

CBCS SCHEME



USN

--	--	--	--	--	--	--	--	--	--

15CS61

Sixth Semester B.E. Degree Examination, Jan./Feb. 2021

Cryptography, Network Security and Cyber Law

Time: 3 hrs.

Max. Marks: 80

Note: Answer any FIVE full questions, choosing ONE full question from each module.

Module-1

- 1 a. Explain different defence strategies and techniques. (10 Marks)
- b. Explain Extended Euclidean Algorithm. Compute the inverse of 12 modulo 79 using Extended Euclidean Algorithm. (06 Marks)

OR

- 2 a. Explain Hill Cipher polyalphabetic cipher method of plain text. Solve the same for block size of 2, where $K = \begin{bmatrix} 3 & 7 \\ 15 & 12 \end{bmatrix}$. (06 Marks)
- b. With a neat diagram, explain DES construction. (10 Marks)

Module-2

- 3 a. Explain RSA operations and compute the same for $p = 3$ and $q = 11$ as prime numbers. (06 Marks)
- b. Explain with a neat diagram computation of SHA-1 hash construction. (10 Marks)

OR

- 4 a. Explain Diffie-Hellman key exchange protocol for more than two parties. (08 Marks)
- b. Explain EL Gamal encryption for large prime numbers. Solve the same for $p = 131$, $q = 2$, private key = 97, $m = 75$. (08 Marks)

Module-3

- 5 a. With a neat diagram, explain different PKI architectures. (10 Marks)
- b. With a neat scenario, how mutual authentication can be performed using public key encryption. (06 Marks)

OR

- 6 a. Explain Kerberos message sequence with steps involved. (06 Marks)
- b. Explain SSL Handshake Protocol. (10 Marks)

Module-4

- 7 a. Explain Worm characteristics. (10 Marks)
- b. Explain firewall functionality and firewall types. (06 Marks)



15CS61

OR

- 8 a. Explain different technologies for web services. (10 Marks)
b. Explain Security Assertions Markup Language (SAML) with Authentication Statement. (06 Marks)

Module-5

- 9 a. Give the aim and objectives of IT Act, 2000. (06 Marks)
b. Explain briefly different regulations of Certifying Authorities. (10 Marks)

OR

- 10 a. Explain briefly Digital Signature Certificates necessary for an undertaking digitally sign a document. (08 Marks)
b. Explain briefly any eight offences in IT. (08 Marks)

* * * * *

