Mode of Examination: Online

M.Sc.(Computer Science) Semester – III Examination, 2020

Subject: Computer Science

Paper: CSM 304 - CBCS-B (Cryptography & Network Security)

Full Marks: 70

Date: 17.03.2021 **Time: 12:00 noon to 3:00 PM**

Please note the following instructions carefully:

Promise not to commit any academic dishonesty.
Marks will be deducted if the same/similar answers are found in different answer-scripts.
Candidates are required to answer in their own words as far as applicable.
Each page of the answer scripts should have your University Roll # on the right-top corner.
The name of the scanned copy of the answer script will be of the following format:
CSM304-CNS-Roll Number.pdf
(Example: CSM304-CNS-C91-CSC-191001.pdf)

The subject of the mail should be the file name only.

The name of the scanned answer-script is to be sent to cucse2020@gmail.com
The report should have the top page (Page #1) as an index page; mention page number(s) against the answer of each question number.
The answer-script may not be accepted after the scheduled time.

Answer ***Question No.1 Question No. 2,*** and ***any four*** from the rest.

1. **Answer any five from the questions given below** (5 x 2 =10)

a) Explain the avalanche effect.

b) List all multiplicative inverse pairs in modulus 20.

c) Find all solutions for the linear equation $9x + 4 \equiv 5 \pmod 7$

d) Prove that $<Z_6^*, x>$ is an abelian group.

e) State the role of "nonce" in authentication scheme? Is it possible to use timestamp as a nonce?

f) Test the primality of the integer 19 using square root test.

g) What do you mean by Diffusion Optimality in AES?

h) Should we have variable-length message digests or fixed-length ones? Justify.

2. **Answer any five from the followings:** (5 x 4 =20)

a) Find the orders of all elements in the group G = < Z_9 *>.

b) Use the Extended Euclidian Algorithm to find the multiplicative inverse of $X^4 + X^3 + 1$ in GF (2^5) with the modulus $X^5 + X^2 + 1$.

c) "The mixing transformation (Mix-Column) is not needed in DES but essential in AES" Justify the statement.

d) The Miller-Rabin test can determine if a number is not prime but cannot determine if a number is prime. How can such an algorithm be used to test for primality?

e) State the possible threat(s) in context of password based authentication. Also state measure(s) to conquer the said threats.

f) Through an example, explain chosen Plain text attack. How it differs from PT-CT attack?

g) Explain how same plain text block may result in different cipher text block using CFB mode of operation.

3. (a) Discuss the role of Key Distribution Centre (KDC) for authentication and key-distribution through an example.

(b) Explain the concept of Challenge-Response authentication through Needham-Schroder Algorithm. [4+6]

4. (a) Given integers *a* and *x*, what is the bit level complexity of the classical algorithm to compute the expression a^x. Consider *a* and *x* as two large numbers. Is it possible to improve the complexity by proposing a different approach? Discuss in detail with necessary justification.

(b) State the Pigeon hole principle and mention it's usefulness on analyzing attack on Hash functions.

[7+3]

5. (a) State the motivation behind proposing Elliptic Curve Cryptography even if the performance of RSA is satisfactory.

(b) What is the one way function and trapdoor used in ECC?

(c) Define the key generation process and also comment on the strength of the algorithm.

[2+3+ (3+2)]

6. (a) State the importance of collision resistance criterion of a Hash function.

(b) State the birthday paradox problem and discuss its utility for maintaining collision resistance property in MD.

(c) State the principal advantage of HMAC over SHA-1. [2+6+2]

7. (a) Critically comment - "It is possible for a spoofing attack to occur in Diffie Hellman Key exchange algorithm"

(b) Is DES a Feistel Cipher? Why or Why not? Describe the necessity of S-Box in context of DES algorithm. [5+(1+4)]

8. (a) State the security services provided by the Digital Signature. Discuss the El Gamal scheme for achieving the said security services.

(b) Is Zero knowledge authentication better than other alternative approaches?

[(2+6) +2]

9. Find the value of $\Phi(77)$ using Euler's Totient function. Design a LFSR of length 4 whose connection polynomial is $1+D+D^4$. Write down its sequence. [2 + 4 + 4]