



Printed Pages : 2

CS-023/IT-701

(Following Paper ID and Roll No. to be filled in your Answer Book)

**PAPER ID : 1013**

Roll No.

--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

**B. Tech.****(SEM. VII) EXAMINATION, 2007-08****CRYPTOGRAPHY & NETWORK SECURITY***Time : 3 Hours]**[Total Marks : 100**Note : Attempt all questions.*

1. Answer any **four** of the following: **4×6=24**
- (a) Write the effect of security attacks. What is cryptography ?
  - (b) What is Encryption and decryption ? Write DES for encryption.
  - (c) Describe the substitution and transposition algorithm.
  - (d) Describe the Shanon's theorem of confusion and diffusion.
  - (e) Describe the triple DES and IDEA.
  - (f) Describe the key distribution with example.
2. Answer any **four** of the following : **4×6=24**
- (a) Explain the terms : graph ring and field.
  - (b) Describe the Euclid's algorithm.
  - (c) Discuss the discrete algorithm.
  - (d) Describe with example the RSA algorithm.
  - (e) Describe the Diffe-Hellman key algorithm.
  - (f) Describe the Elliptic curve cryptography.

VK-1013]

1

[Contd...

- (a) Describe the authentication requirement and functions.
- (b) Describe the Hash functions and message authentication codes.
- (c) Discuss the security of Hash function & MACS.
- (d) Describe the MDS message digest algorithm.
- (e) What is Digital signatures ? Describe its authentication protocol.
- (f) Discuss the DS standards and the proof of digital signature algorithm.

4. Answer any **two** of the following :

**2×7=14**

- (a) Describe the functions and features of Kerberos and X.509.
- (b) Discuss the directory authentication service.
- (c) Describe the Pretty Good Privacy and S/MIME algorithms.

5. Answer any **two** of the following :

**2×7=14**

- (a) Describe the architecture and functions of IP.
  - (b) Describe the Secure Electronic Transaction (SET).
  - (c) Describe the effect of virus and related threads.
-