NIST College Banepa

Department of BScCSIT

5th Semester

Cyrptography

Tutorial 1

1. Define the terms:
    a. Computer security
    b. Network security
    c. Internet security
    d. Cryptography
    e. Cryptanalysis
    f. Cryptosystem
    g. Encryption
    h. Decryption
    i. Cipher
2. Define the goals of security goals.
3. Distinguish between passive and active security attack. Name some passive attacks and name some active attacks.
4. What do you mean by reply attacks? Describe with an example
5. Define the type of security attack in each of the following cases:
    a. A student breaks into a professor's office to obtain a copy of the next day's test.
    b. A student gives a check for $ to buy a used book. Later she finds that the check was cashed for $100.
    c. A student sends hundreds of e-mails per day to another student using a phony return e-mail address.
    d. Suppose a key logger program intercepts user password and is used to modify the user account. Now, justify whether it's a violation of confidentiality, integrity, or availability or some of combination of them.
6. Which security mechanism(s) are provided in each of the following cases?
    a. A school demands student identification and a password to let students log into the school server.
    b. A school server disconnects a student if she is logged into the system for more than two hours.
    c. A professor refuses to send students their grades by e-mail unless they provide student identification they were preassigned by the professor.

d. A bank requires the customer's signature for a withdrawal.

7. Describe the main requirements for the secure use of symmetric encryption.
8. What are the two basic functions used in encryption algorithms?
9. Differentiate between secret-key encryption and public-key encryption.
10. What is the difference between a block cipher and a stream cipher?
11. Mention the advantages of using stream ciphers over block ciphers.
12. Are all stream ciphers monoalphabetics? Explain.
13. Are all block ciphers polyalphabetic? Explain.
14. What are the two general approaches to attacking a cipher?
15. List and briefly define types of cryptanalytic attacks based on what is known to the attacker.
16. What is the difference between an unconditionally secure cipher and a computation ally secure cipher?
17. Why is the Caesar cipher substitution technique vulnerable to a brute-force cryptanalysis?
18. How much key space is available when a monoalphabetic substitution cipher is used to replace plaintext with ciphertext?
19. What is the drawback of a Playfair cipher?
20. All classical ciphers are based on symmetric key encryption. What does that mean?
21. What makes Vigenere cipher more secure that say, the Playfair cipher?
22. What is the difference between a monoalphabetic cipher and a polyalphabetic cipher? Justify with suitable examples.
23. What are two problems with the one-time pad?
24. What is a transposition cipher?
25. What are the drawbacks of Steganography?
26. How chosen plaintext attack differs from chosen ciphertext attack?
27. Explain different kinds of cryptanalysis attacks.

Date of Submission: 15th Sep, 2023