Computer Security 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 CIA triad.  
3. A loss of availability 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 FERPA.  
5. A(n) attack is a threat that is carried out and, if successful, leads to an undesirable  
violation of security, or threat consequence.  
6. A(n) countermeasure is any means taken to deal with a security attack.  
7. Misappropriation and misuse are attacks that result in usurpation threat consequences.  
8. The assets of a computer system can be categorized as hardware, software, communication  
lines and networks, and data.  
9. Release of message contents and traffic analysis are two types of passive attacks.  
10. Replay, masquerade, modification of messages, and denial of service are example of  
active 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 contingency plan.  
12. A(n) risk 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, mechanisms and services.  
14. A digital signature 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 recovery.

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 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.

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 proactive password checking strategy a user is allowed to select their own password, but the system 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 some similar 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.

X.800 defines access control as the prevention of unauthorized use of a resource,  
including the prevention of use of a resource in an unauthorized manner.  
2. An independent review and examination of system records and activities in order to test for  
adequacy of system controls, to ensure compliance with established policy and operational  
procedures, to detect breaches in security, and to recommend any indicated changes in control,  
policy and procedures is a(n) audit.  
3. Role based access control controls access based on the roles that users have within the system  
and on rules stating what accesses are allowed to users in given roles.  
4. Discretionary access control controls access based on the identity of the requestor and on access  
rules stating what requestors are or are not allowed to do.  
5. The basic elements of access control are: subject, object and access right.  
6. Basic access control systems typically define three classes of subject: owner, group and  
world.  
7. A discretionary access control scheme is one in which an entity may be granted access rights  
that permit the entity, by its own volition, to enable another entity to access some resource.  
8. The super user ID is exempt from the usual file access control constraints and has system  
wide access.  
9. A session is a mapping between a user and an activated subset of the set of roles to which  
the user is assigned.  
10. Role hierarchies make use of the concept of inheritance to enable one role to implicitly  
include access rights associated with a subordinate role.  
11. A prerequisite dictates that a user can only be assigned to a particular role if it is already  
assigned to some other specified role and can be used to structure the implementation of the least  
privilege concept.  
12. Object functions provide the capability to create, delete, and maintain RBAC elements  
and relations.  
13. The NIST model defines two types of role hierarchies: general role hierarchies and  
limited hierarchies.  
14. Static Separation of Duty enables the definition of a set of mutually exclusive roles, such  
that if a user is assigned to one role in the set, the user may not be assigned to any other role in the  
set.  
15. The administrative functions include the following: create a user session with a default set of  
active roles; add an active role to a session; delete a role from a session; and check if the session  
subject has permission to perform a request operation on an object.

A DBMS is a suite of programs for constructing and maintaining the database and for  
offering ad hoc query facilities to multiple users and applications.  
2. In a relational database columns are referred to as attributes.  
3. A view is the result of a query that returns selected rows and columns from one or more  
tables.  
4. SQL is a standardized language that can be used to define schema, manipulate, and  
query data in a relational database.  
5. With ownership-based administration the owner (creator) of a table may grant and revoke access  
rights to the table.  
6. In a centralized administration a small number of privileged users may grant and revoke  
access rights.  
7. In addition to granting and revoking access rights to a table, in a decentralized administration  
the owner of the table may grant and revoke authorization rights to other users, allowing them to  
grant and revoke access rights to the table.  
8. In a discretionary access control environment database users are classified into three broad  
categories: administrator, end user other than application owner, and application owner.  
9. The information transfer path by which unauthorized data is obtained is referred to as an  
10. A statistical database is one that provides data of a statistical nature such as counts and  
averages.  
11. When using the data swapping method attribute values are exchanged (swapped) between records  
in sufficient quantity so that nothing can be deduced from the disclosure of individual records.  
12. The user is a human entity that presents requests (queries) to the system.  
13. Cloud Computing is a model for enabling ubiquitous, convenient, on-demand network access to a  
shared pool of configurable computing resources that can be rapidly provisioned and released with  
minimal management effort or service provider interaction.  
14. A \_\_\_\_\_\_\_\_\_\_ cloud infrastructure is made available to the general public or a large industry  
group and is owned by an organization selling cloud services.  
15. The \_\_\_\_\_\_\_\_\_ model provides a predefined environment for the cloud subscriber that is shared  
with other tenants, typically through tagging data with a subscriber identifier.

A rootkit is a set of programs installed on a system to maintain covert access to that system with administrator (root) privileges while hiding evidence of its presence.

2. A blended attack uses multiple methods of infection or propagation to maximize the speed of contagion and the severity of the attack.

3. A computer virus is a piece of software that can “infect” other programs or any type of executable content and tries to replicate itself.

4. Sometimes referred to as the “infection vector”, the infection mechanism is the means by which a virus spreads or propagates.

5. Sometimes known as a “logic bomb”, the trigger is the event or condition that determines when the payload is activated or delivered.

6. The four phases of a typical virus are: dormant phase, triggering phase, execution phase and propagation phase.

7. During the triggering phase the virus is activated to perform the function for which it was intended. 8. A stealth virus is explicitly designed to hide itself from detection by anti-virus software.

9. Mobile code refers to programs that can be shipped unchanged to a heterogeneous collection of platforms and execute with identical semantics.

10. A drive-by-download is when a user views a Web page controlled by the attacker that contains a code that exploits the browser bug and downloads and installs malware on the system without the user’s knowledge or consent.

11. A botnet is a collection of bots capable of acting in a coordinated manner.

12. A bot can use a keylogger to capture keystrokes on the infected machine to retrieve sensitive information.

13. Countermeasures for malware are generally known as anti-virus mechanisms because they were first developed to specifically target virus infections.

14. Developed by IBM and refined by Symantec, the digital immune system provides a malware detection system that will automatically capture, analyze, add detection and shielding, or remove new malware and pass information about it to client systems so the malware can be detected before it is allowed to run elsewhere.

15. Generic decryption technology is an anti-virus approach that enables the anti-virus program to easily detect even the most complex polymorphic viruses and other malware, while maintaining fast scanning speeds.

A symmetric encryption scheme has five ingredients: plaintext, encryption algorithm, ciphertext, decryption algorithm and secret key.

2. Cryptanalysis is the process of attempting to discover the plaintext or key.

3. A block cipher processes the input one block of elements at a time, producing an output block for each input block.

4. A stream cipher processes the input elements continuously, producing output one element at a time as it goes along.

5. An encryption scheme is computationally secure if the cost of breaking the cipher exceeds the value of the encrypted information and/or the time required to break the cipher exceeds the useful lifetime of the information.

6. The AES was issued as a federal information-processing standard and is intended to replace DES and 3DES with an algorithm that is more secure and efficient.

7. RC4 was designed in 1987 by Ron Rivest and is a variable key-size stream cipher with byte-oriented operations.

8. “The input to the encryption algorithm is the XOR of the next 64 bits of plaintext and the preceding 64 bits of ciphertext” is a description of the CBC mode of operation.

9. Unlike ECB and CBC modes, CTR mode requires only the implementation of the encryption algorithm and not the decryption algorithm.

10. The most powerful, and most common, approach to countering the threats to network security is encryption.

11. With end-to-end encryption the encryption process is carried out at the two end systems.

12. With link encryption each vulnerable communications link is equipped on both ends with an encryption device.

13. For symmetric encryption to work the two parties to an exchange must share the same key, which must be protected from access by others.

14. All encryption algorithms are based on two general principles: substitution and transposition.

15. The three most important symmetric block ciphers are: 3DES, AES, and DES.

The Secure Hash Algorithm (SHA) was developed by the NIST and published as a federal information processing standard (FIPS 180) in 1993.

2. Versions of SHA, with hash value lengths of 256, 384, and 512 bits, (SHA-256, SHA-384, and SHA 512) are collectively known as SHA-2

3. The evaluation criteria for the new hash function are: security, cost and algorithm and implementation characteristics.

4. HMAC has been issued as RFC 2014, has been chosen as the mandatory-toimplement MAC for IP Security, and is used in other Internet protocols, such as Transport Layer Security.

5. One of the first public-key schemes, RSA was developed in 1977 by Ron Rivest, Adi Shamir, and Len Adleman.

6. Timing attacks are alarming for two reasons: they come from a completely unexpected direction and they are a ciphertext-only attack.

7. Four possible approaches to attacking the RSA algorithm are: brute force, timing attacks, mathematical attacks, and chosen ciphertext attacks.

8. NIST has published FIPS PUB 186, which is known as the DSS.

9. The purpose of the secret key algorithm is to enable two users to exchange a secret key securely that can then be used for subsequent encryption of messages.

10. One of the simplest hash functions is the XOR of every block.

11. “Must support hash value lengths of 224, 256,384, and 512 bits” and “algorithm must process small blocks at a time instead of requiring the entire message to be buffered in memory before processing it” are requirements for SHA-3.  
12. If speed is a concern, it is fully acceptable to use MD5 rather than SHA as the embedded hash function for HMAC.

14. The security of any MAC function based on an embedded hash function depends in some way on the cryptographic strength of the underlying hash function.

15. Perhaps the most widely used public-key algorithms are RSA and DiffieHellman.

SHA-1 is not very secure

A token can be forged or stolen by an adversary

The authentication process does not determine who is trusted for a given purpose

Diffie Hellman was the first published public key algorithm

Presenting or generating authentication info that corroborates the binding between the entity and the identifier is the verification step.

Challenge threats to remote user authentication, systems rely on some form of challenge-response protocol.

DAC is the traditional method of implementing access control

RBAC is based on the roles the users assume in a system rather than the user identity

An approval to perform an operation on one or more RBAC protected objects is permission

ECB is every 64 bits independently with the same key

CBC is an XOR with the next 64 bits of plaintext and the previous 64 bits of ciphertext

CTR – every block of plaintext is XOR with an encrypted counter. The counter is incremented for each subsequent block

Programmers use backdoors to debug and test their programs