.
   a) replaced b) over viewed
   c) changed d) violated

6. To check the integrity of a message or document, the receiver ~~must~~ creates the ___.
   a) hash_table b) hash tag
   c) hyper_text d) finger print

7. A digital signature needs a ___.
a) private-key system b) shared-key system
c) public-key system d) secret key

8. One way to preserve the integrity of a document is through the use of a ___.
a) eye-rays b) finger print
c) biometric d) X-Rays

9. A session symmetric key between two parties is used ___.
a) only once b) twice
c) multiple times d) conditions dependent

10. Encryption and decryption provide secrecy, or confidentiality, but not ___.
a) authentication b) integrity
c) privacy d) modularity

11. MAC stands for ___.
a) Message Authentication Code
b) Message Arbitrary Connection
c) Message Authentication Control
d) Message Authentication Cipher

12. The 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

13. Message Confidentiality is using —.
a) Cipher text b) cipher
c) Symmetric-key d) asymmetric-key

14. A sender must not be able to deny sending a message that was sent, is known as —
a) Message non-repudiation b) message integrity
c) message confidentiality d) message sending

15. To preserve the integrity of a document, both the document and the fingerprint are —.
a) not used b) unimportant
c) needed d) not needed

16. When the data must arrive at the receiver exactly as they were sent, is called —.
a) message confidentiality b) message integrity
c) message splashing d) message sending

17. The message digest needs to be —.
a) public b) private
c) kept secret d) integrity

18. In message integrity, the message digest needs to be kept —.
a) secret b) low
c) high d) Constant 0.

19. In Message Integrity, Secure Hash Algorithm 1 (SHA-1) creates a N-bit message-digest out of a message of —.

a) 512 bits blocks b) 1001 bit blocks
c) 1510 bit blocks d) 2020 bit blocks

20. The message confidentiality or private means that the sender and the receiver expect ___.
a) Integrity b) Confidentiality
c) authentication d) Non-repudiation

21. The message must be encrypted at the sender site and decrypted at the ___.
a) sender site b) site
c) receiver site d) conferencing

Set-3

1. Which of the following is passive attack?
   a) Masquerade b) Replay
   c) Modification d) Release of message content

2. What is the algorithm that converts plain text into cipher text?
   a) Encryption b) Decryption
   c) Key generation d) Verification

3. In which block cipher mode of operation previous cipher text is used as input for encrypting next block of input?
   a) ECB b) CFB
   c) CBC d) CTR

4. What will be the cipher text for the plain text 123 if the RSA public key pair is (17, 3233)?
   a) 312 b) 855 c) 231 d) 173

5. What is the block size of DES?
   a) 256-bit b) 64-bit
   c) 128-bit d) 32-bit

6. Which of the following is message digest algorithm?
   a) RSA b) DES
   c) AES d) SHA

7. What stands for WEP?

a) Wired Equivalent Privacy
b) Wireless Equivalent Protocol
c) Wireless Ensemble Protocol
d) Wireless Entity Protocol

8. Which protocol is used for Transport Layer Security?
a) 3DES b) S/MIME
c) PGP d) WAP

9. Which type of malicious software spreads using network?
a) Virus b) Worm
c) Trojan Horse d) Spyware

10. Why SNMP is used?
a) For detecting malware
b) For securing firewalls
c) For monitoring network
d) For transporting messages

11. What is the algorithms that convert cipher into plain text?
a) Encryption
b) Decryption
c) Key Generation
d) Certification

12. Any action that compromises the security of information owned by an organization is called ____.
Ans → Security attack

13. ____ is a weakness in the security system.
→ Vulnerability

14. When one entity pretends to be a different entity, we call it ____.
→ Masquerade

15. ____ means that asset can be modified only by authorized parties or only in authorized ways.
→ Integrity

16. Confidentiality can be achieved with ____.
→ Encryption

17. A control is an action, device, procedure, or the technique that remove or reduces ____.
→ Vulnerability

18. Cryptography is the art of ____.
→ secret writing

19. The encrypted text is also called ____.
→ Ciphertext

20. Ciphertext depends on the original plaintext message, the algorithm, and the ____.
→ Key-value

21. ____ is a rearrangement of the characters of the plaintext into columns.
→ Column transposition

प्रश्न न.

22. Because a transposition is a rearrangement of the symbols of a message, it is also known as ___.
→ Permutation

23. DES stands for ___.
→ Data Encryption Standard.

24. The size of the enciphered text should be no longer than the text of the original message. True / False.
→ True

25. Symmetric algorithm uses ___ key(s).
→ One

26. ___ enables such an analyst to infer data that should be kept confidential in the database.
→ Linear Programming

27. ___ is a person who attempts to break a cypher text message to obtain the original plaintext message.
→ Cryptanalyst

28. The public key algorithm uses ___.
→ Pair of keys (two keys)

29. The Columnar transposition and other transpositions are examples of ___.
→ Block Cyphers

30. The data encryption algorithm developed by IBM for NBS was based on ___.
→ Lucifer

31. DES encrypting the plaintext as blocks of ___ bits.
→ 64

32. The DES algorithm is fixed for a ___ bit key.
→ 56

33. Triple-DES procedure is $C = E(k_1, D(k_2, E(k_1, m)))$.
True/False
→ True

34. The ___ is likely to be the commercial grade symmetric algorithm of choice for years, if not decades.
→ AES

35. AES is a ___ algorithm.
→ Symmetric key encryption

36. Asymmetric or public-key encryption systems use two keys ___ and ___.
→ A public key, a private key

37. ___ can be used to distribute other keys.
→ Public key

38. Diffie-Hellman scheme is based on ___.
→ Discrete logarithm problem

39. Because the users share a common secret key, the Diffie Hellman scheme is an example of an asymmetric key exchange protocol. True/False.
→ True

40. ___ gives us a reliable means to prove the origin of data or code.
→ Digital Signature

41. ___ are ideally suited to digital signatures.
→ Public key encryption systems

42. A digital signature must meet two primary conditions ___ and ___.
→ Unforgeable, authentic

43. Flaws are first divided into ___ and ___ flaws.
→ Intentional, inadvertent

44. The inadvertent flaws fall into ___ categories.
→ Six

45. ___ runs under the user's authority.
→ Malicious code

46. Virus attaches itself to the program and propagates copies of it to other programs. True/ False
→ True

47. Controls, encouraged by managers and administrators, are called ___.
→ Administrative Controls

48. ___ is often used as a safe way for general users to access sensitive data.
→ Trusted Software

49. ___ is an undocumented entry point to a module.
→ Trapdoor

50. ___ is a feature in program by which someone can access the program other than by the obvious, direct call, perhaps with special privileges.
→ Backdoor

51. In ___ separation, processes conceal their data and computations in such a way that they are unintelligible to outside processes.
→ Cryptographic

52. Separation in an Operating System cannot occur in several ways. True/False
→ False

53. The most obvious problem of ___ is preventing one program from affecting the memory of other programs.
→ Multiprogramming

54. A key advantage of the group protection approach is its ease of implementation. True/False.
→ True

55. ___ are mutually agreed-upon code words, assumed to be known only to the user and the system.
→ Passwords

56. A key advantage of the group protection approach is its ___.
→ Ease of implementation

57. In ___, each piece of information is ranked at a particular sensitivity level, such as unclassified, restricted, confidential, secret or top secret.
→ Military security

58. The military security model is representative of a more general scheme, called a ___.
→ Lattice

59. Unlike regular operating systems, trusted systems incorporate technology to address both ___ and ___.
→ features, assurance

60. Memory protection is usually performed by hardware mechanisms, such as ___ or ___.
→ paging, segmentation

61. ___ is a characteristic that often grows over time, in accordance with evidence and experience.
→ Trust

62. A single computing system in a network is often called ___ and its processor (computer) is called ___.
→ A node, a host

63. The way a network is configured, in terms of nodes and connections, is called the network firewall. True/False.

→ False

64. To maintain or improve reliability and performance, routings between two endpoints are ___.
→ Dynamic

65. Impersonation is a more significant threat in a wide area network than in a local ~~area~~ one. True/False.
→ True

66. ___ can be used to implement a VPN.
→ Firewalls

67. ___ is another way to segment the network.
→ Separate access.

68. ___ is a process created to enable users to implement public-key cryptography.
→ PKI

69. You can protect the IP datagrams by using one of the IPsec protocol elements, the ___ or the ___.
→ Encapsulating Security Payload (ESP), Authentication Header (AH).

70. The modes of operation of IPsec are ___ and ___.
→ Tunnel mode and Transport mode

71. The Security association that applies to a given IPsec header is determined by the packets ___ and the ___ in the packet header.

→ Destination IP address, Security Parameter Index (SPI)

72. The management of SA's can be either manual or through an Internet standard called ___.
→ Key management protocol.

73. ESP seeks to provide ___ and ___ key encrypting data to be protected and placing the encrypted data in the data portion of the ESP.
→ Confidentiality and Integrity

74. IKE is considered a hybrid protocol because it combines (and supplements) the functions of three other protocols ___ and ___.
→ ISAKMP, OAKLEY and SKEME

75. ___ is a generic protocol that supports many different key exchange methods.
→ ISAKMP

76. The ___ has established a service for assessing the security of commercial websites.
→ National Computer Security Association (NCSA)

77. On the upper layer, a protocol for initial authentication and transfer of encryption keys is called ___.
→ SSL Handshake Protocol

78. The Combination of key exchange, hash and encryption algorithm for each SSL session is defined as ___.
→ Cipher Suite

प्रश्न ?. उत्तर

79. SSL uses the ___ for reporting errors and abnormal conditions.
→ Alert Protocol

80. A ___ is an association between a client and a server.
→ Session

81. In SET ___ is to link two messages that are intended for two different recipients.
→ Dual Signature

82. ___ is an open encryption and security specification designed to protect credit card transactions on the Internet.
→ Secure Electronic Transaction (SET)

83. Confidentiality and content forgery are often handled by ___.
→ Encryption

84. Symmetric Encryption can protect against forgery by a recipient. True/False.
→ False

85. Encrypted E-mail messages always carry a digital signature, so the ___ and ___ of the sender are assured.
→ Authenticity, non-repudiability

86. DES stands for ___.
→ Data Encryption Standard

87. ___ cannot protect against forgery by a recipient, since both sender and recipient share a common key.
→ Symmetric Encryption

88. The principal differences between S/MIME and PGP is ___.
→ Method of Key Exchange

89. PGP stands for ___.
→ Pretty Good Privacy

90. ___ Encrypted e-mail messages are carry a ___. So they authenticity and non-repudiability of the sender are assumed.
→ Digital Signature

91. ___ is a device that filters all traffic between a protected or "inside" network and a less trustworthy or "outside" network.
→ firewall

92. A packet filtering gateway control access to packets based on packet address (source or destination) or ___.
→ Specific transport protocol type

93. An application proxy gateway is also called ___.
→ Bastion host

94. ___ maintains state information from one packet to another in input stream.
→ Stateful Inspection firewall

95. The primary disadvantage of packet filtering routers is a combination of ___ and ___.
→ Simplicity, Complexity

96. ___ identifies and organizes the security activities for a computing system.
→ Security Plan

97. ___ is the difference in risk exposure divided by the cost of reducing the risk.
→ Risk leverage

98 A security policy should not be comprehensive. True/ false
→ False

99. Security Policy must be realistic. True / False
→ True

100. ___ and ___ address external security threats.
→ Redundancy, Physical Controls

101. Risk assessment is a technique of supporting ___.
→ Security Planning.

102. ___ is a process that drives the rest of the security administration.
→ Security Planning

Set-4
Cryptography related

1. An asymmetric-key (or public-key) cipher use _
a) 1 key b) 2 key c) 3 key d) 4 key

2. A straight permutation cipher or a straight P-box has the same number of input as _
a) Cipher b) frames
c) outputs d) Bits

3. We use Cryptography term to transforming message to make them _
c) Secure and immune to attacks

4. The man in the middle attack can endanger the security of the Diffie-Hellman method if two parties are not _.
a) Authenticated b) Joined
c) Submit d) Separate

5. The shift cipher is sometimes referred to as the _
a) Caeser cipher b) Shift Cipher
c) Cipher d) Cipher text

6. The substitutional ciphers are _.
a) monoalphabetic b) semi-alphabetic
c) poly-alphabetic d) bi-alphabetic

7. The heart of Data Encryption Standard (DES) is the _.

a) Cipher b) rounds
c) encryption d) DES Function

8. The cryptography algorithms (ciphers) are devided into
a) two groups b) four groups
c) one single group d) zero single group

9. The Advanced Encryption Standard (AES), has three different configurations with respect to the number of rounds and
a) data size b) round size
c) Key size d) encryption size

10. In Cryptography, the original message, before being transformed, is called—
a) simple text b) plaintext
c) empty text d) filled text

11. In Cryptography, the Input bits are rotated to right or left in
a) rotation cipher b) xor cipher
c) cipher d) cipher text

12. An encryption algorithm transforms the plaintext into—
a) ciphertext b) simple text
c) plain text d) empty text

13. The International Data Encryption Algorithm (IDEA) was developed by:
→ Xeuija Lai and James Massey

14. Data Encryption Standard (DES) was designed by
a) Intel b) IBM
c) HP d) Sony

15. In Asymmetric-key Cryptography, although Rivest, Shamir, and Adelman (RSA) can be used to encrypt and decrypt actual message, it is very slow if the message is
a) Short b) Long
c) Flat d) Thin

16. In Symmetric-key cryptography, the key used by the sender and the receiver is ___.
a) shared b) different
b) two keys are used d) same keys are used

17. In Rotation Cipher, keylen rotation, the number of rotation is
a) Jammed b) Idle
c) Rotating d) fixed

18. In symmetric-key cryptography both party used
a) Same keys b) multi keys
c) different keys d) two keys

19. In symmetric Cryptography, the key locks and unlocks the box is:
a) Same b) shared c) private d) public

20.

20. The keys used in cryptography are ___.
a) Secret key b) private key
c) public key d) different key

21. Data Encryption Standard (DES) is an example of:
a) Complex box cipher b) cryptography
c) Electronic cipher Book d) Electronic Code Book

22. The relationship between a character in the plaintext to a character is:
a) many-to-one relationship b) one-to-many relationship
c) many-to-many relationship d) one-to-one relationship

23. Cryptography, a word with Greek origins, means
a) Grupting data b) Secret writing
c) Open writing d) closed writing

24. A transposition cipher reorders (permutes) symbols in a
a) Block of packets b) Block of slots
c) Block of signals d) Block of symbols

25. The Cipher feedback (CFB) mode was created for those situations in which we need to send or receive R bits of:
a) frames b) pixels
c) data d) encryption

26. In cryptography, when text is treated at the bit level, each character is replaced by:
a) 4 bits b) 6 bits
c) 8 bits d) 10 bits

प्रश्न न.

27. The Advanced Encryption Standard (AES) was designed by ___.
a) National Institute of Standards and Technology
b) IBM c) HP d) Intel

28. ECB stands for ___
→ Electronic Code Book

29. The cipher which uses the exclusive-or operation as defined in computer science is called ___.
a) Caesar cipher b) xor cipher
c) Cipher d) Cipher text

30. The cryptography can provide
a) entity authentication b) non-repudiation of message
c) Confidentiality d) authentication

32. The shift ciphers sometimes referred to as the
a) caesar cipher b) julia cipher
c) plain cipher d) XOR cipher

32. RSA stands for
→ Rivest, Shamir and Adleman

33. The Data Encryption standard (DES) was designed by:
a) Microsoft b) Apple
c) IBM d) HP