**NAME: DABO LAURA I.**

**MATRIC NUMBER: 16/SCI01/053.**

**COURSE CODE: CSC 418.**

**COURSE TITLE: INFORMATION SYSTEMS SECURITY.**

**ASSIGNMENT TITLE: REVISED QUESTIONS PART II.**

**Question**

1. Differentiate between these types of integrity:
2. A connection-oriented integrity service
3. Connection Integrity with Recovery
4. Connection Integrity without Recovery
5. Selective-Field Connection Integrity
6. Selective-Field Connectionless Integrity
7. Define the following:
8. Nonrepudiation, Origin
9. Nonrepudiation, Destination
10. Encipherment
11. Digital signature
12. Authentication exchange
13. Routing control
14. Notarization
15. Traffic Padding
16. Security Label
17. Define the following:
18. Plaintext
19. Ciphertext
20. Encryption
21. Decryption
22. Cryptography
23. Cryptanalysis
24. Cryptology
25. Cryptosystem
26. Symmetric encryption scheme has five ingredients; state and discuss.
27. What are two requirements for secure use of conventional encryption?
28. Discuss four key objectives of cryptography. Or four key objectives of cryptography are: confidentiality, integrity, non-repudiation and authentication. Discuss.
29. Discuss symmetric algorithm.
30. What is a compromise?
31. Give another name for attempted cryptanalysis.
32. Discuss four general types of cryptanalytic attack. Or four general types of cryptanalytic attack are ciphertext-only attack, known-plaintext attck, chosen plaintext attack and adaptive-chosen plaintext attack, discuss.

**ANSWERS**

1. A connection-oriented integrity service is the service that deals with a stream of messages, assures that messages are received as sent with no duplication, insertion, modification, reordering, or replays.

The connection-oriented integrity service addresses both message stream modification and denial of service.

1. Connection integrity with recovery provides for the integrity of all user data on a connection and detects any modification, insertion, deletion, or replay of any data within an entire data sequence, with recovery attempted.
2. Connection integrity without recovery provides for the integrity of all user data on a connection and detects any modification, insertion, deletion, or replay of any data within an entire data sequence, without recovery but detection only.
3. Selective-field connection integrity provides for the integrity of selected fields within the user data of a data block transferred over a connection and takes the form of determination of whether the selected fields have been modified, inserted, deleted, or replayed.
4. Selective-field connectionless integrity Provides for the integrity of selected fields within a single connectionless data block; takes the form of determination of whether the selected fields have been modified.
5. Nonrepudiation, origin can be defined as the proof that the message was sent by the specified party.
6. Nonrepudiation, destination can be defined as the proof that the message was received by the specified party.
7. Encipherment can be defined as the use of mathematical algorithms to transform data into a form that is not readily intelligible. The transformation and subsequent recovery of the data depend on an algorithm and zero or more encryption keys.
8. Digital signature can be defined as 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 (e.g., by the recipient).
9. Authentication exchange can be defined as a mechanism intended to ensure the identity of an entity by means of information exchange.
10. Routing control enables selection of particular physically secure routes for certain data and allows routing changes, especially when a breach of security is suspected.
11. Notarization can be defined as the use of a trusted third party to assure certain properties of a data exchange.
12. Traffic Padding can be defined as the insertion of bits into gaps in a data stream to frustrate traffic analysis attempts.
13. Security Label can be defined as the marking bound to a resource (which may be a data unit) that names or designates the security attributes of that resource.
14. Plaintext can be defined as the original message/data.
15. Ciphertext can be defined as the coded message/data.
16. Encryption can be defined as the process of converting from plaintext to ciphertext
17. Decryption can be defined as restoring the plaintext from the ciphertext.
18. Cryptography can be defined as the coding of message so as to render them unintelligible to other, than authorized recipients.
19. Cryptanalysis can be defined as the processing of an encrypted message to derive the original message by an attacker lacking prior knowledge of the secret key.
20. Cryptology can be defined as the field of both cryptography and cryptanalysis
21. Cryptosystem can be defined as an algorithm, and all possible plaintext, ciphertext and keys.
22. Plaintext: This is the original intelligible message or data that is fed into the algorithm as input.
23. Encryption algorithm: The encryption algorithm performs various substitutions and transformations on the plaintext.
24. Secret key: The secret key is also input to the encryption algorithm. The key is a value independent of the plaintext and of the algorithm. The algorithm will produce a different output depending on the specific key being used at the time. The exact substitutions and transformations performed by the algorithm depend on the key.
25. Ciphertext: This is the scrambled message produced as output. It depends on the plaintext and the secret key. For a given message, two different keys will produce two different ciphertexts. The ciphertext is an apparently random stream of data and, as it stands, is unintelligible.
26. Decryption algorithm: This is essentially the encryption algorithm run in reverse. It takes the ciphertext and the secret key and produces the original plaintext.
27. There is need for strong encryption algorithm. The algorithm must be such that an opponent who knows the algorithm and has access to one or more ciphertexts would be unable to decipher the ciphertext or figure out the key. This requirement is usually stated in a stronger form: The opponent should be unable to decrypt ciphertext or discover the key even if he or she is in possession of a number of ciphertexts together with the plaintext that produced each ciphertext.
28. Sender and receiver must obtained copies of the secret key in a secure fashion and must keep the key secure.
29. The four key objectives of cryptography are;
30. Confidentiality: The fundamental task of cryptography is to provide confidentiality by encryption methods. The encryption should guarantee secrecy and prevent attacker from deriving any information about the plaintext from the observed ciphertext.
31. Integrity: This is security service that deals with identifying any alteration to the data. The receiver of a message should be able to check whether the message was modified during transmission, either accidentally or deliberately. No one should be able to substitute a false message for the original message, or for parts of it.
32. Non-repudiation is a security service that ensures that an entity cannot refuse the ownership of a previous commitment or an action. The sender should not be able to later deny that he/she sent a message.
33. Authentication provides the identification of the originator. The receiver of a message should be able to verify its origin. No one should be able to send a message to the receiver and pretend to be the sender (data origin authentication). When initiating a communication sender and receiver should be able to identify each other (entity authentication).
34. Symmetric algorithms sometimes referred to as conventional algorithms are algorithms where encryption key can be calculated from the decryption key and vice versa. In most symmetric algorithm encryption and decryption key are the same. These algorithms are also called secret key algorithm, single key algorithm or one key algorithm require that the sender and receiver agree on a key before they can communicate securely.

The security of the symmetric rests in the key: divulging the key means that anyone could encrypt and decrypt messages. As long as communication needs to remain secret, the key must remain secret. Symmetric algorithm can be divided into two categories which are stream algorithm also known as stream cipher (which operates on the plaintext a single bit/byte at a time) and block algorithm also known as block cipher (which operates on the plaintext in groups of bits/blocks).

1. A compromise is the use of key through non-cryptanalytic means.
2. Another name for attempted cryptanalysis is an attack.
3. Ciphertext-only attack: The cryptanalyst has the ciphertext of several messages, all of which have been encrypted using the same encryption algorithm. The cryptanalyst’s job is to recover the plaintext of as many messages as possible or to deduce the key (or keys) used to encrypt the message in order to decrypt other messages encrypted with the same key.
4. Known-plaintext attack: The cryptanalyst has access not only to the ciphertext of several messages, but also to the plaintext of those messages. His job is to deduce the key (or keys) used to decrypt any new messages encrypted with the same key(s).
5. Chosen plaintext attack: The cryptanalyst does not only have access to the ciphertext and associated plaintext for several messages, but he also chooses the plaintext that gets encrypted. This more powerful than a known-plaintext attacks because the cryptanalyst can choose specific plaintext blocks to encrypt, ones that might yield more information about the key. His job is to deduce the key(s) used to encrypt the messages or an algorithm to decrypt any new messages encrypted with the same key(s).
6. Adaptive-chosen plaintext attack: This is a special case of a chosen-plaintext attack. Not only can the cryptanalyst choose the plaintext that is encrypted but he can also modify his choice based on the results of previous encryption.