Printed Pages – 4 Roll No. : ....

328840(28)

B. E. (Eighth Semester) Examination,

April-May 2021

(New Scheme)

(ET & T Engg. Branch)

CRYPTOGRAPHY & SECURE COMMUNICATION

Time Allowed : Three hours

Maximum Marks : 80

Minimum Pass Marks : 28

Note : *Part (a) is compulsory. Attempt any **two** parts from (b), (c) and (d).*

Unit-I

1. (a) Explain Euclidean algorithm. 2

(b) Perform the following operation : 7

(i) Subtract 11 from 7 in Z_{13}.

(ii) Add 17 to 27 in Z_{14}.

(iii) Multiply 123 by -10 in Z_{19}.

(iv) Given $a = 161$ and $b = 28$, find gcd (a, b) and the values of s and t.

(v) Given $a = 0$ and $b = 45$, find gcd (a, b) and the values of s and t.

(c) Perform the following operation : 7

(i) Find the multiplicative inverse of 11 in Z_{26}.

(ii) Find the multiplicative inverse of 23 in Z_{100}.

(iii) Find the inverse of 12 in Z_{26}.

(d) Do the following operation : 7

(i) Is 97 a prime

(ii) What is the value of $\phi(10)$?

(iii) Find the result of 6^{10} mod 11, using Fermat's little theorem.

(iv) Find the result of 6^{24} mod 35, using Euler's theorem.

(v) What are the square roots of 1 mod n if n is 7 (a prime)? Using square root test.

Unit-II

2. (a) Draw block diagram of symmetric and asymmetric encryption method. 2

(b) Explain the rules of Playfair Cipher Encryption and Decryption method. Encrypt the message "Ballon" with the keyword "Monarchy". 7

(c) Explain the operation of DES stream cipher. 7

(d) Explain the operation of Diffie and Hellman key exchange algorithm. 7

Unit-III

3. (a) What is the need of message Authentication? 2

(b) Explain the working of MD-5. 7

(c) Explain the operation of Hash based message authentication codes. (HMAC). 7

(d) Explain the working principle of digital signature algorithm. 7

Unit-IV

4. (a) Why we need Internet Security? 2

(b) What is Virus? What is the ways of virus transmission and types of virus present in networks? 7

(c) Explain the operation of firewall with its advantages and disadvantages. 7

(d) Explain IP security architecture. How authentication helps it? 7

Unit-V

5. (a) What is Web Security? 2

(b) Explain the working of SSL architecture and SSL protocol. 7

(c) Explain the operation of dual signature and how it works. 7

(d) How Secure Electronic Transaction (SET) achieves its objective of confidentiality? 7