Seat No. : _____

AL-103

April-2022

B.Com., Sem.-VI

CE-303 (D) : Computer Application

(Information Security)

Time : 2 Hours] **[Max. Marks : 25**

સૂચનાઓ : (1) **તમામ** પ્રશ્નો વિભાગ-**I**માં સમાન ગુણ ધરાવે છે.

(2) વિભાગ-**I**માંથી કોઈપણ **બે** પ્રશ્નોનો પ્રયાસ કરો.

(3) વિભાગ-**II**માં પ્રશ્ન **5** ફરજીયાત છે.

વિભાગ – I

1. (A) માહિતી સુરક્ષાનો (Information security) અર્થ શું છે ? માહિતીની બધી જ મહત્ત્વની લાક્ષણિકતાઓ સમજાવો. **5**

(B) સંસ્થામાં વિવિધ સુરક્ષા વ્યાવસાયિકોની (security professionals) ભૂમિકા સમજાવો. **5**

2. (A) નીચેના શબ્દો સમજાવો : **5**

(1) તોડફોડ (Sabotage)

(2) જાસૂસી (Espionage)

(3) પોલિમોર્ફિક થ્રેટ (Polymorphic Threat)

(4) ટ્રોજન હોર્સ (Trojan Horse)

(5) વાયરસ (Virus)

(B) માહિતી સુરક્ષા માટેની તમામ જોખમ નિયંત્રણ વ્યૂહરચનાઓ (Risk Control Strategies) સમજાવો. **5**

3. (A) એક્સેસ કન્ટ્રોલ મિકેનિઝમ સાથે સંબંધિત નીચેની પરિભાષાઓ સમજાવો : **5**

(i) ઓળખ (Identification)

(ii) પ્રમાણભૂતતા (Authentication)

(iii) અધિકૃતતા (Authorization)

(iv) જવાબદારી (Accountability)

(v) ફરજિયાત ઍક્સેસ કન્ટ્રોલ (Mandatory Access Control)

(B) નોંધ લખો : **5**

(1) વી પી એન

(2) ફાયરવોલ

4. (A) ઉદાહરણ આપીને "અવેજી (Substitution)" અને "એક્સક્લુઝિવ ઓર" સાઈફર પદ્ધતિ સમજાવો. **5**

(B) "સિમેટ્રિક" અને "એસિમેટ્રિક" એનક્રિપ્શન સમજાવો. **5**

વિભાગ – II

5. ખાલી જગ્યા ભરો. (કોઈપણ **પાંચ**નો પ્રયત્ન કરો.) **5**

1. _____ એ સિસ્ટમમાં નબળાઈઓ અથવા દોષ છે જે તેને હુમલો કરવા અથવા નુકસાન માટે ખોલે છે.

(a) નબળાઈ (Vulnerability) (b) ધમકી (Threat)

(c) હુમલો (Attack) (d) સંપત્તિ (Asset)

2. _____ ડેટા માલિકો સાથે સીધું જ કામ કરે છે. તેઓ માહિતીના સંગ્રહ, જાળવણી અને રક્ષણ માટે જવાબદાર હોય છે.

(a) ડેટા કસ્ટોડિયન્સ (b) ડેટા ઓનર્સ

(c) ડેટા વપરાશકર્તાઓ (d) આ બધા

3. _____ એ એક પ્રોગ્રામ અથવા ઉપકરણ છે જે નેટવર્ક પર મુસાફરી કરતા ડેટાનું નિરીક્ષણ કરી શકે છે.

(a) સ્નિફર (b) ચોર

(c) લૂંટારુ (d) આ બધા

4. _____ એક જાણીતી ઈલેક્ટ્રોનિક અને માનવીય પ્રવૃત્તિઓ છે જે માહિતીની ગોપનીયતાનો ભંગ કરી શકે છે.

(a) એસ્પીઓનેજ (Espionage)

(b) ટ્રેસપાસ (Trespass)

(c) ટ્રેસપાસ અને એસ્પીઓનેજ બંને (Trespass and espionage both)

(d) આમાંથી એકપણ નહીં

5. મેઈલ બોમ્બમાં એક હુમલાખોર મોટી માત્રામાં ઈ-મેઈલને ટાર્ગેટ સુધી પહોંચાડે છે.

(a) સાચું (b) ખોટું

6. _____ હુમલામાં હુમલાખોર મોટી સંખ્યામાં કનેક્શન કે માહિતીની વિનંતીઓ લક્ષ્યને મોકલે છે.

(a) ડીનાયલ ઑફ સર્વિસ (b) વાયરસ

(c) વોર્મ (d) આમાંથી એકપણ નહીં

7. RADIUSનું પૂર્ણ સ્વરૂપ _____

(a) રિમોટ ઓથોરાઈઝેશન ડાયલ-ઈન યુઝર સર્વિસ

(b) રિમોટ ઓથેન્ટિકેશન ડાયલ-ઈન યુઝર સર્વિસ

(c) રેન્ડમ ઓથેન્ટિકેશન ડાયલ-ઈન યુઝર સર્વિસ

(d) રેન્ડમ ઓથોરાઈઝેશન ડાયલ-ઈન યુઝર સર્વિસ

8. _____ એ એનકોડ કરેલો સંદેશો છે જે એનક્રિપ્શનમાંથી પરિણમી રહ્યો છે.

(a) સાયફર લખાણ (b) ડીસાયફર

(c) એનસાયફર (d) આમાંથી એકપણ નહીં

9. ડિજિટલ હસ્તાક્ષરો એ ડિજિટલ કોડ છે, જે ઈલેક્ટ્રોનિકલી ટ્રાન્સમિટેડ ડોક્યુમેન્ટ સાથે જોડાયેલો હોય છે, જેથી તેની સામગ્રી અને મોકલનારની ઓળખ ચકાસી શકાય.

(a) સાચું (b) ખોટું

10. HTTPનું સંપૂર્ણ ફોર્મ _____ છે.

(a) હાઈપર ટેક્સ્ટ ટ્રાન્સફર પ્રોટોકોલ (b) હાઈપર ટેક્સ્ટ ટ્રાન્સફર પ્રોસીજર

(c) હાઈપર ટેક્સ્ટ ટ્રાન્સફર પ્રોગ્રામ (d) હાઈપર ટેક્સ્ટ ટ્રાન્સપોર્ટ પ્રોટોકોલ

Seat No. : _____

AL-103

April-2022

B.Com., Sem.-VI

CE-303 (D) : Computer Application

(Information Security)

Time : 2 Hours] **[Max. Marks : 25**

Instructions : (1) **All** questions carry equal marks in Section-**I**.

(2) Attempt any **two** questions in Section-**I**.

(3) Question **5** in Section-**II** is Compulsory.

SECTION – I

1. (A) What do you mean by Information security ? Explain all important Characteristics of Information. **5**

   (B) Explain role of different security professionals in an organization. **5**

2. (A) Explain following terms : **5**

   (1) Sabotage

   (2) Espionage

   (3) Polymorphic Threat

   (4) Trojan Horse

   (5) Virus

   (B) Explain all Risk Control Strategies for Information Security. **5**

3. (A) Explain following terminologies related to access control mechanism : **5**

   (i) Identification

   (ii) Authentication

   (iii) Authorization

   (iv) Accountability

   (v) Mandatory Access Control

   (B) Write note : **5**

   (1) VPN

   (2) Firewall

4. (A) Explain "Substitution" and "Exclusive OR" cipher method giving example. **5**

(B) Explain "Symmetric" and "Asymmetric" Encryption. **5**

SECTION – II

5. Fill in the blanks. (Attempt any **five**) **5**

1. _____ is weaknesses or fault in a system that opens it to attack or damage.

   (a) Vulnerability (b) Threat

   (c) Attack (d) Asset

2. _____ work directly with data owners. They are responsible for the storage, maintenance, and protection of the information.

   (a) Data custodians (b) Data Owners

   (c) Data Users (d) All of these

3. A _____ is a program or device that can monitor data travelling over a network.

   (a) Sniffer (b) Thief

   (c) Robber (d) All of these

4. _____ is a well-known electronic and human activities that can breach the confidentiality of information.

   (a) Espionage

   (b) Trespass

   (c) Trespass and espionage both

   (d) None of these

5. In mail bomb, an attacker routes large quantities of e-mail to the target.

   (a) True

   (b) False

6. In a _____ attack, the attacker sends a large number of connection or information requests to a target.

(a) Denial of service (b) Virus

(c) Worm (d) None of these

7. Full form of RADIUS is

(a) Remote Authorization Dial-In User Service

(b) Remote Authentication Dial-In User Service

(c) Random Authentication Dial-In User Service

(d) Random Authorization Dial-In User Service

8. _____ is the encoded message resulting from an encryption.

(a) Cipher text (b) Decipher

(c) Encipher (d) None of these

9. Digital signatures is a digital code, which is attached to an electronically transmitted document to verify its contents and the sender's identity.

(a) True

(b) False

10. Full form of HTTP is _____

(a) Hyper Text Transfer Protocol

(b) Hyper Text Transfer Procedure

(c) Hyper Text Transfer Program

(d) Hyper Text Transport Protocol