Chapter 1

TRUE/FALSE QUESTIONS:

T [✓ F] 1. Threats are attacks carried out.

[✓ T] F 2. Computer security is protection of the integrity, availability, and confidentiality of information system resources.

[✓ T] F 3. Data integrity assures that information and programs are changed only in a specified and authorized manner.

[✓ T] F 4. Availability assures that systems works promptly and service is not denied to authorized users.

T [✓ F] 5. The “A” in the CIA triad stands for “authenticity”.

[✓ T] F 6. The more critical a component or service, the higher the level of availability required.

[✓ T] F 7. Computer security is essentially a battle of wits between a perpetrator who tries to find holes and the administrator who tries to close them.

T [✓ F] 8. Security mechanisms typically do not involve more than one particular algorithm or protocol.

[✓ T] F 9. Many security administrators view strong security as an impediment to efficient and user-friendly operation of an information system.

[✓ T] F 10. In the context of security our concern is with the vulnerabilities of system resources.

T F 11. Hardware is the most vulnerable to attack and the least susceptible to automated controls.

T F 12. Contingency planning is a functional area that primarily requires computer security technical measures.

T F 13. X.800 architecture was developed as an international standard and focuses on security in the context of networks and communications.

T F 14. The first step in devising security services and mechanisms is to develop a security policy.

T F 15. Assurance is the process of examining a computer product or system with respect to certain criteria.

MULTIPLE CHOICE QUESTIONS:

1. __________ assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.

   A. Availability
   [✓ B. Privacy]
   C. System Integrity
   D. Data Integrity

2. ________ assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

   [✓ A. System Integrity]
   B. Availability
   C. Data Integrity
   D. Confidentiality

3. A loss of _________ is the unauthorized disclosure of information.

   [✓ A. confidentiality]
   B. authenticity
   C. integrity
   D. availability

4. A _________ level breach of security could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

   A. low
   B. moderate
   C. normal
   [✓ D. high]

5. A flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy is a(n) __________.

   A. countermeasure
   B. adversary
   [✓ C. vulnerability]
   D. risk

6. An assault on system security that derives from an intelligent act that is a deliberate attempt to evade security services and violate the security policy of a system is a(n) __________.

   A. risk
   [✓ B. attack]
   C. asset
   D. vulnerability

7. A(n) __________ is an action, device, procedure, or technique that reduces a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that correct action can be taken.

A. attack
B. adversary
C. countermeasure
D. protocol

8. A(n) _________ is an attempt to learn or make use of information from the system that does not affect system resources.

A. passive attack
B. outside attack
C. inside attack
D. active attack

9. Masquerade, falsification, and repudiation are threat actions that cause __________ threat consequences.

A. unauthorized disclosure
B. disruption
C. deception
D. usurpation

10. A threat action in which sensitive data are directly released to an unauthorized entity is __________.

A. corruption
B. intrusion
C. disruption
D. exposure

11. An example of __________ is an attempt by an unauthorized user to gain access to a system by posing as an authorized user.

A. masquerade
B. repudiation
C. interception
D. inference

12. The _________ prevents or inhibits the normal use or management of communications facilities.

A. passive attack
B. denial of service
C. traffic encryption
D. masquerade

13. A __________ is any action that compromises the security of information owned by an organization.

A. security mechanism
B. security policy
C. security attack
D. security service

14. The assurance that data received are exactly as sent by an authorized entity is __________.

A. authentication

B. access control

C. data confidentiality

D. data integrity

15. __________ is the insertion of bits into gaps in a data stream to frustrate traffic analysis attempts.

A. Traffic padding

B. Traffic control

C. Traffic routing

D. Traffic integrity

SHORT ANSWER QUESTIONS:

1. __________ is the protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources.

2. Confidentiality, Integrity, and Availability form what is often referred to as the _____.

3. A loss of _________ is the disruption of access to or use of information or an information system.

4. In the United States, student grade information is an asset whose confidentiality is regulated by the __________.

5. A(n) _________ is a threat that is carried out and, if successful, leads to an undesirable violation of security, or threat consequence.

6. A(n) _________ is any means taken to deal with a security attack.

7. Misappropriation and misuse are attacks that result in ________ threat consequences.

8. The assets of a computer system can be categorized as hardware, software, communication lines and networks, and _________.

9. Release of message contents and traffic analysis are two types of _________ attacks.

10. Replay, masquerade, modification of messages, and denial of service are example of _________ attacks.

11. Establishing, maintaining, and implementing plans for emergency response, backup operations, and post disaster recovery for organizational information systems to ensure the availability of critical information resources and continuity of operations in emergency situations is a __________ plan.

12. A(n) __________ assessment is periodically assessing the risk to organizational operations, organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission or organizational information.

13. The OSI security architecture focuses on security attacks, ___________, and services.

14. A ___________ is data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery.

15. Security implementation involves four complementary courses of action: prevention, detection, response, and __________.

Chapter 2

[✓ T] F 1. Symmetric encryption is used primarily to provide confidentiality.

[✓ T] F 2. Two of the most important applications of public-key encryption are digital signatures and key management.

T [✓ F] 3. Cryptanalytic attacks try every possible key on a piece of ciphertext until an intelligible translation into plaintext is obtained.

[✓ T] F 4. The secret key is input to the encryption algorithm.

T [✓ F] 5. Triple DES takes a plaintext block of 64 bits and a key of 56 bits to produce a ciphertext block of 64 bits.

[✓ T] F 6. Modes of operation are the alternative techniques that have been developed to increase the security of symmetric block encryption for large sequences of data.

T [✓ F] 7. The advantage of a stream cipher is that you can reuse keys.

[✓ T] F 8. A message authentication code is a small block of data generated by a secret key and appended to a message.

T [✓ F] 9. Like the MAC, a hash function also takes a secret key as input.

T F 10. The strength of a hash function against brute-force attacks depends solely on the length of the hash code produced by the algorithm.

T F 11. Public-key cryptography is asymmetric.

T **F** 12. Public-key algorithms are based on simple operations on bit patterns.

T **F** 13. The purpose of the DSS algorithm is to enable two users to securely reach agreement about a shared secret that can be used as a secret key for subsequent symmetric encryption of messages.

T F 14. An important element in many computer security services and applications is the use of cryptographic algorithms.

T F 15. Some form of protocol is needed for public-key distribution.

1. The original message or data that is fed into the algorithm is ___________.

A. encryption algorithm B. secret key

C. decryption algorithm **D. plaintext**

2. The ___________ is the encryption algorithm run in reverse.

A. decryption algorithm B. plaintext

C. ciphertext D. encryption algorithm

3. ___________ is the scrambled message produced as output.

A. Plaintext **B. Ciphertext**

C. Secret key D. Cryptanalysis

4. On average, ___________ of all possible keys must be tried in order to achieve success with a brute-force attack.

A. one-fourth **B. half**

C. two-thirds D. three-fourths

5. The most important symmetric algorithms, all of which are block ciphers, are the DES, triple DES, and the ___________.

A. SHA B. RSA

C. AES D. DSS

6. If the only form of attack that could be made on an encryption algorithm is brute-force, then the way to counter such attacks would be to ___________ .

A. use longer keys B. use shorter keys

C. use more keys D. use less keys

7. ___________ is a procedure that allows communicating parties to verify that received or stored messages are authentic.

A. Cryptanalysis B. Decryption

C. Message authentication D. Collision resistance

8. The purpose of a ___________ is to produce a "fingerprint" of a file, message, or other block of data.

A. secret key B. digital signature

C. keystream **D. hash function**

9. ___________ is a block cipher in which the plaintext and ciphertext are integers between 0 and n-1 for some n.

A. DSS **B. RSA**

C. SHA C. AES

10. A ___________ is created by using a secure hash function to generate a hash value for a message and then encrypting the hash code with a private key.

A. digital signature B. keystream

C. one way hash function D. secret key

11. Transmitted data stored locally are referred to as ___________ .

A. ciphertext B. DES

C. data at rest D. ECC

12. Digital signatures and key management are the two most important applications of ___________ encryption.

A. private-key **B. public-key**

C. preimage resistant C. advanced

13. A ___________ is to try every possible key on a piece of ciphertext until an intelligible translation into plaintext is obtained.

A. mode of operation B. hash function

C. cryptanalysis **D. brute-force attack**

14. Combined one byte at a time with the plaintext stream using the XOR operation, a ___________ is the output of the pseudorandom bit generator.

A. keystream B. digital signature

C. secure hash D. message authentication code

15. A __________ protects against an attack in which one party generates a message for another party to sign.

A. data authenticator **B. strong hash function**

C. weak hash function D. digital signature

SHORT ANSWER QUESTIONS:

1. Also referred to as single-key encryption, the universal technique for providing confidentiality for transmitted or stored data is _symmetric encryption_ .

2. There are two general approaches to attacking a symmetric encryption scheme: cryptanalytic attacks and ____brute-force______ attacks.

3. The ____decryption______ algorithm takes the ciphertext and the secret key and produces
the original plaintext.

4. A _____cryptanalytic_____ attack exploits the characteristics of the algorithm to attempt to deduce a specific plaintext or to deduce the key being used.

5. A ____block cipher______ processes the plaintext input in fixed-size blocks and produces a block of ciphertext of equal size for each plaintext block.

6. A ____stream cipher______ processes the input elements continuously, producing output one element at a time.

7. Public-key encryption was first publicly proposed by _____Diffie and Hellman_____ in 1976.

8. The two criteria used to validate that a sequence of numbers is random are independence and _____uniform distribution____ .

9. A ____back-end appliance_____ is a hardware device that sits between servers and storage systems and encrypts all data going from the server to the storage system and decrypts data going in the opposite direction.

10. In July 1998 the ____Electronic Frontier Foundation (EFF)______ announced that it had broken a DES encryption using a special purpose "DES cracker" machine.

11. The simplest approach to multiple block encryption is known as _____electronic codebook (ECB)_____ mode, in which plaintext is handled *b* bits at a time and each block of plaintext is encrypted using the same key.

12. A ____pseudorandom______ stream is one that is unpredictable without knowledge of the input key and which has an apparently random character.

13. The ____public and private key______ is a pair of keys that have been selected so that if one is used for encryption, the other is used for decryption.

14. _____library-based tape encryption_____ is provided by means of a co-processor board embedded in the tape drive and tape library hardware.

15. The purpose of the ____Diffie-Hellman Key Agreement______ algorithm is to enable two users to securely reach agreement about a shared secret that can be used as a secret key for subsequent symmetric encryption of messages.

Chapter 3

TRUE/FALSE QUESTIONS:

[✓ T] F 1. User authentication is the fundamental building block and the primary line of defense.

[✓ T] F 2. Identification is the means of establishing the validity of a claimed identity provided by a user.

T [✓ F] 3. Depending on the details of the overall authentication system, the registration authority issues some sort of electronic credential to the subscriber.

[✓ T] F 4. Many users choose a password that is too short or too easy to guess.

T [✓ F] 5. User authentication is a procedure that allows communicating parties to verify that the contents of a received message have not been altered and that the source is authentic.

[✓ T] F 6. A good technique for choosing a password is to use the first letter of each word of a phrase.

[✓ T] F 7. User authentication is the basis for most types of access control and for user accountability.

T [✓ F] 8. Memory cards store and process data.

[✓ T] F 9. Depending on the application, user authentication on a biometric system involves either verification or identification.

[✓ T] F 10. Enrollment creates an association between a user and the user's biometric characteristics.

T [✓ F] 11. An individual's signature is not unique enough to use in biometric applications.

[✓ T] F 12. Identifiers should be assigned carefully because authenticated identities are the basis for other security services.

[✓ T] F 13. A smart card contains an entire microprocessor.

T [✓ F] 14. Keylogging is a form of host attack.

[✓ T] F 15. In a biometric scheme some physical characteristic of the individual is mapped into a digital representation.

MULTIPLE CHOICE QUESTIONS:

1. ___________defines user authentication as “the process of verifying an identity claimed by or for a system entity”.

   [✓ A. RFC 4949] C. RFC 2298

   B. RFC 2493 D. RFC 2328

2. Presenting or generating authentication information that corroborates the binding between the entity and the identifier is the____________.

   A. identification step [✓ C. verification step]

   B. authentication step D. corroboration step

3. Recognition by fingerprint, retina, and face are examples of____________.

   A. face recognition C. dynamic biometrics

   [✓ B. static biometrics] D. token authentication

4. A____________is a password guessing program.

   A. password hash [✓ C. password cracker]

   B. password biometric D. password salt

5. The____________strategy is when users are told the importance of using hard to guess passwords and provided with guidelines for selecting strong passwords.

   A. reactive password checking C. proactive password checking

   [✓ B.] computer-generated password [✓ D. user education]

6. A___________strategy is one in which the system periodically runs its own password cracker to find guessable passwords.

A. user education

B. reactive password checking

C. proactive password checking

D. computer-generated password

7. The most common means of human-to-human identification are __________.

A. facial characteristics

B. retinal patterns

C. signatures

D. fingerprints

8. ___________systems identify features of the hand, including shape, and lengths and widths of fingers.

A. Signature

B. Fingerprint

C. Hand geometry

D. Palm print

9. Each individual who is to be included in the database of authorized users must first be___________in the system.

A. verified

B. identified

C. authenticated

D. enrolled

10. To counter threats to remote user authentication, systems generally rely on some form of____________protocol.

A. eavesdropping

B. challenge-response

C. Trojan horse

D. denial-of-service

11. A____________is when an adversary attempts to achieve user authentication without access to the remote host or to the intervening communications path.

A. client attack

B. host attack

C. eavesdropping attack

D. Trojan horse attack

12. A____________is directed at the user file at the host where passwords, token passcodes, or biometric templates are stored.

A. eavesdropping attack C. denial-of-service attack

B. client attack D. host attack

13. A____________attack involves an adversary repeating a previously captured user response.

A. client C. replay

B. Trojan horse D. eavesdropping

14. An institution that issues debit cards to cardholders and is responsible for the cardholder's account and authorizing transactions is the__________.

A. cardholder C. auditor

B. issuer D. processor

15. ___________allows an issuer to access regional and national networks that connect point of sale devices and bank teller machines worldwide.

A. EFT C. POS

B. BTM D. ATF

SHORT ANSWER QUESTIONS:

1. An authentication process consists of the identification_____step and the verification step.

2. Voice pattern, handwriting characteristics, and typing rhythm are examples of dynamic _____biometrics.

3. A shadow password file ______is a separate file from the user IDs where hashed passwords are kept.

4. With the complex password___policy a user is allowed to select their own password, but thesystem checks to see if the password is allowable.

5. The technique for developing an effective and efficient proactive password checker based on rejecting words on a list is based on the use of a Bloom_filter.

6. Objects that a user possesses for the purpose of user authentication are called tokens

7. Authentication protocols used with smart tokens can be classified into three categories: static, dynamic password generator, and challenge-response.

8. A biometric_authentication system attempts to authenticate an individual based on his or her unique physical characteristics.

9. The retinal pattern_ is the pattern formed by veins beneath the retinal surface.

10. A host generated random number is often called a nonce_____ .

11. _Eavesdropping______, in the context of passwords, refers to an adversary's attempt to learn the password by observing the user, finding a written copy of the password, or somesimilar attack that involves the physical proximity of user and adversary.

12. In a Trojan horse_attack, an application or physical device masquerades as an authentic application or device for the purpose of capturing a user password, passcode, or biometric.

13. A denial-of-service___attack attempts to disable a user authentication service by flooding the service with numerous authentication attempts.

14. A cardholder__is an individual to whom a debit card is issued.

15. The verification_step is presenting or generating authentication information that corroborates the binding between the entity and the identifier.