MCA.V/12.14.1155 Reg. No. | | | | | | | | |

B

MCA DEGREE V SEMESTER EXAMINATION DECEMBER 2014

CAS 2504 CRYPTOGRAPHY AND NETWORK SECURITY

(Regular and Supplementary)

Time: 3 Hours Maximum Marks: 50

PART A

(Answer *ALL* questions)

(15 x 2 = 30)

I. (a) Define the three security goals.
(b) What is cryptanalysis?
(c) Define greatest common devisor of two integers. Which algorithm can be effectively find the greatest common devisor?

II. (a) What is IDEA? Explain briefly.
(b) What is blowfish?
(c) Explain the term 'One Time pad'.

III. (a) What are the three groups of positive integers? Define each one.
(b) What is factorization? List different methods.
(c) Distinguish between symmetric key and asymmetric key cryptosystems.

IV. (a) Explain hash function.
(b) Compare conventional signature and digital signature.
(c) What is SHA?

V. (a) Write short notes on S/MIME.
(b) What are the different services provided by the SSL protocol?
(c) What is digital water marking?

PART B

(5 x 4 = 20)

VI. Explain different cryptographic attacks.

OR

VII. What is substitution cipher? Explain monoalphabetic ciphers in detail.

VIII. Explain AES in detail.

OR

IX. Explain different block cipher modes of operation.

X. Explain RSA algorithm.

OR

XI. Explain Diffie-Hellman method.

XII. Explain message authentication.

OR

XIII. Explain DSS.

XIV. Explain Keberos Version 4.

OR

XV. Explain Pretty Good privacy.

***