BAHIR DAR UNIVERSITY

BAHIR DAR INSTITUTE OF TECHNOLOGY

FACULTY OF COMPUTING

INFORMATION SECURITY AND ASSURANCE MODEL EXAM FOR GRADUATING STUDENTS

Instruction: Select the best answer from the given alternatives

1. Which of the following is true statement about block cipher?
   A. It utilizes transposition methods
   B. Suitable for implementation in hardwares
   C. Take one byte of plaintext at a time.
   D. Easy to reverse the encrypted text.
2. Which of the following is not a non-malicious human threat?
   A. someone's accidentally spilling a soft drink on a laptop
   B. unintentionally deleting text
   C. inadvertently sending an email message to the wrong person
   D. posting a malicious code on a website which can be accessed by anybody.
3. Which of the following was the first internet worm to cause significant damage and "bring down the internet"?
   A. Code Red
   B. Morris
   C. Melissa
   D. I LOVE YOU
4. Assume you've been hired as a security engineer at company A, and you've recently installed a biometric authentication system. Unfortunately, the biometric system rejects a large number of legitimate, registered users. So, as a security engineer, how do you tune the system?
   A. Increase the number of false rejections.
   B. Reduce the number of false rejections.
   C. Increase the False Acceptance Rate
   D. Reduce the number of false acceptances.
5. A smart card is a good form of two-factor authentication because:
   A. It contains a certificate on a microchip that is resistant to cloning or cracking

B. It can double as a proximity card for building entrance key card systems

C. It does not rely on internal power like a token

D. A smart card is portable and can be loaned to others

6. An information system that processes sensitive information is configured to require a valid user_id and strong password from any user. This process of accepting and validating this information is known as:

A. Strong authentication

B. Two-factor authentication

C. Authentication

D. Single sign-on

7. The main objective of information security is preserving the CIA triad which are:

A. Consistency, inspection, authentication

B. Confidentiality, integrity, authentication

C. Certification, integrity, availability

D. Confidentiality, integrity, availability

8. Suppose you have 80 hosts on your network. If you want establish a connection for these hosts to communicate to each other, how many keys are required for each pair of hosts?

A. 6320

B. 3160

C. 3200

D. 3120

9. Revocation of certificate may be happened before the expired date of the certificate during public key distribution if one of the following conditions happens.

A. user's private key is compromised

B. user is no longer certified by the certificate authority (CA)

C. CA's certificate is compromised

D. All

10. Which one of the following is true statement?

A. Interruption is an attack on integrity

B. Interception is an attack on availability

C. Fabrication is an attack on authenticity

D. Modification is an attack on confidentiality

11. Which one of the following is differ from the other?

A. Denial of service

B. Masquerade

C. Modification of messages

D. Traffic analysis

12. Which of the following statement is false about unconditionally secure systems?
    A. Only one-time pad scheme qualifies
    B. No matter how much resource is available, the cipher cannot be broken
    C. The cost of breaking the cipher exceeds the value of the encrypted information
    D. The ciphertext provides insufficient information to uniquely determine the corresponding plaintext

13. If A and B want to communicate using asymmetric key cryptography. However, there has been no prior communication between them. So, how can they start the conversation? (Consider A as a sender and B as a receiver).
    A. B should send its private encryption key to A.
    B. A should send its private encryption key to B.
    C. B should send its public encryption key to A.
    D. A should send its public encryption key to B.

14. Defense-in-Depth is an approach to security in which a series of defensive mechanisms are layered in order to protect valuable data. Which one of the following technologies can be applied to achieve this?
    A. Boundary controllers (firewall and access control)
    B. Intrusion detection systems (IDs)
    C. Threat or attack intrusion response
    D. All can be applied

15. Which one of the following is true about monoalphabetic cipher?
    A. It is multiple substitutions cipher.
    B. Each alphabetic character of plain text is mapped onto a unique alphabetic character of a cipher text.
    C. The relationship between a character in the plain text and the characters in the cipher text is one-to-many.
    D. Monoalphabetic ciphers are much stronger than polyalphabetic ciphers

16. Which one of the following uses the same key for both encryption and decryption of your message?

A. Symmetric Cryptosystem	C. Cryptography
B. Asymmetric Cryptosystem	D. None

17. In public key cryptography, what is the purpose of private key?

    A. Establishing a common key
    B. Create a digital signature
    C. Encrypting data
    D. All of the above

18. What is the best way to protect against social engineering attacks?

    A. Employee awareness
    B. Strong encryption
    C. Strong authentication
    D. Risk Mitigation

19. Which of the following Security principles is violated if the computer system is not accessible for authorized users?

    A. Availability
    B. Confidentiality
    C. Access Control
    D. Authentication

20. During your lunch break, your phone begins to receive unsolicited messages. What might this be an example of?

    A. Packet sniffing
    B. Bluesnarfing
    C. Bluejacking
    D. Spoofing

21. Alice and Bob decided to use public key cryptography. If Alice encrypted the original message using her own private key before transmitting the message to Bob, which one of the following security services is guaranteed?

    A. Confidentiality
    B. Authentication
    C. Non-repudiation
    D. B and C

22. Which one of the following is true statement?

    A. Active attack is an attack in which the attacker observes interaction with the system.
    B. Passive attack is an attack in which the attacker directly interacts with the system.
    C. Unintentional attack is an attack where there is a deliberate goal of misuse
    D. Ignoring notifications to install new updates and security patches is an unintentional attack.

23. Which one of the following is statement is false about confusion?

    A. It is achieved by substitution.
    B. Redundancy is increased as a result of confusion.
    C. It protects the relationship between the ciphertext and key.
    D. As a result of confusion, the resultant is vague.

24. A network station transmits hundreds of SYN packets to a destination computer. What is the computer doing that sends the message?
    A. Sending the contents of a large file to the destination computer
    B. Attempting to establish a TCP connection with the destination computer
    C. Attacking the destination computer with a SYN flood
    D. Transmitting streaming audio or video to the destination computer
25. According to researchers, which of the following security threats has the highest percentage of attacks?
    A. Insider human attack
    B. Outsider human attack
    C. Threats caused by non-human agents.
    D. All
26. Which one of the following is different from others
    A. Trojan
    C. Virus
    B. Worms
    D. Logic Bomb
27. Which one of the following service attacks causes a system or app to crash or behave unexpectedly?
    A. SQL Injection
    C. Buffer overflow
    B. Typosquatting
    D. DDoS
28. Alice and Bob decided to use public key cryptography to exchange messages. If Alice wants to send an encrypted message to Bob, which one is appropriate to transmit the encrypted message?
    A. Alice encrypts the message using the Bob's public key, and Bob decrypts the message using his private key.
    B. Alice encrypts the message using the Bob's public key, and Bob decrypts the message using his public key.
    C. Alice encrypts the message using the Bob's private key, and Bob decrypts the message using his private key.
    D. Alice encrypts the message using the Bob's public key, and Bob decrypts the message using Alice's public key.

29. Which one is true statement about identification and authentication?

A. Identification is usually kept private whereas authentication should be open to the public.

B. Identification is the process of proving that a user is who he or she claims to be whereas authentication is the process of determining access levels or privileges to system resources

C. Identification is the assertion of a person's identity, while authentication is the process of proving that asserted identity.

D. None

30. Who are "gray-hat" hackers?

A. They can be anyone, and their motivation for attacking a system or network can be completely random.

B. They are hackers who can be a good guy/girl during the day as a cybersecurity professional and a bad guy/girl at night by using their skills maliciously.

C. Penetration testers are examples of gray hat hackers.

D. All

31. Which of the following is not a benefit of using self-signed SSL certificates?

A. Cost reduction

B. Very easy to create

C. Authentication of the server

D. More sophisticated to crack

32. Which of the following statement is not true about polyalphabetic cipher?

A. It employs a number of substitution alphabets.

B. It is not vulnerable to frequency analysis attacks.

C. It is a simple substitution cipher.

D. It is a form of one-time pad cipher

33. Which of the following statement is true about stream cipher?

A. Takes one block of plaintext at a time.

B. Utilizes substitution methods

C. Uses 64 or more bits

D. Suitable for implementation in softwares

34. Among the following which one is differ from the other?

A. Playfair cipher

B. Caesar cipher

C. Vernam cipher

D. Vigenère cipher

35. Suppose you are an employee in an organization and you have made a risk assessment to identify the vulnerability of the system that the organization uses. After you have completed your risk assessment, the organization decided to purchase insurance to cover potential losses based on your findings. This strategy can be considered as:

A. Risk avoidance

B. Risk mitigation

C. Risk transfer

D. Risk acceptance

36. Assume you are the founder of ABC, a software development and consulting company. Your company wishes to protect your internet web application from SQL and script injection attacks. So, which one is the best solution to implement?

A. SSL certificate

B. Firewall

C. Intrusion detection system

D. Application firewall

37. In your final year project, you create a login page for your system and authenticate the user by using a username and password. However, the password stored in your database table is the hash value of the password, not the encrypted password. What is the root cause of this?

A. When a user's password is hashed, support personnel can more easily reset it.

B. Hashing algorithms consume less CPU power than encryption algorithms.

C. Nobody, not even system administrators, can guess the password.

D. Hashed passwords take up less space than encrypted passwords.

38. Which one of the following is true about Data encryption standard (DES) algorithm?

A. It employs a 56-bit encryption key.

B. It has been replaced by the International Data Encryption Algorithm (IDEA)

C. It Uses a 64-bit encryption key

D. It can be used by Secure Sockets Layer (SSL) encryption

39. Which of the following is the best order to treat a risk?

A. Risk acceptance, Risk avoidance, Risk mitigation, Risk transfer

B. Risk avoidance, Risk mitigation, Risk transfer, Risk acceptance

C. Risk acceptance, Risk transfer, Risk mitigation, Risk avoidance

D. Risk mitigation, Risk transfer, Risk avoidance, Risk acceptance

40. What is the purpose of the Diffie-Hellman key exchange protocol?
    A. Allowing two parties who have never communicated before to create public encryption keys
    B. To encrypt a symmetric encryption key
    C. Allowing two parties who have never communicated before to create a secret encryption key
    D. To decrypt a symmetric encryption key
41. What is the purpose of digitally signing your document or message before sending it to the intended recipient?
    A. To ensure integrity of the sender
    B. To ensure Confidentiality of the message
    C. To ensure Authenticity of the sender
    D. To ensure Confidentiality of the sender
42. If P and Q want to communicate using symmetric key cryptography. However, there has been no prior communication between them. So, how can they start the conversation?
    A. The receiving party should send its public encryption key to the transmitting party.
    B. Each party (P and Q) must exchange their public encryption keys.
    C. Each party should send the encryption key to the other party through the communications channel.
    D. One party should send the encryption key to the other party over an out-of-band communications channel.
43. Bob and Alice communicate using public key cryptography on a regular basis. Bob is concerned that his personal encryption key has been compromised. What course of action should Alice take?
    A. Request a new public key from Bob.
    B. Request a new private key from Bob.
    C. Send a new public key to Bob.
    D. Send a new private key to Bob.
44. Which is the best approach for two parties who wish to establish a means for confirming the confidentiality and integrity of messages that they exchange:

A. Digital signatures

B. Encryption and digital signatures

C. Key exchange

D. Encryption

45. Which one of the following shows the failure of data confidentiality?

A. A data item is accessed by an authorized individual.

B. An authorized person learns the existence of a piece of data

C. A person who is authorized to access certain data gains access to other data that is not authorized.

D. A data item is accessed by an authorized process or program.

46. Which one of the following is true about the cryptographic system?

A. Transformation is changing the plaintext one piece at a time.

B. A cryptographic system can be done based on the number of keys used for encryptions and decryption.

C. The Substitution method encrypts plaintext by moving small pieces of the message around.

D. All

47. Which of the following statements is incorrect about the Feistel cipher

A. The inputs to the encryption algorithm are a plaintext block of length 2W bits and a key K.

B. The ciphertext block is formed by combining the two halves of the data after n rounds of processing that include a substitution on the right data half followed by permutation.

C. The structure of all encryption rounds is the same.

D. The structure of DES is identical to that of a Feistel cipher.

48. Which of the following hash algorithms takes the most time to compute?

A. Secure hash algorithm

B. MD5

C. HMAC

D. RIPEMD-160

49. As a penetration tester, which of the following ethics must be followed?

A. Avoid being malicious.

B. Do not attack targets unless you have written permission.

C. Think about the consequences of your actions.

D. Don't be a moron.

50. Which one of the following encryption algorithms can easily be decrypted by brute force?

A. One-time pad

B. Feistel cipher

C. Vigenère

D. Playfair cipher

51. An attack on standard file protection can be carried out by booting a computer with a new operating system via USB. Which of the following statements provides a defense against this type of attack?

   A. by disconnecting every computer from every network.

   B. Configuring the bios to prompt for a password when the operating system boots.

   C. By providing passwords for the hardware components on our computer.

52. Which of the following approaches is best for balancing information security and access level?

   A. The level of security must permit reasonable access while also protecting against threats.

   B. Allowing complete access to the assets.

   C. Denying access to the assets completely.

   D. Consider one at a time, because balancing security and access is difficult.

53. Which one of the following statements is incorrect about Rootkit?

   A. It is a malicious code that installs itself at the kernel level.

   B. It loads before the OS loads.

   C. It can disable antivirus and antimalware

   D. It is very easy to detect.

54. Which of the following is the mechanism used by highly skilled hackers to breach government and commercial systems?

   A. Cyber espionage

   B. Sabotage

   C. Cyber warfare

   D. All

55. Which of the following statements about interception attacks is correct?

   A. It is insertion of spurious messages in a network

   B. It is modifying the content of messages being transmitted in a network

   C. It is illegal copying of files or programs

   D. It is disabling the file management system

56. Which type of social engineering attack is the best strategy if you want to perform an attack on BiT, specifically the institution's higher management team?

   A. Phishing

   B. Spear Phishing

   C. Whaling

   D. Vishing

57. Which of the following is true about authentication and authorization?
    A. authentication is the process of verifying who a user is, while authorization is the process of verifying what they have access to.
    B. Authentication verifies the identity of a user or service, and authorization determines their access rights.
    C. Authentication is visible and changeable by the user while authorization not visible or changeable by the user.
    D. all
58. which of the following can be used to distribute public key?
    A. Publicly available directory
    B. Public-key authority
    C. Public-key certificates
    D. All can be used
59. Which of the following is true about public key infrastructure (PKI)?
    A. It contains certification authorities (CA) to proof the identity users.
    B. It contains registration authority (RA) to issue certificates and CRL's
    C. It is a technology for authenticating users and devices in the digital world.
    D. It has no repositories to hold certificates and CRL's
60. When we say that we haven't kept an item's integrity, we may mean that the item is:
    A. Modified only in acceptable way
    B. Precise and accurate
    C. Internally consistent
    D. Modified only by unauthorized processes
61. Which one of the following statements is false?
    A. An advanced persistent threat (APT) attack is carefully planned and designed to infiltrate a specific organization.
    B. Secure Sockets Layer (SSL) is a protocol that provides secure communication over the Internet.
    C. When the exchange of data is encrypted with SSL/TLS, then we call it HTTP.
    D. Transport Layer Security **(**TLS) is the new protocol for secured encryption on the web

62. Which of the following is an authentication function that is used for message authentication?
    A. Encryption of messages
    B. Message authentication code
    C. Hash function
    D. None
63. _______ is the practice of safeguarding valuable information against unauthorized access, recording, disclosure, or destruction.
    A. Network security
    B. Information security
    C. Software security
    D. Internet security
64. Which of the following is an information security vulnerability?
    A. Unable to change default password
    B. Eavesdropping
    C. Earthquake
    D. Information leakage
65. Which of the following is a threat to an information security?
    A. Storage media disposal without erasing data
    B. Unable to change default password
    C. latest patches and updates have not been applied
    D. Lightning and Wind
66. Which of the following types of information security technology is used to protect against browser-based hacking?
    A. Make private mode in a browser
    B. Try to establish remote browser access
    C. Use adware remover in browsers
    D. Use anti-malwares in browsers
67. Which of the following can be an example of fabrication attack?
    A. Spoofing attacks in a network
    B. Hacking to deface a website
    C. packet sniffing
    D. A denial-of-service attack on a website
68. Operational security is one of the methods which helps us to assure our information. Which of the following activity can be done in the operational security?

A. Analyze vulnerabilities
B. Assess risks
C. Apply appropriate countermeasures
D. All of the above

69. Which of the following is false about information security?
A. It is a measure taken to protect and defend information and information systems.
B. It is the protection of information and information systems from unauthorized access.
C. It is the detection and remediation of security breaches.
D. It is the protection of information no matter where that information is.

70. Which of the following attack takes place when one entity pretends to be a different entity?
A. Denial of service
B. Masquerade
C. Modification of messages
D. Traffic analysis

71. Among the possible approaches to attack RSA algorithm, which type of attack exploits the properties of the algorithm?
A. Brute force attacks
B. Mathematical attacks
C. Chosen cipher text attacks
D. Timing attacks

72. Which of the following can’t be the objective information security?
A. Prevent unauthorized access
B. Ensure security flaws are immediately reported.
C. Maintain integrity of data assets.
D. None

73. Which of the following attributes didn’t Shannon suggest as a way to recognize a good cipher??
A. The set of keys and the enciphering algorithm should be free from complexity.
B. The implementation of the process should be as simple as possible.
C. Errors in ciphering should propagate and cause corruption of further information in the message.
D. The size of the enciphered text should be no larger than the text of the original message

74. Which of the following statement is incorrect about one-way hash functions?
A. They are used in integrity checking
B. They are used in authentication

C. They are used in communications protocols.

D. They are the workhorses of traditional cryptography

75. Which of the following criteria must a digital signature meet?

A. It should be unforgeable

B. It should be authentic

C. It should not reusable

D. All except C

76. Which of the following is incorrect about quantum cryptography?

A. It utilizes the principles of quantum mechanics to encrypt messages

B. It requires intricate mathematical computation, just as regular encryption.

C. It uses physics to detect an eavesdropper.

D. It is a method of encryption that performs cryptographic operations using quantum mechanical principles.

77. Which of the following is false statement?

A. Modification happens when an unauthorized party tampers with an asset.

B. Fabrication happens when an asset has been counterfeiting.

C. Interception happens an authorized party gains access to an information asset.

D. Interruption happens an asset becomes unusable, unavailable, or lost.

78. Let P and Q are two prime numbers with values 13 and 11 respectively. If the value of encryption key e=13, what will be the value of the decryption key d using RSA algorithm?

A. 27

B. 37

C. 18

D. 9

79. Based on question number 78, what will be the public key?

A. {37,143}

B. {13,120}

C. {13,143}

D. {9,120}

80. Based on question number 78, what will be the private key?

A. {27,120}

B. {13,143}

C. {18,120}

D. {37,143}

81. During which stage of penetration testing do we discover any existing vulnerabilities on a target system?

A. Vulnerability Analysis

B. Threat Modeling

C. Post Exploitation

D. Intelligence Gathering

82. Which of the following statement is correct?

A. Overt testing can be costly and time consuming than covert testing.

B. Covert testing requires more skill than overt testing.

C. Overt testing is performed without the knowledge of most of the organization.

D. You collaborate with the organization to identify potential security threats during covert testing.

83. Which of the following is incorrect statement about script kiddies?

A. They are someone who does not understand the technical details of cybersecurity

B. They follow the instructions or tutorials of real hackers to perform their own attacks

C. They have the required knowledge and skill to perform an attack on a target system

D. They can create an equal amount of damage as a real hacker

84. Which of the following is not true statement about white hat hackers?

A. They use their skills to assist organizations and individuals in securing their networks.

B. They use their abilities for malicious purposes.

C. They are trustworthy hackers.

D. They are the good guys and girls of the industry.

85. Which of the following statement is true?

A. Vulnerability is anything that has the potential to cause harm to a system

B. Threat is a weakness or security flaw that exists in your system

C. An exploit is a tool, or code that is used to take advantage of a vulnerability on a system.

D. Zero-day attack occurs when hackers exploit the flaw after developers have fix it.

86. Which of the following is true about cyber espionage?

A. It is a subset of cyber crime

B. It is a type of cyber-attack in which criminals target governments and organizations to steal sensitive information.

C. We can detect and prevent it by establishing an effective security policy.

D. All

87. Which of the following is major problem of conventional encryption?

A. It is more complex and time consuming.

B. Secure transmission of the secret key

C. It uses less secure encryption function

D. It is no longer used today.

88. What is the best statement for taking advantage of a weakness in the security of an IT system?

A. Vulnerability
B. Threat
C. Exploit
D. Attack

89. If the value of P, Q, and the encryption key e are 11, 17, and 7 respectively. Find the plaintext value using RSA algorithm if the cipher text value is 11.

A. 122
B. 143
C. 221
D. 88

90. Why is an SSL certificate required in HTTP?

A. To encrypted data transmitted through the HTTP protocol
B. To send and receive unencrypted emails
C. To make information move more quickly
D. To compromise security

91. Helen has chosen to use public key cryptography when sending a message to David. She appends a digital signature " α" to her message M and encrypts it E (M, α). The message is then encrypted and sent to David. Which of the following key sequences is used for the encryption and decryption of the message?

A. Encryption: Helen's private key followed by David's private key; Decryption: Helen's public key followed by David's public key
B. Encryption: Helen's private key followed by David's public key; Decryption: Helen's public key followed by David's private key
C. Encryption: Helen's public key followed by David's private key; Decryption: David's public key followed by Helen's private key
D. Encryption: Helen's private key followed by David's public key; Decryption: David's private key followed by Helen's public key

92. What do we use in SSL to authenticate a message?

A. Message Authentication Code
B. Machine Authentication Code
C. Message Access Code
D. Machine Access Code

93. How can we describe Φ(n) in terms of p and q large prime numbers in RSA algorithm?

A. p*q
B. (p+1) *(q+1)
C. p/q
D. (p-1) *(q-1)

94. What are the total number of keys required for a group of n people to communicate with one another using secret key and public key crypto-systems respectively?

A. ((n *(n – 1))/2) & n
B. 2n & ((n *(n – 1))/2)
C. ((n*(n – 1))/2) & 2n
D. ((n*(n – 1))/2) * n

95. If the value of P, Q, and the encryption key e are 11, 17, and 7 respectively. Find the ciphertext value using RSA algorithm if the plaintext value is 22.

A. 44
B. 128
C. 22
D. 78

96. Which of the following is not an element of the X.509 certificates?

A. Issuer unique identifier
B. Name of the Issuer
C. Serial Modifier
D. Identifier Signature

97. Which of the following is incorrect about Trojan horses?

A. They contain the program that corrupt a data or damage a file.
B. They must be executed by the victim to do their work
C. They can replicate themselves
D. They are types of malwares that frequently masquerades as legitimate software.

98. Which one of the following is no a security mechanism?

A. User identification and authentication
B. Intrusion detection system and cryptography
C. Digital signature
D. None

99. Which of the following is not the function of firewall?

A. Prevent valuable information from being leaked without knowing.
B. Hiding the structure and the contents of internal network from internal users.
C. Prevent users on the network from sending valuable confidential files to other parties.
D. Prevent unauthorized modification of data

100. Assume Abyssinia Bank uses a scalable database to store detailed information about its customers, including account numbers. Which of the following is a potential threat to the bank's database?

A. Worms and trojan horses

B. Unauthorized access to client information

C. Unauthorized modification of client information

D. All can be considered as threat