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

Question Paper Code: 36804

B.E. / B.Tech. DEGREE EXAMINATION, NOV 2018

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. Find the GCD (82, 126) using Euclid's algorithm.
2. State Fermat's theorem.
3. Describe Chinese remainder theorem.
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. Can routers and bridges be used as firewalls? How?
10. State the strategies used in password selection.

PART - B (5 x 16 = 80 Marks)

11. (a) (i) What are different types of attacks? Explain. (8)

(ii) Discuss about Monoalphabetic Cipher and Hill Cipher. (8)

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) Describe the AES algorithm in detail. (16)

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

Or

(b) Explain about the Diffie-Hellman key exchange algorithm with its advantages and dis advantages in detail. (16)

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

Or

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

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

Or

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