

AIB
23/11/13 FN

Reg. No. :

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

Question Paper Code : 31513

B.E./B.Tech. DEGREE EXAMINATION, NOVEMBER/DECEMBER 2013.

Seventh Semester

Computer Science and Engineering

IT 2352/IT 62/10144 IT 603/10144 CSE 46 – CRYPTOGRAPHY AND NETWORK SECURITY

(Common to Sixth Semester – Information Technology)

(Regulation 2008/2010)

Time : Three hours

Maximum : 100 marks

Answer ALL questions.

PART A — (10 × 2 = 20 marks)

1. Give an example each for substitution and transposition ciphers.
2. Why modular arithmetic has been used in cryptography?
3. What are the modes of DES?
4. List the uses of RC4.
5. Write any two differences between MD4 and secure hash algorithm.
6. How digital signature is different from conventional? Give any two.
7. Define : SET.
8. What do you mean by PGP?
9. What are the effects of malicious software? Write any two.
10. What is 'Worm'?

PART B — (5 × 16 = 80 marks)

11. (a) (i) What are the different types of attacks? Explain. (8)
(ii) State and explain Chinese remainder theorem with example. (8)

Or

- (b) (i) State Fermat's theorem. (4)
- (ii) Find $3^{21} \bmod 11$ using Fermat's theorem. (6)
- (iii) State Euler's theorem to find gcd with example. (6)

12. (a) Write down the Triple DES algorithm and explain with neat diagram.

Or

- (b) Explain about the RSA algorithm with example as :
 $p = 11, q = 5, e = 3$ and $PT = 9$.

13. (a) (i) Define a hashing function. (2)
- (ii) What are the properties of hashing function in cryptography? (6)
 - (iii) Explain Secure Hashing Algorithm (SHA). (8)

Or

- (b) (i) Illustrate about the Birthday attacks. (8)
- (ii) Explain digital signaturing with ElGamal public key cryptosystem. (8)

14. (a) Write short notes about

- (i) Web security (8)
- (ii) SSL. (8)

Or

(b) Explain about the PKI.

15. (a) Explain about the Security standards.

Or

(b) Write short notes on

- (i) Firewalls
- (ii) Viruses.