KATHMANDU UNIVERSITY
End Semester Examination [C]
11 April, 2023

Marks Scored:

Level : B.Sc.
Year : IV

Course : COMP 485
Semester : I

Exam Roll No. :

Time: 30 mins.

F. M. : 10

Registration No.:

Date :

SECTION "A"
[20Q. × 0.5 = 10 marks]

Encircle the most appropriate alternative from each set of choices.

1. Which of the following is an objective of network security?
   a. Confidentiality
   b. Integrity
   c. Availability
   d. All of the above

2. Caesar Cipher is an example of _____.
   a. Poly-alphabetic Cipher
   b. Mono-alphabetic Cipher
   c. Multi-alphabetic Cipher
   d. Bi-alphabetic Cipher

3. On Encrypting "thepepsiisintherefrigerator" using Vignere Cipher System using the keyword "HUMOR" we get cipher text-
   a. abqdnwewuwjphfvrrtrfznsdokvl
   b. abqdvmwuwjphfvvyyrfznydokvl
   c. tbqyrvmwuwjphfvvyyrfznydokvl
   d. baiuvmwuwjphfoeiyrfznydokvl

4. Which one of the following is **NOT** a RC5 mode of operation?
   a. RC5 block cipher
   b. RC5-Cipher Block Chaining
   c. RC5-Cipher Padding
   d. RC5-CipherText Stealing

5. Which of these is **NOT** a characteristic of block ciphers?
   a. Variable key length / block size / number of rounds
   b. Mixed operators, data/key dependent rotation
   c. Key independent S-boxes
   d. More complex key scheduling

6. The DES Algorithm Cipher System consists of _____rounds (iterations) each with a round key.
   a. 12 b. 18 c. 9 d. 16

7. In the DES algorithm the round key is ____ bit and the Round Input is _____ bits.
   a. 48, 32 b. 64,32 c. 56, 24 d. 32, 32

8. What is the minimum size of the key in blowfish algorithm?
   a. 64 bits b. 32 bits c. 56 bits d. 48 bits

9. When a hash function is used to provide message authentication, the hash function value is referred to as _____.
   a. Message Field b. Message Digest c. Message Score d. Message Leap

10. Message authentication code is also known as _____.
    a. key code
    b. hash code
    c. keyed hash function
    d. message key hash function

11. SHA-1 produces a hash value of _____.
    a. 256 bits
    b. 160 bits
    c. 180 bits
    d. 128 bits

12. For the Knapsack: {1 6 8 15 24}, Find the cipher text value for the plain text 10011.
    a. 40
    b. 22
    c. 31
    d. 47

13. In the RSA algorithm, we select 2 random large values 'p' and 'q'. Which of the following is the property of 'p' and 'q'?
    a. p and q should be divisible by $\Phi(n)$
    b. p and q should be co-prime
    c. p and q should be prime
    d. p/q should give no remainder

14. What is the PGP stand for?
    a. Permuted Gap Permission
    b. Permuted Great Privacy
    c. Pretty Good Permission
    d. Pretty Good Privacy

15. PGP makes use of which cryptographic algorithm?
    a. DES
    b. AES
    c. RSA
    d. Rabin

16. Which system uses a trusted third party interface?
    a. Public-Key Certificates
    b. Public announcements
    c. Publicly available directories
    d. Public-Key authority

17. A false positive in an IDS can be defined as _____.
    a. An alert that indicates nefarious activity on a system that, upon further inspection, turns out to represent legitimate network traffic or behavior
    b. An alert that indicates nefarious activity on a system that, upon further inspection, turns out to truly be nefarious activity
    c. The lack of an alert for nefarious activity
    d. All of the above

18. Where an IPS is commonly placed in a network?
    a. In front of the firewall
    b. In line with the firewall
    c. Behind the firewall
    d. On the end users' device

19. Which one of the following is not a public key distribution means?
    a. Public-Key Certificates
    b. Hashing Certificates
    c. Publicly available directories
    d. Public-Key authority

20. Encryption transformations are known as _____.
    a. Diffusion
    b. Confusion
    c. Diffusion & Confusion
    d. None of the mentioned

KATHMANDU UNIVERSITY
End Semester Examination [C]
11, April, 2023

Level : B.Sc.
Year : IV
Time : 2 hrs. 30 mins.

Course : COMP 485
Semester : I
F.M. : 40

SECTION "B"
[6Q. × 4 = 24 marks]

Attempt *ANY SIX* questions.

1. Explain the components of Information Security.

2. Explain the working mechanism of RSA algorithm with suitable example.

3. Differentiate between Hashing and Encryption. State and explain all three resistant properties of Hash function.

4. Explain the purpose of Public Key Infrastructure (PKI). How does Certificates help the resource in the internet?

5. Discuss all three authentication mechanism that X.509 certificate follows.

6. Explain the SSL protocol architecture. Also explain the steps of SSL handshake protocol.

7. What is the purpose of using VPN? Also discuss the types of VPN and their purposes.

SECTION "C"
[2Q. × 8 = 16 marks]

Attempt *ANY TWO* questions.

8. You are a security officer working for a medium-sized research company. You have been assigned to guard the facility. Two incidents occur. The first, a well-known manager walks out with a box of papers. The second, someone believed to be an outsider assesses the company information and goes away with the company blue prints for the next generation product. [4+4]
   a. Briefly explain security gaps, vulnerabilities and threats.
   b. Describe how these incidents can be prevented.

9. Explain the Data Encryption Standard (DES) algorithm with suitable diagram about its operation. Also differentiate the performance of DES with AES. [6+2]

10. Explain the necessary mechanism required to conduct a virtual election. What would be the main security concerns in such a virtual elections? How digital signatures can be used to authenticate the voters in virtual election? [8]