B. Sc. (Part-III) Examination, 2016
Mathematics- Fourth Paper (Optional)
(A) Number Theory and Cryptography

Note :- Answer any five questions in all. Question No. 1 is compulsory. Answer one question from each unit. Marks allotted to each question are indicated in the right hand margin.

1. Answer the following : $3.5 \times 10 = 35$
   (a) By using the Euclidean algorithm find the GCD of 32768 and 4096.
   (b) Determine the additive inverse of Matrix A modulo 9
   (c) If $a = 43$, $b = 37$, find $(a \times b) \bmod 7$.
   (d) Encrypt WORK using additive modular arithmetic when the encryption key is 11.
   (e) Decrypt PUKPH which has been encrypted using additive modular arithmetic. The encryption key is 7.
   (f) What do you mean by a Block Cipher? Explain briefly its basic principle of operation.
   (g) Define floor and ceiling function. What are its applications to Number Theory and Cryptography?
   (h) A Hill Cipher machine uses 2×2 matrix K. It gives ciphertext HC for input BA and GT for input ZZ. What is the matrix K?
   (i) Solve the following quadratic congruence :
   $x^2 = 36 \pmod{77}$
   (j) Define : Elliptic Curve, Elliptic Curve Cryptography

Unit-I

2. (a) Discuss and state Fermat's theorem and Euler's theorem for prime numbers. 5+5
   (b) Use Fermat's theorem to compute the following :
   (a) $7^{14} \bmod 13$ (b) $5^{-1} \bmod 23$ **Or**
3. (a) State and explain Chinese Remainder Theorem 5+5
   (b) Discuss the applications of CRT in Cryptography.

Unit-II

4. (i) State and explain : 6+4
   (a) Fermat's Primality Test. (b) Square Root Primality Test.
   (ii) Conduct Square Root Primality Test if $n = 7$ Or
5. Solve the following quadratic congruences, if the solution exists : 5+5
   (i) $x^2 = 3 \pmod{11}$ (ii) $x^2 + 12 \pmod{17}$

6. Write explanatory notes on : 5+5
   (a) Cryptography services and Mechanism
   (b) Random Number Generation Techniques. Or
7. Explain with examples : 5+5
   (a) Pollard's $(p-1)$ method (b) Fermat's Pseudoprimes

Unit-IV

8. (i) Describe the Diffie-Hellman key exchange method with the help of a suitable example. 5+5
   (ii) Compute the half-keys and the shared secret for the Diffie-Hellman parameters

given below :

(a) $p = 23, g = 5, a = 4, b = 3$ (b) $p = 47, g = 5, a = 3, b = 4$ **Or**

9. (i) Describe the RSA cryptosystem algorithm. 5+5

(ii) An RSA cryptosystem has $p = 3$, $q = 11$ and $e = 7$

(a) Find the Decryption key, d.

(b) Encrypt 8.