C 17327

Name..

Reg. No......................................

SECOND SEMESTER M.C.A. DEGREE EXAMINATION, AUGUST 2006

MCA 2K 201—NUMBER THEORY AND CRYPTOGRAPHY

(New Scheme)

Time : Three Hours

Maximum : 100 Marks

Answer any **five** *questions.*
All questions carry equal marks.

1. (a) Define the G.C.D. (Greatest Common Divisor) of two positive numbers. (2 marks)

   (b) Let d = G.C.D. (a, b). Prove that there are integers x and y such that $ax - by = d$. (7 marks)

   (c) Using Extended Euclidean Algorithm, find integers x and y such that $73x + 31y = 1$. (4 marks)

   (d) Define prime numbers. (2 marks)

   (e) Check whether or not the Euler function ϕ is multiplicative. (5 marks)

2. (a) State and prove Fermat's little theorem. Is the converse true ? Why or why not ? (8 marks)

   (b) Solve the congruence $2x + 7y \equiv 5 \pmod{12}$. (2 marks)

   (c) Solve the Diophantine equation $x^2 + y^2 = z^2$, with $0 < z < 30$. (4 marks)

   (d) State and prove Wilson's theorem. Is the converse true ? Prove your assertion. (6 marks)

3. (a) State Chinese Remainder Theorem. What is its relevance ? (4 marks)

   (b) Solve the congruence $x^2 \equiv 186 \pmod{401}$, given that 401 is prime, with 3 as a non-residue. (6 marks)

   (c) Find all those odd primes for which 3 is a quadratic residues. (6 marks)

   (d) Briefly discuss Block Cipher Principles. (4 marks)

4. (a) What is steganography ? Explain. (5 marks)

   (b) Explain briefly classical encryption techniques. (5 marks)

   (c) What do you mean by double encryption is equivalent to single encryption ? Is this true in the case of DES ? (10 marks)

5. (a) Briefly explain Block cipher principles. (4 marks)

   (b) Explain International Data Encryption Algorithm. (10 marks)

   (c) Describe BLOWFISH encryption. (6 marks)

6. (a) Describe in detail, the RSA Algorithm. (6 marks)

   (b) A point P on the elliptic curve is said to be of order r, if r is the smallest + ve integer such that rP = O. Prove that the order of the point P = (2, 3) on $y^2 = x^3 + 1$ is 6. (6 marks)

   (c) Explain the role of Hash function in cryptography. (8 marks)

7. (a) Explain SHA-1 algorithm. (8 marks)

   (b) Write short ..ote on multimedia security. (7 marks)

   (c) What is DSS ? Explain. (5 marks)