UKA TARSADIA UNIVERSITY

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

Date :31/05/2017 **Time :**1:30PM- 4:30PM
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 goal of cryptanalyst.

II) What is the point of Kreckoff's principle?

III) Give name of any two stream cipher algorithm.

IV) State deffusion principle of Claude Shannon.

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

I) Briefly define the concept of CIA with an example.

II) "Crypto refers as a black box" – Justify the statement.

III) Briefly define the execution process of stream cipher. Also give one example of stream cipher.

IV) What is RC4? Briefly define RC4 initialization process.

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

A) Using the letter encoding from below table, ciphertext message "KITLKE" was encrypted with a one-time pad:

Letter Encoding Table								
Letter	E	H	I	K	L	R	S	T
Binary	000	001	010	011	100	101	110	111

If the plaintext is "thrill", what is the key? If the plaintext is "tiller", what is the key?

OR

A) Encrypt the message "we are all together" using double transposition cipher with 4 rows and 4 columns, using the following row and column permutation.
For row permutation use,
(1, 2, 3, 4) --> (2, 4, 1, 3)
For column permutation use,
(1, 2, 3, 4) --> (3, 1, 2, 4)
Also decrypt the encrypted message to retrieve the plain text.

B) Demonstrate feistel cipher principle with diagram. How DES algorithm implements feistel cipher principle? Explain in detail.

OR

B) Differentiate AES with DES. Discuss AES in detail with proper structure.

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

I) What are the steps involved in encryption and decryption process for RSA algorithm?

II) Explain DH key exchange principle in detail. Which major concern must have to focus while using DH algorithm?

III) What is PKI? Among the following explain any two in detail,

1) Digital certificate
2) Certificate Revocation List
3) Monopoly model and Oligarchy model

SECTION - 2

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

I) State one difference between MD5 and SHA-1.

II) What is the probability that at least one person having same birthday as you?

III) Write number of outer round and inner round performed in tiger hash.

IV) What can be used in place of MAC in case of message integrity?

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

I) What is the use of hash function? List any two properties of hash function.

II) Briefly define outer round of tiger hash.

III) How hash functions play an important role while receiving spam e-mails?

IV) Briefly define one non-cryptographic hash that is widely used.

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

A) Mr. Aanand is new in cyber world. Help him for selecting password. Provide list of possible password, do certain experiment on it to crack the password. So based on this experiment Mr. Aanand can choose strong password.

OR

A) Among the following which one is most popular? Which one is more secure? Provide the reason for same. Write a brief note on any one of following.
- Something you know
- Something you are
- Something you have

B) What is the job of firewall? Demonstrate packet filter firewall in detail.

OR

B) Illustrate application proxy firewall in detail.

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

I) What is intrusion detection system? Who can be intruder? What sorts of attack might an intruder launch?

II) Provide example of bio-metric. Explain any two in detail.

III) Explain CAPTCHA in detail.