Operating system and computer security Short note

HNDIT-2nd year 1st semester

Q1 briefly explain following terms

1.) **Cryptanalysis**- The study of principles and methods of transforming an unintelligible message back into an intelligible message **without knowledge of the key**

security concepts

1) **Confidentiality**- the ability of a system to ensure that an asset is **viewed** only by authorized parties
   mechanism -**Encryption**

2) **Integrity** -the ability of a system to ensure that an asset is **modified** only by authorized parties
   mechanism -**Digital signature /message authentication code**

3) **Availability**- the ability of a system to ensure that an asset **can be used** by any authorized parties

1) **Vulnerability**–a weak point in a system where a threat can sneak in

2) **Threat**–a potential damage that can be materialized through some flaw in the system

3) **Risk**–the probability of a threat being materialized by exploiting a vulnerability

4) **Control**–any procedure that is in place to assure security of a system

5) **Computer Security**- **protect data** and to thwart hackers

6) **Network Security**- **protect data** during their **transmission**

7) **Internet Security**-measures to **protect data** during their transmission **over a collection of interconnected networks**

8) **Data Integrity -** **accuracy & Consistency of data** stored in database

9) **Integrity control on constrains -** a condition or restriction that is applied to a particular set of data is commonly termed as integrity control on constrains

10) **Plain text –** the original message

11) **Cipher Text –** the coded message

12) **Cipher – algorithm** use to encrypt plain text to cipher text

13) **Key –** the price of information which used to encrypt message

14) **Encipher (encrypt) –** Converting plain text to cypher text

15) **Decipher (decrypt)** - Convert cipher text to plain text

16) **Authentication -** assurance that the communicating entity is the one claimed

17) **Access Control** - prevention of the unauthorized use of a resource

18) **Non-Repudiation -** protection against denial by one of the parties in a communication

Q2 Briefly explain security attack

1) **Security attack**: any action that compromises the security of information owned by an organization
2) **passive attacks** - eavesdropping on, or monitoring of, transmissions to:
   –obtain message contents, or
   –monitor traffic flows

3) **active attacks**–modification of data stream to:
   –masquerade of one entity as some other
   –replay previous messages
   –modify messages in transit
   –denial of service(ddos)
4) **Security Mechanism** - a mechanism that is designed to detect, prevent, or recover from a security attack

Q3 Encryption algorithm

1) Substitution Ciphers
   Caesar Cipher,
   Monoalphabetic Cipher,
   One-Time Pad

2) Transposition Ciphers
   Rail Fence cipher,
   Row Transposition Ciphers

Created by- Shan Pathiraja HNDIT(2018) A/Pura

If you have any problem regarding this please contact me 0778113997