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

Question Paper Code: 36804

B.E. / B.Tech. DEGREE EXAMINATION, APRIL 2019

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. What is the difference between passive and active attacks?
2. State the condition which makes a group as an abelian.
3. What is an avalanche effect?
4. What is an avalanche effect?
5. State the one-way property.
6. What are the properties a digital signature should have?
7. How is an X.509 certificate revoked?
8. What is dual signature and write its purpose?
9. Differentiate statistical anomaly detection and rule-based intrusion detection.
10. List the types of viruses.

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 in detail about Fermat and Euler's theorem. (16)

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

Or

(b) Write down Triple DES algorithm with neat diagram. (16)

13. (a) How do you use digital signatures to authenticate users? Explain. (16)

Or

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

14. (a) Write short notes on (i) X.509 authentication service (ii) Secure Socket Layer. (16)

Or

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

15. (a) Explain the technical details of firewall and describe any three types of firewalls with examples. (16)

Or

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