UKA TARSADIA UNIVERSITY

B.Sc. (IT)/Integrated M.Sc. (IT) (Semester 5)
IT5012(2021-22)/060010509(2017-18)
DSE9 Information Security/Fundamentals of 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 the difference between private key and public key.

II) What is a stream cipher? Give an example.

III) Define the term cryptology.

IV) What is the use of a key?

Q 1 B) Answer the following in brief. (Any 3) **[6]**

I) List out the steps of initialization of RC4 algorithm.

II) What is non-repudiation? Why is non-repudiation important in security?

III) List the principles given by Claude Shannon.

IV) Convert the following ciphertext to plaintext by using the ceaser cipher.
IRXUVFRUHDQGVHYHQBHDUVDJR

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

A) Manav and Aarav both are using letter encoding table which is as follow, how Manav will encrypt the given plain text and Aarav will decrypt the same to receive actual plain text? Plain text is "Nathuram Godse killed Gandhiji", where key is, "Mahatmaji Mahatmaji Mahatmaji"

A	D	E	G	H	I	J	K	L	M	N	O	R	S	T	U
0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111

OR

A) Briefly define double transposition cipher. Discuss the cryptanalysis technique on classis cipher with an example.

B) What is block size and key length of AES algorithm? How many rounds performed in AES? Briefly define all possible function performed in one round of AES.

OR

B) Demonstrate ECB and CBC block cipher mode in detail.

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

I) Demonstrate DH key exchange principle along with its cryptanalysis technique.

II) Sender's RSA public key is (e,N)=(3, 33) and her private key is d=7. If sender encrypts the message M=17, what is the ciphertext C? Show that how receiver can decrypt ciphertext C to obtain plaintext M.

III) Discuss public key cryptography uses with reference to any real world application.

SECTION - 2

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

I) Define the term: Hash Function.

II) State the probability expression used to solve the birthday problem.

III) List two properties of hash function.

IV) Give two examples of one-way functions.

Q 4 B) Answer the following in brief. (Any 3) **[6]**

I) What is the block size in tiger hash and HMAC?

II) What is the main difference between encryption and hashing?

III) List two uses of hash functions.

IV) State two advanatges of HMAC algorithm.

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

A) Among the different method of authentication, provide your comment on following,

1. Which method is more secure?
2. Which method is more popular?

Explain any one authentication method in detail.

OR

A) State the difference between key and password? Discuss different cryptanalysis technique for password cracking.

B) Write a detail note on application proxy firewall with an example.

OR

B) Write a detail note on stateful packet filter firewall with an example.

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

I) "Salt value makes life more difficult for the bad guys by hashing each password." – Discuss the given statement with an appropriate example.

II) Which are the two type of subject for biometric scanning? Explain fingerprint scan biometric in detail.

III) List and define two basic architecture of IDSs. Explain any one method of IDSs.