UNIVERSITY OF CALCUTTA
Mode of Examination: Online
M.Sc. (Computer Science) Semester – III Examination, 2021

2021

Subject: Computer Science

Paper Code & Name: CSM304 (CBCS B) Cryptography & Network Security

Date: 25.01.2022 **Time and Duration: 12:00 pm to 3:00 pm (3 hours)**

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:
(Example: CSM-304B-CNS-My Roll Number.pdf)
The subject of the mail should be the file name only.
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.
Extra 30 minutes is allowed for uploading the answer script.

Answer Question number 1, 2, and any Four from the rest.

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

a) Find the orders of all elements in the group G = $< Z_7^*, X >$.
b) Find the value of Φ(32) and Φ(80) .
c) Find the value of 12^{-11} mod 77 using Euler's theorem.
d) In RSA, why the specific group $< Z_{\Phi(n)}^*, X >$ is used for key generation?
e) Test the primality of the integer 19 using square root test.
f) State the feature(s) for discriminating the challenge of response-based authentication approach than password-based authentication.
g) State the advantage of using KDC for key distribution.

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

a) Show an LFSR with the characteristic polynomial x^5+x^2+1. What will be the maximum period? State the main feature for discrimination between this stream cipher generation technique with the CFB method. (3+1)
b) Explain why the 64 bit MD is not preferable in an ideal Hash generation algorithm.
c) Use the Extended Euclidian Algorithm to find the multiplicative inverse of $X^3 + X + 1$ in GF (2^4) with the modulus $X^4 + X + 1$.
d) Consider the elliptic curve $E_{11}(1, 6)$; Determine all of the points in the curve.

e) In a group G = $<Z_n^*, X>$ with primitive roots the number of primitive roots is $\Phi(\Phi(n))$. Show that it holds for n=7.

f) Write an algorithm to form the sub-keys as needed in AES-128, from a single secret key.

g) Explain the reasons behind the widely acceptance of $GF(2^n)$ field in the cryptography domain.

3. (a) Show that the bit-operation complexity of encryption or decryption in El Gamal cryptosystem is Polynomial.

(b) Write a note on possible "factorization attack" in RSA. [6+4]

4 (a) Through a neat diagram, describe the process of signing and verifying for RSA digital signature scheme.

(b) A club has only 100 members. How many secret keys are needed for the given cases:
i) If all members of the club need to send secret messages to each other.
ii) If everyone trusts the President of the club i.e. messages are transferred between members through president.
iii) If President decides that two members should inform President; then the President creates a temporary key to be used between the two. The temporary key is encrypted and sent to both members.
[6+4]

5. (a) On the elliptic curve over the real numbers, let P (x_1,y_1) and Q (x_2, y_2) are two points. Find the co-ordinates of the points P+Q and 2P. The detailed calculations must be described.

(b) Describe the Key exchange procedure as used in IPSec to overcome the meet in the middle attack.
[6+4]

6. (a) Explain the "Statistical digram attack" and state a method to overcome it.

(b) "2047 is a strong pseudo prime number for the base 2" ---- Comment with explanation.

[(2+3) +5]

7. Encrypt the message "ATTACK IS TONIGHT" using the Hill cipher with the key as given below. Show your calculations and the result. Also show the calculations for the corresponding decryption of the cipher text to recover the original plaintext.

3	10	20
20	9	17
9	4	17

[5+5]

8. a) "Mix column is the only bit level substitution in AES" Comment with necessary explanation.
b) The fixed and one-time passwords are two extreme solutions. Propose a scheme for frequently changed password avoiding the typical disadvantage of one-time password scheme.
[6+4]