

Registration No. :

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

Total number of printed pages – 2

B. Tech  
PECS 5402

**Seventh Semester (Special) Examination – 2013**

**CRYPTOGRAPHY AND NETWORK SECURITY**

**BRANCH : CSE**

**QUESTION CODE : D 410**

**Full Marks – 70**

**Time : 3 Hours**

*Answer Question No. 1 which is compulsory and any **five** from the rest.  
The figures in the right-hand margin indicate marks.*

1. Answer the following questions : 2×10
- What is the purpose of S boxes in DES ?
  - What is the use of Fermat's Theorem ?
  - Name any two numbers to test prime number
  - Define and Differentiate between Ring and field.
  - What do you mean by stereography ? Explain with an example.
  - Mention four SSL protocols ?
  - What do you mean by Trojan Horses ?
  - Define one way property in hash function with an example.
  - What is discrete logarithm ? How it is helpful in security mechanism ?
  - List two methods used for Asymmetric key ciphers.
2. (a) What are the key principles of security ? Explain with example. 5
- (b) Why some attacks are passive and some are active ? Explain each category of attacks with example. 5



**P.T.O.**

3. (a) Describe Euler's Theorem ? How it is different from Chinese remainder theorem ? 5  
(b) State Euclidean algorithm ? Explain how it is helpful for information security ? 5
4. (a) Differentiate between substitution cipher and rotor cipher. 5  
(b) Given two prime numbers  $P = 17$  and  $Q = 29$  find out  $N$ ,  $E$  and  $D$  in RSA encryption. 5
5. (a) Briefly explain Elliptic curve cryptosystem. Why it is gaining popularity over RSA algorithm ? Explain with an appropriate example. 5  
(b) List and explain the problems with public key exchange in ELGamal cryptosystem. 5
6. (a) What are the advantages of MIME protocol over SMTP ? Discuss the functionality of MIME protocols in detail. 5  
(b) Compare and contrast between Secure Socket Layer and transport Layer Security. 5
7. (a) How IP security and System security are helpful for securing the network ? Explain with an appropriate example. 5  
(b) Explain Diffie-Hellman key exchange principle. Discuss its advantage and disadvantages. 5
8. Write short notes on : 5×2  
(a) Whirlpool  
(b) Malware and its application.

