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

**Question Paper Code: 36084**

B.E. / B.Tech. DEGREE EXAMINATION, NOV 2017

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. Describe Chinese remainder theorem.
4. What is an avalanche effect?
5. List the characteristics of hash functions.
6. What are the properties a digital signature should have?
7. What are the technical shortcomings of Kerberos version 4?
8. What is dual signature and write its purpose?
9. Can routers and bridges be used as firewalls? How?
10. Differentiate statistical anomaly detection and rule-based intrusion detection.

PART - B (5 x 16 = 80 Marks)

11. (a) What are different types of attacks? Explain. (16)

Or

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

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

Or

(b) Describe the AES algorithm in detail. (16)

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

Or

(b) Describe about RSA algorithm in detail. (16)

14. (a) Explain about IP security architecture in detail. (16)

Or

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

15. (a) List and briefly define four techniques used to avoid guessable passwords. (16)

Or

(b) Explain the Denial of service attacks. What kinds of damages are caused by viruses and worms? (16)

———————