Exam.Code:0923
Sub. Code: 33551

2125

B.E. (Information Technology)

Fifth Semester

PCIT-501: Network Security and Cryptography

Time allowed: 3 Hours | Max. Marks: 50

NOTE: Attempt five questions in all, including Question No. I which is compulsory.

x-x-x

1 a) What is a transposition cipher? Demonstrate with an example.

b) Define Euler's Totient Function φ(n). Compute φ(10).

c) What is Secure Socket Layer (SSL)? Mention any two of its features.

d) Discuss any two major security challenges faced in modern networks.

e) What is the Digital Signature Algorithm (DSA)? Mention one application. 5x2

2 a) Explain the Feistel structure used in DES. Draw and describe all components. 5

b) Differentiate between DES and Triple DES in terms of security. Why was Triple DES developed? 5

3 Explain in detail the process of cryptanalysis of a monoalphabetic substitution cipher using frequency analysis, digram analysis, and trial substitutions. Support your explanation with a worked example. 10

4 Using the Euclidean Algorithm, compute the greatest common divisor (gcd) of the numbers: 10

$$a = 252, b = 198$$

i) Use the Euclidean Algorithm to find gcd (252,198). Show each division step clearly.

ii) Using the Extended Euclidean Algorithm, express the gcd in the form:

$$\gcd(252,198) = 252x + 198y$$

where x and y are integers.

iii) Verify your answer by substituting the values of x and y.

5 a) State the difference between a connection and a session in SSL/TLS? 2.5

b) Explain the working of the Electronic Transaction Protocol (ETP) in secure e-commerce. 2.5

c) We say that SSL/TLS is not really a single protocol, but a stack of protocols. Briefly explain what are the different protocols in the SSL/TLS protocol stack with a suitable diagram. 5

P.T.O.

6 a) In a Diffie–Hellman key exchange system, two users agree on a prime modulus, $p = 23$, and a primitive root, $g = 5$. Alice selects her private key as, $a = 6$, and Bob selects his private key as $b = 15$. 5

i) Compute Alice's public key.

ii) Compute Bob's public key.

iii) Determine the common shared secret key generated by both users.

Show all calculations clearly.

b) In a communication network of n users, each user needs to communicate securely with every other user. If symmetric key cryptography is used, derive a formula for the number of secret keys required, and compute the value forn = 100 users. If public key cryptography is used, derive a formula for the number of public–private key pairs required, and compute the value forn = 100 users. 5

x-x-x