USN	1	S	I							

MOBILE PHONES PROHIBITED

7CCI01

Siddaganga Institute of Technology, Tumakuru – 572 103

(An Autonomous Institution affiliated to VTU, Belagavi, Approved by AICTE, New Delhi)

Seventh Semester Bachelor of Engineering Examinations Dec. 2019

Cryptography and Network Security

(Common to CS & IS)

Time: 3 Hours **Max. Marks: 100**

Note : Answer any five questions choosing one full question from each unit.

Unit - I

1 a) Briefly explain active and passive attacks. 08

b) Given the key $\begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix}$ encrypt the message "THURSDAY" by applying Hill Cipher. 08

c) Apply Playfair Cipher technique to find the cipher text for the message "ADVANCED TECHNOLOGY" using key "SIENCE". 04

OR

2 a) What are security services? Briefly explain any 5 security services defined in X.800. 06

b) Apply Vignere Cipher to encrypt the message "PROGRAMMING" using the word "KEY". Highlight the differences between monoalphabetic and polyalphabetic ciphers. 08

c) With a block schematic diagram analyze single round DES encryption/decryption. 06

Unit - II

3 a) Analyze how double DES is susceptible for reduction to a single stage and meet in the middle attacks. 06

b) Explain the working of cipher block chaining mode by highlighting the security issues. 06

c) What are the tests for randomness defined by NIST SP 800-22? Find the period of this random number generator: $5X_{n-1} + 1 \bmod 16$ for $X_0 = 20$ 08

OR

4 a) How triple DES algorithm with two keys is vulnerable to known plaintext attack proposed by Merkle and Hellman? Explain. 07

b) Write Blum Blum Shub (BBS) Generator algorithm. Why BBS is referred as cryptographically secure pseudorandom bit generator? 06

c) Discuss ANSI X9.17 pseudorandom number generator. 07

Unit - III

5 a) State Fermat's theorem. Using Fermat's theorem, find 3^{201} mod 11. 05

b) Write Miller Rabin algorithm to test a number for primality. Apply the algorithm to find whether 343 is prime or composite. 08

c) Write RSA algorithm. Apply the same to perform encryption and decryption of the following: $n = 77$, $e = 13$, $M = 5$. 07

OR

6 a) Consider Diffie Hellman scheme with a common prime $q = 7$ and primitive root $\alpha = 3$. If user A has private key $X_A = 6$ find Y_A. If user B has private key $X_B = 5$ find Y_B. Compute shared key and verify. 08

b) With suitable diagrams show how public key encryption can be used to achieve confidentiality, authentication and both. 07

c) What is Euler's Totient function? Compute $\phi(441)$ and $\phi(14)$ 05

Unit – IV

7 a) Define cryptographic hash function and message digest. List and describe any 6 requirements for a cryptographic hash function. 08

b) Differentiate SHA 256 and SHA 512 based on the following parameters:
i) Message size ii) Block size iii) Word size iv) Message digest size 04

c) Describe message digest generation using SHA 512 with a neat diagram. 08

OR

8 a) Mention any 3 design objectives for HMAC given by RFC 2104. Illustrate and explain overall operation of HMAC with a neat diagram. 10

b) Depict the functions of signing and verification process using Digital Signature algorithm with a neat diagram. 10

Unit – V

9 a) Why do we need IP level security? Explain any 4 important applications of IPSec. 10

b) What is a firewall? Listing its characteristics, explain the function of packet filtering router and its application level gateway. 10

OR

10 a) Draw SSL protocol stack and briefly explain the concept of SSL. 07

b) Give an overview on the spectrum of malicious programs by highlighting the types and roles of viruses in breaching the security. 07

c) Explain the services provided by Pretty Good Privacy (PGP). 06

____