Enrollment No: _____ Exam Seat No: _____

C. U. SHAH UNIVERSITY

Winter Examination-2021

Subject Name: Computer Security

Subject Code: 2TE05CSE1 **Branch: Diploma (CE)**

Semester: 5 **Date: 15/12/2021** **Time: 11:00 To 02:00** **Marks: 70**

Instructions:

(1) Use of Programmable calculator & any other electronic instrument is prohibited.
(2) Instructions written on main answer book are strictly to be obeyed.
(3) Draw neat diagrams and figures (if necessary) at right places.
(4) Assume suitable data if needed.

Q-1 **Attempt the following questions. (1 mark for each question)** **(14)**

a) The process of converting plain text into cipher text is known as _____
(A) Encryption (B) Decryption (C) Cryptography (D) None

b) The process of converting cipher text into plain text is known as _____
(A) Encryption (B) Decryption (C) Cryptography (D) None

c) Which of the following is type of intruder?
(A) Masquerader (B) Misfeasor (C) Clandestine user (D) All

d) Which of the following is rule based intrusion detection technique?
(A) Anomaly Detection (B) Penetration Identification
(C) Both A & B (D) None

e) Which of the following is initial phase of virus?
(A) Execution (B) Triggering (C) Propagation (D) Dormant

f) Which of the following type of Firewall is also known as proxy server?
(A) Circuit level gateway (B) Application level gateway
(C) Packet filtering router (D) None

g) In which type of attack alteration of data does not take place?
(A) Active attack (B) Passive attack (C) Replay (D) None

h) In Playfair Cipher Substitution Technique _____ key matrix is used.
(A) 3 × 3 (B) 4 × 4 (C) 5 × 4 (D) 5 × 5

i) $C = PK \bmod 26$ and $P = CK^{-1} \bmod 26$ formulas are used for which substitution technique?
(A)Monoalphabetic Cipher (B) Hill Cipher
(C) Vigenere Cipher (D) Vernam Cipher

j) _____ is the original message before transformation.
(A) cipher text (B) plain text (C) secret text (D) None

k) _____ is the message after transformation.

(A) cipher text (B) plain text (C) secret text (D) None

l) A _____ method replaces one character with other character.
(A) substitution (B) transposition (C) either A or B (D) None

m) Which of the following techniques include the involvement of matrix operations in their algorithms of encryption and decryption?
(A) Hill Cipher (B) Playfair (C) either A or B (D) None

n) If sender and receiver use same key, the system is referred as_____ encryption.
(A) Asymmetric (B) Symmetric (C) Public Key (D) None

Attempt any four questions from Q-2 to Q-8

Q-2		**Attempt all questions**	**(14)**
	a)	Explain Symmetric Encryption Model with diagram.	**(07)**
	b)	Explain various types of active attacks in detail.	**(07)**
Q-3		**Attempt all questions**	**(14)**
	a)	Carry out Encryption and Decryption (using formula) of following using Caesar Cipher Substitution method. **Plain Text: TOMORROW Key: 5**	**(07)**
	b)	Write down steps for Playfair Substitution Method. Solve the following using Playfair Substitution Method. **Plain Text: DECEMBER Key: WINTER**	**(07)**
Q-4		**Attempt all questions**	**(14)**
	a)	What is virus? Explain various types of virus in detail.	**(07)**
	b)	Which points should be kept in mind while doing online transaction?	**(07)**
Q-5		**Attempt all questions**	**(14)**
	a)	Draw and explain Sniffing and Spoofing in detail.	**(07)**
	b)	Explain DOS and DDos in detail.	**(07)**
Q-6		**Attempt all questions**	**(14)**
	a)	Write a note on Digital Signature.	**(07)**
	b)	Which points should be kept in mind while selecting a password?	**(07)**
Q-7		**Attempt all questions**	**(14)**
	a)	Write a note on Kerberos.	**(07)**
	b)	Explain Man in Middle Attack in detail.	**(07)**
Q-8		**Attempt all questions**	**(14)**
	a)	Write a note on Secured Electronic Transaction.	**(07)**
	b)	Explain Handshake Protocol in detail.	**(07)**

Q-1 **Attempt the following questions. (1 mark for each question)** **(14)**

a) સાદા ટેક્સ્ટને સાઇફર ટેક્સ્ટમાં રૂપાંતરિત કરવાની પ્રક્રિયા _____ તરીકે ઓળખાય છે.

(A) એન્ક્રિપ્શન (B) ડિક્રિપ્શન (C) ક્રિપ્ટોગ્રાફી (D) કોઈ નહીં

b) સાઇફર ટેક્સ્ટને સાદા ટેક્સ્ટમાં રૂપાંતરિત કરવાની પ્રક્રિયા _____ તરીકે ઓળખાય છે.

(A) એન્ક્રિપ્શન (B) ડિક્રિપ્શન (C) ક્રિપ્ટોગ્રાફી (D) કોઈ નહીં

c) નીચેનામાંથી કયો ઈન્ટ્રુડરનો પ્રકાર છે?

(A) માસ્કરેડર (B) મિસફિસર (C) કલેન્ડએસ્ટીન ઉઝર (D) બધા

d) નીચેનામાંથી કઈ નિયમ આધારિત ઈન્ટ્રુઝન ડિટેક્શન ટેકનિક છે?

(A) અનોમલી ડિટેકશન (B) પેનિટ્રેશન ડિટેકશન (C) બંને A અને B

(D) કોઈ નહીં

e) નીચેનામાંથી કયો વાયરસનો પ્રારંભિક તબક્કો છે?

(A) એક્ઝિક્યુશન (B) ટ્રિગરિંગ (C) પ્રોપોગેશન (D) ડોરમેન્ટ

f) નીચેનામાંથી કયા પ્રકારની ફાયરવોલને પ્રોક્સી સર્વર તરીકે પણ ઓળખવામાં આવે છે?

(A) સર્કિટ લેવલ ગેટવે (B) એપ્લિકેશન લેવલ ગેટવે

(C) પેકેટ ફિલ્ટરિંગ રાઉટર (D) કોઈ નહીં

g) કયા પ્રકારના હુમલામાં ડેટામાં ફેરફાર થતો નથી?

(A) એકટીવ એટેક (B) પેસીવ એટેક (C) રીપ્લે (D) કોઈ નહીં

h) પ્લેફેર સાઇફર સબસ્ટીટ્યુશન ટેકનીકમાં _____ કી મેટ્રિક્સનો ઉપયોગ થાય છે.

(A) 3×3 (B) 4×4 (C) 5×4 (D) 5×5

i) $C = PK$ મોડ 26 અને $P = CK^{-1}$ મોડ 26 ફોર્મ્યુલાનો ઉપયોગ કઈ અવેજીની તકનીક માટે થાય છે?

(A) મોનોઆલ્ફાબેટિક સાઇફર (B) હિલ સાઇફર

(C) વિજેનેર સાઇફર (D) વર્નામ સાઇફર

j) _____ એ રૂપાંતર પહેલાનો મૂળ સંદેશ છે.

(A) સાઇફર ટેક્સ્ટ (B) સાદો ટેક્સ્ટ (C) ગુપ્ત ટેક્સ્ટ (D) કોઈ નહીં

k) _____ એ પરિવર્તન પછીનો સંદેશ છે.

(A) સાઇફર ટેક્સ્ટ (B) સાદો ટેક્સ્ટ (C) ગુપ્ત ટેક્સ્ટ (D) કોઈ નહીં

l) _____ પદ્ધતિ એક અક્ષરને અન્ય અક્ષર સાથે બદલે છે.

(A) સબસ્ટિટ્યૂશન (B) ટ્રાન્સપોઝિશન (C) A અથવા B (D) કોઈ નહીં

m) નીચેનામાંથી કઈ તકનીકમાં એન્ક્રિપ્શન અને ડિક્રિપ્શનના તેમના અલ્ગોરિધમ્સમાં મેટ્રિક્સ કામગીરીની સંડોવણીનો સમાવેશ થાય છે?

(A) હિલ સાઇફર (B) પ્લેફેર (C) ક્યાં તો A અથવા B (D) કોઈ નહીં

n) જો સેન્ડર અને રિસિવર સમાન કીનો ઉપયોગ કરે છે, તો સિસ્ટમને _____ એન્ક્રિપ્શન તરીકે ઓળખવામાં આવે છે.

(A) એસિમેટ્રિક (B) સિમેટ્રિક (C) પબ્લિક કી (D) કોઈ નહીં

Attempt any four questions from Q-2 to Q-8

Q-2		**Attempt all questions**	**(14)**
	a)	આકૃતિ સાથે સિમેટ્રિક એન્ક્રિપ્શન મોડેલ સમજાવો.	**(07)**
	b)	વિવિધ પ્રકારના એકટીવ એટેકનું વિગતવાર વર્ણન કરો.	**(07)**
Q-3		**Attempt all questions**	**(14)**
	a)	સીઝર સાઇફર સબસ્ટિટ્યૂશન પદ્ધતિનો ઉપયોગ કરીને નીચેનાનું એન્ક્રિપ્શન અને ડિક્રિપ્શન (સૂત્રનો ઉપયોગ કરીને) કરો. Plain Text: TOMORROW Key: 5	**(07)**
	b)	પ્લેફેર સબસ્ટિટ્યૂશન પદ્ધતિ માટે સ્ટેપ્સ લખો. પ્લેફેયર સબસ્ટિટ્યૂશન પદ્ધતિનો ઉપયોગ કરીને નીચે નું સોલ્વ કરો. Plain Text: DECEMBER Key: WINTER	**(07)**
Q-4		**Attempt all questions**	**(14)**
	a)	વાયરસ શું છે? વિવિધ પ્રકારના વાઈરસને વિગતવાર સમજાવો.	**(07)**
	b)	ઓનલાઈન ટ્રાન્ઝેક્શન કરતી વખતે કયા મુદ્દા ધ્યાનમાં રાખવા જોઈએ?	**(07)**
Q-5		**Attempt all questions**	**(14)**
	a)	સ્નિફિંગ અને સ્પુફિંગને વિગતવાર દોરો અને સમજાવો.	**(07)**
	b)	DOS અને DDos ને વિગતવાર સમજાવો.	**(07)**
Q-6		**Attempt all questions**	**(14)**
	a)	ડિજિટલ સિગ્નેચર પર નોંધ લખો.	**(07)**
	b)	પાસવર્ડ પસંદ કરતી વખતે કયા મુદ્દા ધ્યાનમાં રાખવા જોઈએ?	**(07)**
Q-7		**Attempt all questions**	**(14)**
	a)	Kerberos પર નોંધ લખો.	**(07)**
	b)	મેન ઇન મિડલ એટેકને વિગતવાર સમજાવો.	**(07)**
Q-8		**Attempt all questions**	**(14)**
	a)	સિકયોર ઇલેક્ટ્રોનિક ટ્રાન્ઝેક્શન પર નોંધ લખો.	**(07)**
	b)	હેન્ડશેક પ્રોટોકોલ વિગતવાર સમજાવો.	**(07)**