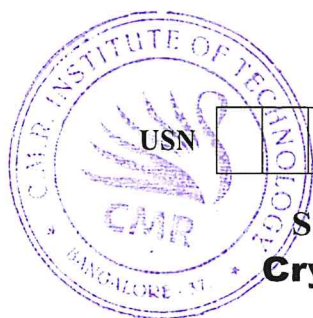


CBCS SCHEME



USN

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

15CS61

Sixth Semester B.E. Degree Examination, Aug./Sept.2020 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 Euclid's algorithm to find gcd of two integers with example. (07 Marks)
- b. Explain the following Algebraic structures with example:
(i) Groups (ii) Rings (iii) Fields (09 Marks)

OR

- 2 a. Explain monoalphabetic and polyalphabetic ciphers with examples. (10 Marks)
- b. Explain the DES construction with a neat diagram. (06 Marks)

Module-2

- 3 a. Explain RSA algorithm with suitable example. (10 Marks)
- b. Explain Weak Collision Resistance and Strong Collision Resistance with examples. (06 Marks)

OR

- 4 a. Explain the following :
(i) Hash-based MAC (ii) Digital Signatures (08 Marks)
- b. Explain Diffie-Hellman key exchange with an example. (08 Marks)

Module-3

- 5 a. Explain the different PKI architectures. (08 Marks)
- b. Explain Mutual authentication using shared secret-based and asymmetric key-based authentication (08 Marks)

OR

- 6 a. How the sequence of messages exchanged between the client, the Kerberos servers and the requested servers? Explain with diagram. (08 Marks)
- b. Explain the main mode and aggressive mode of Internet key exchange protocol. (08 Marks)

Module-4

- 7 a. Explain the authentication and master session key exchange in 802.11i with the help of diagram. (08 Marks)
- b. List out and explain the different worm characteristics. (08 Marks)

OR

- 8 a. Explain the following technologies of web services with suitable examples:
(i) XML (ii) SOAP. (08 Marks)
- b. Explain the different types of Intrusion Detection Systems. (08 Marks)

CMRIT LIBRARY
BANGALORE - 560 037

Important Note : 1. On completing your answers, compulsorily draw diagonal cross lines on the remaining blank pages.
2. Any revealing of identification, appeal to evaluator and/or equations written eg, 42+8 = 50, will be treated as malpractice.

Module-5

- 9 a. What is the Information Technology Act? Discuss the aim and objectives. (06 Marks)
b. Describe the provisions of the IT Act as regards the following :
(i) Legal recognition of electronic records
(ii) Authentication of electronic records.
(iii) Retention of electronic records
(iv) Publications of rules, regulations etc., in the Electronic Gazette. (10 Marks)

OR

- 10 a. Who is a controller? Outline its functions and powers. (08 Marks)
b. Discuss the penalties and adjudication under section 43 of the IT Act 2000 for
(i) damage to a computer, computer system etc.
(ii) failure to furnish information, return, etc. (08 Marks)
