Enrollment No: _____ Exam Seat No:_____

C.U.SHAH UNIVERSITY

Summer Examination-2018

Subject Name : Computer Security

Subject Code : 2TE05CSE1 Branch: Diploma (CE)

Semester: 5 Date: 19/03/2018 Time: 10:30 To 01:30 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: (14)

a) Release of Message Content is a _____Attack
A) Active Attack B) Passive Attack C) Both A and B D) None of these

b) Who is the founder of Caesar cipher?
A) Bom Cipher B) D.B.Cipher C) Julius Cipher D) Julius Caesar

c) Full Form of SSL_____
A) Secure Socket Layer B) Secure Security Layer
C) Secure Set Layer D) None of These

d) Caesar Cipher is an example of
A) Poly-alphabetic Cipher B) Mono-alphabetic Cipher
C) Multi-alphabetic Cipher D) Bi-alphabetic Cipher

e) An asymmetric-key (or public-key) cipher uses
A) 1 Key B) 2 Key C) 3 Key D) 4 Key

f) What is the Full Form of TLS?
A) Transport Layer Security B) Transport Layer Service
C) Transport Layer Layer D) None of these

g) Masquerade is an _____ Attack
A) Active Attack B) Passive Attack C) Both A and B D) None of these

h) Authentication is
A) Verification of User Identification B) Verification of Data
C) Both A and B D) None of these

i) CA Stands for
A) Certified Auditing B) Certification Authorities
C) Cyber Abuses D) Certificate Authentication

j) The Original Message is called
A) Plaintext B) Cipher text C) Simple text D) Encryption

k) Which technique is used at a time two letter encrypted?
A) Onetime Pad B) Play fair C) Monoalaphabetic D) Polyalphabetic

l) Substution box provides
A) Diffusion B) Confusion C) Both A and B D) None of These

m) Which attacks are called as masquerade attacks?
A) Interception B) Interruption C) modification D) fabrication

n) User A if wanting to send an authenticated message to user B , it would encrypt the message with A's _private key
A) Public Key B) Private Key C) both key D) third party key

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

Q-2 **Attempt all questions**

a) Explain Playfair with examples. **(07)**
b) Explain OSI Security Architecture. **(07)**

Q-3 **Attempt all questions**

a) Write a note on "VPN". Also explain E - Mail Security. **(07)**
b) What is a Firewall? Explain different types of Firewall. **(07)**

Q-4 **Attempt all questions**

a) Define Virus. Explain different types of Virus. **(07)**
b) Explain Transposition cipher with examples **(07)**

Q-5 **Attempt all questions**

a) Explain Symmetric Cipher Model with suitable diagram. **(07)**
b) Explain Phishing Attack in respect to real time scenario. **(07)**

Q-6 **Attempt all questions**

a) Explain SSL Architecture with suitable diagram **(07)**
b) Write a note on "Secure Electronic Transaction". **(07)**

Q-7 **Attempt all questions**

a) Define Digital Signature. Explain Digital Signature Algorithm. **(07)**
b) Discuss Dos and DDos Attack in detail with appropriate example. **(07)**

Q-8 **Attempt all questions**

a) Explain Physical Security Component with examples. **(07)**
b) Compare Centralized and decentralized infrastructure. **(07)**

Q -1 નીચેના પ્રશ્નોનો પ્રયાસ કરો: **(14)**

a) સંદેશ સામગ્રીની પ્રકાશન એ _____ એટેક્ટ છે
એ) સક્રિય એટેક બી) નિષ્ક્રીય એટેક સી) બંને એ અને બી ડી) આમાંથી કોઈ નહીં

b) સીઝર સાઈફરના સ્થાપક કોણ છે?
એ) બોમ સાઈફર બી) ડી.બી.સિફર સી) જુલિયસ સાઈફર ડી) જુલિયસ સીઝર

c) **SSL**_____ નું પૂર્ણ સ્વરૂપ
એ) સિક્યોર સોકેટ લેયર **B)** સિક્યોર સિક્યોરિટી લેયર સી) સિક્યોર સેટ લેયર ડી) આમાંથી કોઈ નહીં

d) સીઝર સાઈફરનું ઉદાહરણ છે
એ) પોલી-આલ્ફાબેટીક સાઈફર બી) મોનો-આલ્ફાબેટીક સાઈફર
સી) મલ્ટી-આલ્ફાબેટીક સાઈફર ડી) બાય-આલ્ફાબેટીક સાઈફર

e) **Asymmetric** સાઈફર કેટલી **Key** ઉપયોગ કરે છે
એ) 1 કી બી) 2 કી સી) 3 કી ડી) 4 કી

f) **TLS** નું પુરુ નામ શું છે?
A) ટ્રાન્સપોર્ટ લેયર સિક્યોરિટી **B)** ટ્રાન્સપોર્ટ લેયર સર્વિસ
C) ટ્રાન્સપોર્ટ લેયર લેયર ડી) આમાંથી કોઈ નહીં

g) માસ્કરેડ એ _____ એટેક છે
એ) સક્રિય એટેક બી) નિષ્ક્રીય એટેચમેન્ટ **C)** બંને એ અને બી ડી) આમાંથી કોઈ નહીં

h) Authentication
એ) યુઝર આઈડેન્ટિફિકેશનની ચકાસણી. બી) ડેટાની ચકાસણી
સી) એ અને બી બંને ડી) આમાંથી કોઈ નહીં

i) **CA** માટે સ્ટેન્ડ્સ
એ) સર્ટિફાઈડ ઓડિટિંગ બી) સર્ટિફિકેશન ઓથોરિટીઝ સી) સાયબર અબ્યુઝ ડી) પ્રમાણપત્ર પ્રમાણીકરણ

j) કોને મૂળ સંદેશ કહેવામાં આવે છે
A) પ્લેઈનટેક્સ્ટ B) સાઈફર ટેક્સ્ટ **C)** સાદી ટેક્સ્ટ ડી) એન્ક્રિપ્શન

k) કયા ટેક્નિકનો ઉપયોગ એક સમયે બે અક્ષર એનક્રિપ્ટ થયેલ છે?
A) વન ઈમ પેડ B) પ્લે સીઝન) મોનોઅલફાબેટિક ડી) પોલિઆલ્ફાબેટિક

l) સબસ્ટ્યુશન બોક્સ શું પ્રદાન કરે છે
A) પ્રસરણ બી) મૂંઝવણ **C)** એ અને બી બંને ડી) આમાંથી કોઈ નહીં

m) કયા હુમલાઓને માસ્કરેડ હુમલા કહેવાય છે?
એ) અડચણ બી) વિક્ષેપ સી) ફેરફાર ડી) ફેબ્રિકેશન

n) યુઝર એ, જો યુઝર બીને અધિકૃત સંદેશ મોકલવા ઈચ્છતા હોય, તો તે એની ખાનગી ચોપડે સંદેશને એન્ક્રિપ્ટ કરશે
એ) જાહેર કી B) ખાનગી કી **C)** બન્ને કી **D)** તૃતીય પક્ષ કી

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

Q-2 **Attempt all questions**

a) પ્લેફેર ને ઉદાહરણો સાથે સમજાવો **(07)**

b) **OSI Security** આર્કિટેક્ચર સમજાવો. **(07)**

Q-3 **Attempt all questions**

a) **"VPN"** પર ટૂંકું નોંધ લખો અને ઈ-મેલ સિક્યુરિટી સમજાવો. **(07)**

b) ફાયરવોલ શું છે? વિવિધ પ્રકારના ફાયરવૉલ સમજાવો. **(07)**

Q-4 **Attempt all questions**

a) વાયરસ વ્યાખ્યાયિત કરો વિવિધ પ્રકારના વાયરસ સમજાવો. **(07)**

b) ટ્રાન્સપોઝીશન સાઈફરને ઉદાહરણો સાથે સમજાવો **(07)**

Q-5 **Attempt all questions**

a) સેમિટ્રીક સાઈફર મોડેલ ને યોગ્ય રેખાકૃતિ સાથે સમજાવો **(07)**

b) વાસ્તવિક સમયની સ્થિતિ અંગે ફિશીંગ હુમલો સમજાવો. **(07)**

Q-6 **Attempt all questions**

a) SSL આર્કિટેક્ચર ને યોગ્ય રેખાકૃતિ સાથે સમજાવો **(07)**

b) "સિક્યોર ઈલેક્ટ્રોનિક ટ્રાન્ઝેક્શન" પર ટૂંકું નોંધ લખો **(07)**

Q-7 **Attempt all questions**

a) ડિજિટલ હસ્તાક્ષર નિર્ધારિત કરો. ડિજિટલ હસ્તાક્ષર અલ્ગોરિધમ સમજાવો. **(07)**

b) DOS અને DDos એટેક ને યોગ્ય ઉદાહરણ સાથે વિગતમાં ચર્ચા કરો. **(07)**

Q-8 **Attempt all questions**

a) ઉદાહરણો સાથે શારીરિક સુરક્ષા ઘટકને સમજાવો. **(07)**

b) કેન્દ્રિત અને વિકેન્દ્રિત આંતરમાળખા**ની સરખામણી કરો.** **(07)**