

PC-519
(564) M.Sc. COMPUTER SCIENCE (FOURTH SEMESTER)
Examination JUNE 2020
 Compulsory/Optional
 Group -
 Paper -
SECURITY AND CRYPTOGRAPHY

Time:- Three Hours]

Maximum Marks : 80
 Minimum Passing Marks: 29

नोट : दोनों खण्डों से निर्देशानुसार उत्तर दीजिए। प्रश्नों के अंक उनके दाहिनी ओर अंकित हैं।

Note: Answer From Both the Section as Directed. The Figures in the right-hand margin indicate marks.

Note:- Answer for both the sections as directed. The figures in the right - hand margin indicate marks.

Section -A

1. Answer the following multiple choice type questions: - **1X10 = 10**
 - (a) DES stands for
 - (i) Data encryption standard
 - (ii) Data encryption subscription
 - (iii) Data encryption solution
 - (iv) Data encryption slots.
 - (b) An ----- along with a key is used in the encryption and decryption
 - (i) Data
 - (ii) Cryptography algorithm
 - (iii) Decryption algorithm
 - (iv) Plain text algorithm
 - (c) The ----- is encrypted text:-
 - (i) Cipher text
 - (ii) Secret text
 - (iii) Cipher script
 - (iv) Secret script
 - (d) Which of the following is not used for symmetric encryption.
 - (i) RSA
 - (ii) DES
 - (iii) SHA1
 - (iv) RC4
 - (e) Hash collision means:-
 - (i) Two keys for one message
 - (ii) One key for two message
 - (iii) Two different keys for different message
 - (iv) always the same key
 - (f) What is the length of key (without padding) in DES?
 - (i) 64 bits
 - (ii) 128 bits
 - (iii) 72 bits
 - (iv) 56 bits
 - (g) the advanced encryption standard was designed by.
 - (i) National Institute of standards & technology
 - (ii) IBM
 - (iii) HP
 - (iv) Intel
 - (h) The ----- method provides a one - time session key for two parties.
 - (i) Diffie - Hellman
 - (ii) RSA
 - (iii) DES
 - (iv) AES
 - (i) A digital signature needs a
 - (i) Private - key system
 - (ii) Shared - key system
 - (iii) public - key system
 - (iv) All of them
 - (j) Which are the most frequently found.
 - (i) e, a
 - (ii) e, o
 - (iii) e, t
 - (iv) e, i

2. Answer the following short answer type questions:- **2x5 = 10**
 - (a) What do you understand by DNS?
 - (b) What is cryptograph.
 - (c) Specify the components of encryption algorithm.
 - (d) Define confidentiality & authentication.
 - (e) Differentiate symmetric & asymmetric encryption.

Section -B

3. Answer the following long - answer type questions:- **12x5 = 60**
 - Draw the general structure of DES & Explain the encryption Decryption process?

Or

 - Explain the key generation process in DES algorithm?
4. Explain the technical details of firewall and describe any three types of firewall?

Or

 - Explain DNS and its security?
5. Explain about RSA with one suitable example?

Or

 - Explain digital signatures and authentication protocol?
6. Define hash function? What are the properties of hash function in cryptography? Explain secure hashing algorithm.

OR

 - Write short notes on:-
 - (i) Web security
 - (ii) SSL

UNIT - V
7. Write short notes on:-
 - (i) WAP
 - (ii) MIME

OR

 - Explain the types of intrusion detection system.