UKA TARSADIA UNIVERSITY

Integrated M.Sc. (IT) (Semester 5)
060010504(2013-14)
Information Security

Date :26/11/2021 **Time :**9:30AM- 12:30PM
Max. Marks:60

Instructions :

1. Attempt all questions.
2. Write each section in a separate answer book.
3. Make suitable assumptions wherever necessary.
4. Draw diagrams/figures whenever necessary.
5. Figures to the right indicate full marks allocated to that question.
6. Follow usual meaning of notations/abbreviations.

SECTION - 1

Q 1 A) Answer the following. **[4]**

I) State any two goals of information security.

II) Define the below given terms.
1.Cryptanalysis 2.Cryptography.

Q 1 B) Answer the following in detail. (Any One) **[6]**

I) Write the steps for initialization of the RC4 algorithm.

II) What is a stream cipher? List out two disadvantages of the RC4 algorithm.

Q 2 Answer the following. **[10]**

A) Among the following explain any two classic cipher with proper example.
1. Double transposition cipher
2. One time pad
3. Simple substitution cipher

OR

A) Demonstrate feistel cipher designing principle with proper diagram.

B) What is the block length and key size of advanced encryption standard cipher? Explain AES working mechanism with necessary diagram.

OR

B) Differentiate CBC with ECB mode in detail. Draw diagram to illustrate encryption and decryption in both mode.

Q 3 Answer the following in detail. (Any 2) **[10]**

I) Explain repeated squaring technique of RSA with an example.

II) What are the steps involved in Diffie-Hellman key exchange principle?

III) What is public key infrastructure? Explain confidentiality and non-repudiation in detail.

SECTION - 2

Q 4 A) Answer the following. **[4]**

I) List and define any two non-cryptographic hashes.

II) Note down any four characteristics of hash functions.

Q 4 B) Answer the following in detail. (Any One) **[6]**

I) Briefly define one outer round with all its inner rounds of tiger hash.

II) Write a short note on: Birthday problem in hashing context.

Q 5 Answer the following. **[10]**

A) Write a brief note on common attack path for an attacker to crack the password. Discuss different cryptanalysis technique for password cracking.

OR

A) List all possible authentication method. Explain any one in detail.

B) Demonstrate packet filter firewall with an example. Also discuss advantages and disadvantages of it.

OR

B) Demonstrate stateful packet filter firewall with an example. Also discuss advantages and disadvantages of it.

Q 6 Answer the following in detail. (Any 2) **[10]**

I) Which are the two methods for intrusion detection? Explain any one in detail.

II) Write the example of biometrics. Compare all with the help of advantages and disadvantages.

III) Illustrate verification process for password with an example.