CS4614 - Introductory Network Security

Exam number: □□□□□□

This questionnaire is automatically read by a computer program. Please use a pen for filling in your answers.

Check: ☒ Respond by placing an 'X' in the box next to the chosen answer.

Uncheck to correct: ■ You can correct an answer once, as shown on the left. This cannot be undone.

IMPORTANT: All answers should be provided in the spaces provided on this paper. You must write your exam number on each page.

1 Choice Questions

Answer all of the following questions by choosing one answer per question. Each question is worth 1.5 marks, for a total of 45 marks.

1.1 ________ involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect.

□ Disruption
□ Service denial
□ Replay
□ Masquerade

1.2 Verifying that users are who they say they are and that each input arriving at the system came from a trusted source is ________.

□ authenticity
□ accountability
□ credibility
□ integrity

1.3 When using symmetric encryption, it is very important to keep the algorithm secret.

□ True
□ False

1.4 On average, half of all possible keys must be tried to achieve success with a brute-force attack.

□ True
□ False

1.5 ________ attacks exploit the characteristics of the algorithm to attempt to deduce a specific plaintext or to deduce the key being used.

□ Brute-force
□ Block cipher
□ Cryptanalytic
□ Transposition

1.6 If both sender and receiver use the same key, the system is sometimes referred to as:

□ public-key encryption
□ asymmetric
□ two-key
□ conventional encryption

1.7 DES uses a 56-bit block and a 64-bit key.

□ True
□ False

1.8 All other things being equal, smaller block sizes mean greater security.

□ True
□ False

1.9 For symmetric encryption, key sizes of ________ or less are now considered to be inadequate.

□ 128 bits
□ 16 bits
□ 32 bits
□ 64 bits

1.10 A ________ cipher is one in which a block of plaintext is treated as a whole and used to pro ciphertext block of equal length.

- □ bit
- □ stream
- □ product
- □ block

1.11 The Advanced Encryption Standard (AES) has a fixed key length of 128 bits.

- □ True
- □ False

1.12 The ________ algorithm will work against any block encryption cipher and does not depend o particular property of DES.

- □ cipher block chaining
- □ counter mode attack
- □ meet-in-the-middle attack
- □ counter mode attack

1.13 The most significant characteristic of ________ is that if the same b-bit block of plaintext appe than once in the message, it always produces the same ciphertext.

- □ electronic codebook mode (ECB)
- □ cipher block chaining mode (CBC)
- □ multiple encryption
- □ block ciphers

1.14 There are well-defined tests for determining uniform distribution and independence to valida sequence of numbers is random.

- □ True
- □ False

1.15 The ________ test is the most basic test of randomness and must be included in any test suite

- □ frequency
- □ unpredictability
- □ runs
- □ Maurer

1.16 Asymmetric encryption utilizes only a public key for encryption and decryption.

- □ True
- □ False

1.17 3. Asymmetric encryption can be used for ________.

- □ both confidentiality and authentication
- □ confidentiality
- □ neither confidentiality nor authentication
- □ authentication

1.18 A considerably larger key size can be used for ECC compared to RSA.

- □ True
- □ False

1.19 The Secure Hash Algorithm design closely models, and is based on, the hash function ________

- □ MD5
- □ RFC 4634
- □ FIPS 180
- □ MD4

1.20 A cryptographic hash function is ________ when it is impossible to find an alternative mess input) with the same hash value as a given message (or input).

- □ collision resistant
- □ preimage resistant
- □ pseudorandomness
- □ second preimage resistant

1.21 Message authentication is a mechanism or service used to verify the integrity of a message.

- □ True
- □ False

1.22 Insertion of messages into the network from a fraudulent source is a ________ attack.

- □ content modification
- □ source repudiation
- □ masquerade
- □ sequence modification

1.23 It must be computationally infeasible to forge a digital signature, either by constructing a new message for an existing digital signature or by constructing a fraudulent digital signature for a given message.

□ True

□ False

1.24 Typically the session key is used for the entire duration of a logical connection, such as a frame relay connection or transport connection, and then it is permanently stored.

□ True

□ False

1.25 ________ is an authentication service designed for use in a distributed environment.

□ Kerberos

□ Toklas

□ PCBC

□ X.509

1.26 Cloud computing gives you the ability to expand and reduce resources according to your specific service requirement.

□ True

□ False

1.27 The SSL Internet standard version is called ________.

□ SSH

□ SLP

□ HTTPS

□ TLS

1.28 The most complex part of TLS is the ________.

□ SSL Record Protocol

□ Change Cipher Spec Protocol

□ Handshake Protocol

□ Alert Protocol

1.29 ________ email security threats could prevent end users from being able to send or receive email.

□ Authenticity-related

□ Confidentiality-related

□ Integrity-related

□ Availability-related

1.30 Standard DNS responses are cryptographically signed for authenticity.

□ True

□ False

2 Problems

Answer all of the following questions in the spaces provided on this paper. Each question is worth 15 marks, for a total of 45 marks.

2.1 Suppose $H(m)$ is a collision-resistant hash function that maps a message of arbitrary bit length into an n-bit hash value. Is it true that, for all messages x, y with $x \neq y$, we have $H(x) \neq H(y)$? Explain your answer.

2.2 In what ways can a hash value be secured so as to provide message authentication?

2.3 Consider the following threats to Web security and briefly describe how each is countered by a particular feature of TLS: (a) Brute-Force Cryptanalytic Attack: An exhaustive search of the key space for a conventional encryption algorithm. (b) Password Sniffing: Passwords in HTTP or other application traffic are eavesdropped. (c) Man-in-the-middle attack: An attacker interposes during key exchange, acting as the client to the server and the server to the client.