Replay, masquerade, modification of messages, and denial of service are example of **active** attacks.  
  
An example of  **masquerade** is an attempt by an unauthorized user to gain access to a system by posing  
as an authorized user.

**Privacy** 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.

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

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

Release of message contents and traffic analysis are two types of **passive** attacks.

Contingency planning is a functional area that primarily requires computer security technical measures. **False**

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

Symmetric encryption is used primarily to provide confidentiality. **True**

Digital signatures and key management are the two most important applications of **public-key** encryption.

The **decryption algorithm** is the encryption algorithm run in reverse.

Triple DES takes a plaintext block of 64 bits and a key of 56 bits to produce a ciphertext block of 64  
bits. **False**

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

A message authentication code is a small block of data generated by a secret key and appended to a  
message. **True**  
  
 A good technique for choosing a password is to use the first letter of each word of a phrase. **True**

Each individual who is to be included in the database of authorized users must first be **enrolled** in the system.   
  
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. **False**

User authentication is the basis for most types of access control and for user accountability. **True**

**Hand geometry** systems identify features of the hand, including shape, and lengths and widths of fingers.

Enrollment creates an association between a user and the users biometric characteristics. **True**

A constraint is a defined relationship among roles or a condition related to roles. **True**

A concept that evolved out of requirements for military information security is **mandatory access control**.

External devices such as firewalls cannot provide access control services. **False**

An auditing function monitors and keeps a record of user accesses to system resources. **True**

The main innovation of the NIST standard is the introduction of the RBAC System and Administrative  
Functional Specification, which defines the features required for an RBAC system. **True**

**Constraints** provide a means of adapting RBAC to the specifics of administrative and security policies  
in an organization.

**Data perturbation** is when the data in the SDB can be modified so as to produce statistics that cannot be  
used to infer values for individual records.

A census database is an example of a pure statistical database. **True**

In a relational database rows are referred to as **tuples**.

SQL Server allows users to create roles that can then be assigned access rights to portions of the database. **True**

To create a relationship between two tables, the attributes that define the primary key in one table must appear as attributes in another table, where they are referred to as a foreign key. **True**

Random-sample query is a simple output perturbation technique. **True**

A bot propagates itself and activates itself, whereas a worm is initially controlled from some central  
facility. **False**

In addition to propagating, a worm usually carries some form of payload. **True**

Packet sniffers are mostly used to retrieve sensitive information like usernames and passwords. **True**

A macro virus infects executable portions of code. **False**

The term computer virus is attributed to **Fred Cohen** .

A program that is covertly inserted into a system with the intent of compromising the integrity or  
confidentiality of the victims data is **malware**.

A brute-force approach involves trying every possible key until an intelligible translation of the ciphertext into plaintext in obtained. **True**

A **permanent key** is a key used between entities for the purpose of distributing session keys.

AES uses a Feistel structure. **False**

The most widely used encryption scheme is based on **DES** the adopted in 1977 by the National  
Bureau of Standards.

Plaintext is the scrambled message produced as output. **False**

Symmetric encryption is also referred to as secret-key or single-key encryption. **True**

The operations performed during a round consist of circular shifts, and primitive Boolean functions  
based on DSS, MD5, SHA, and RSA. **False**

A **chosen ciphertext** type of attack exploits properties of the RSA algorithm.

SHA-3 algorithms must be designed to resist any potentially successful attack on SHA-2 functions. **True**

Unlike RSA, DSS cannot be used for encryption or key exchange. **True**

The  **RSA** scheme has reigned supreme as the most widely accepted and implemented approach  
to public-key encryption.

The appeal of HMAC is that its designers have been able to prove an exact relationship between the  
strength of the embedded hash function and the strength of HMAC. **True**