MAHATMA GANDHI UNIVERSITY
MCA DEGREE EXAMINATION
MODEL QUESTION PAPER
(2011 Revised Syllabi)
Fifth Semester

MCA 501 COMPUTER SECURITY

Time : Three hours **Maximum : 75 Marks**

Part A

Answer any ten questions.

Each question carries 3 marks.

1. Illustrate with a diagram the model for Network Security.

2. Explain the extended Euclidean algorithm.

3. What is Linear Cryptanalysis?

4. State Fermat's and Euler's Theorems.

5. How does Substitute byte transformation work?

6. With a schematic diagram explain the working of a Public- Key Cryptosystem that provides both Authentication and Secrecy.

7. Describe the model of PKIX.

8. Write notes on VeriSign Certificates.

9. Differentiate between Transport and Tunnel Modes

10. How does the proactive password checker work?

11. List out the different types of Viruses.

12. Highlight the properties of reference monitor.

(10 x 3 = 30 marks)

Part B

All questions carry equal marks.

13 (a) Find the multiplicative inverse of $x^7 +x+1$ mod $x^8 +x^4 +x^3 +x+1$ in GF(2^8).

OR

(b) Using Miller – Rabin – test check whether 2357 is prime or not .

14 (a) Explain AES with a neat sketch.

OR

(b) Describe in detail Hill Cipher with an example.

15 (a) Write notes on RSA.

OR

(b) Compare HMAC and CMAC. Discuss the two algorithms in detail.

16 (a) Write notes on Secure Socket layer & Transport Layer Security.

OR

(b)Discuss about DDoS attacks

17 (a) Write short notes on

(i) Smart Card cryptography
(ii) Biometric authentications

OR

(b) What are Cryptographic Accelerators? What is the role of authentication tokens in Hardware solutions for implementing Cryptography?

(5 X 9 = 45 marks)