Total No. of Pages : 04 Roll No. .....

PGDCS-08
Computational Number Theory & Cryptography
PG Diploma in Cyber Security (PGDCS-17)

2nd Semester, Examination, 2019

Time : 3 Hours *[Maximum Marks : 80*

Note : This paper is of Eighty (80) marks divided into two (02) Sections A and B. Attempt the questions contained in these sections according to the detailed instructions given therein.

Section–A

Long Answer Types Questions

Note : Section 'A' contains Five (05) long-answer-type questions of Fifteen (15) marks each. Learners are required to answer any three (03) questions only. **(3×15=45)**

1. Explain RSA algorithm and security features of RSA.

2. Users A and B use the Diffie-Hellman key exchange technique with a common prime q = 71 and a primitive root $\alpha = 7$.

   (a) If user A has private key $X_A = 5$, what is A's public key Y_A?

   (b) If user B has private key $X_B = 12$, what is B's public key Y_B?

   (c) What is the shared secret key ?

3. Describe Elgamal Signature Schedule alongwith their elliptic curve version.

4. Write about :

   (a) GCD Computation

   (b) Blind Signature & Proxy Signature

   (c) Elliptic Curve

   (d) Main in the Middle Attack

5. Answer the following :

   (a) What are the premative operations used in RCS ? (4 marks)

   (b) Show how SHA is more secure than MD556. (3 marks)

(c) Explain public key cryptography and when it is preferred. (8 marks)

Section–B

Short Answer Types Questions

Note : Section 'B' contains Eight (08) short-answer-type questions of Seven (07) marks each. Learners are required to answer any Five (05) questions only. **(5×7=35)**

1. What is Complexity of Computation? Explain about two basic types of complexities.
2. Explain Diffie Hellman Key exchange.
3. Write the differences between MD4 and MD5.
4. What do you understand by Cryptographic hash functions?
5. On the elliptic curve $y^2 = x^3-36x$. Let

   P = (– 3, 9) and Q = (– 2, 8). Find P + Q and 2P.
6. Explain Zero Knowledge Protocol with its properties.
7. Explain Digital Signature & Digital Certificate.

8. What do you understand by Cipher text? Explain the difference between the Block Cipher and Stream Cipher.