SB-18

Total No. of Pages : 4

Seat No.	

T.Y. B.Tech. (Computer Science and Engineering) (Part - II) (CBCS) (Semester - V) Examination, January - 2023

INFORMATION SECURITY

Sub. Code : 80798

Day and Date : Friday, 13 - 01 - 2023 **Total Marks : 70**

Time : 10.30 a.m. to 1.00 p.m.

Instructions :
1) **All Questions are compulsory.**
2) **Assume suitable data wherever necessary.**
3) **Figures to the right indicate full marks.**

Q1) Solve MCQs (1Mark Each) **[14]**

a) Protection of all user data in single data block is done by which service.

i) Repudiation

ii) Integrity

iii) Connectionless confidentiality

iv) Both (i) & (ii)

b) The Vernam Cipher is also called as _____

i) Polyalphabetic ii) Caesar

iii) Hill cipher iv) One time Pad

c) In pervasive mechanism _____ is refered to data collected and potentially used to facilitate a security audit.

i) Security recovery ii) Event detection

iii) Security audit trail iv) All the above

d) MAC stands for _____

i) Message authentication code

ii) Message authentication connection

iii) Message authentication control

iv) Message authentication cipher

P.T.O.

e) If any participant can send his or her public key to any other participant or broadcast the key to the community at large then this technique of key distribution is called as _____.

i) Publicly available directory ii) Public announcement

iii) Public-key authority iv) Public-key certificates

f) Hash function is a _____

i) A function that maps a message of any length into a variable-length hash value, which serves as the authenticator

ii) A function that maps a message of any length into a fixed-length hash value, which serves as the authenticator

iii) Both (i) & (ii)

iv) None of the above

g) Digital signature provides _____.

i) Authentication ii) Nonrepudiation

iii) Both (i) & (ii) iv) Neither (i) & (ii)

h) In Kerberos, AS referred as _____.

i) Authorization Service ii) Authentication Service

iii) Authentication Server iv) None of the above

i) Which e-mail standard relies on "Web of Trust"?

i) Pretty Good Privacy (PGP)

ii) Privacy Enhanced Mail (PEM)

iii) MIME Object Security Services (MOSS)

iv) Secure Multipurpose Internet Mail Extensions (S/MIME)

j) _____ uniquely identifies the MIME entities uniquely with reference to multiple contexts.

i) Content description ii) Content - id

iii) Content type iv) Content transfer encoding

k) At the lower layer of SSL, a protocol for transferring data using a variety of predefined cipher and authentication combinations called the _____

i) SSL handshake protocol

ii) SSL authentication protocol

iii) SSL record protocol

iv) SSL cipher protocol

l) Which of the following is/are the types of firewall?

i) Packet Filtering router ii) Application level gateway

iii) Circuit level gateway iv) All of the above

m) When people send you phone emails, pop-up messages, social media messages, texts, calls, or links to fake websites in order to hook you into giving out your personal and financial information.

i) Plagiarizing ii) Skimming

iii) Phishing iv) Identity Theft

n) What is one of the most common and simplest attacks on a system?

i) Denial of service

ii) Buffer overflow

iii) Session hacking

iv) Password cracking

Q2) Solve any 2 of the following (7 Marks Each) **[14]**

a) Explain different types of attacks with example?

b) Write and explain Diffie-Hellman Key exchange algorithm?

c) Explain Difference between Kerberos 4 and kerberos 5?

Q3) Solve any 2 of the following (7 Marks Each) **[14]**

a) Explain Transposition Techniques with Examples?

b) What is message authentication code? What are basics of MAC?

c) Explain X.509 certification formats?

Q4) Solve any 2 of the following (7 Marks Each) **[14]**

a) Explain 5 services of PGP?

b) Explain SSL Handshake Protocol?

c) Explain Pharming Attacks?

Q5) Solve any 2 of the following (7 Marks Each) **[14]**

a) Explain antireplay service?

b) What is SET? Explain SET Participants and Requirements?

c) Explain DOS and DDOS attack?