Reg. No. : | | | | | | | | | | |

Question Paper Code: 31864

B.E. / B.Tech. DEGREE EXAMINATION, NOV 2016

Sixth Semester

Information Technology

01UIT604 - CRYPTOGRAPHY AND NETWORK SECURITY

(Regulation 2013)

Duration: Three hours Maximum: 100 Marks

Answer ALL Questions

PART A - (10 x 2 = 20 Marks)

1. Write short note on classical crypto systems.
2. State Euler's theorem.
3. What are the two general approaches to attacking a cipher?
4. What is the difference between an unconditionally secure cipher and a computationally secure cipher?
5. What is birthday paradox?
6. What is digital signature?
7. What is SSL?
8. What is public key infrastructure?
9. What is honeypot?
10. State the strategies used in password selection.

PART - B (5 x 16 = 80 Marks)

11. (a) What is modular arithmetic? Explain the properties of modular arithmetic with an example. (16)

Or

(b) Explain Euclidean algorithm with an example. (16)

12. (a) Explain the Feistel cipher structure and Feistel encryption and decryption process. (16)

Or

(b) Explain the differential cryptanalysis principles and linear cryptanalysis principles. (16)

13. (a) Explain how public key cryptosystem helps to ensure authentication and secrecy. (16)

Or

(b) Explain the four possible approaches to attacking RSA algorithm. (16)

14. (a) Explain the X.509 framework, certification structure and authentication process. (16)

Or

(b) Explain how Kerberos helps to authenticate users in open distributed environment. (16)

15. (a) Explain the distributed intrusion detection system with its architectural diagram. (16)

Or

(b) Explain how firewalls are used to protect the network from external attacks. (16)