DEC - 18

Time: 3 Hours Marks: 80

N.B: Q.1 Compulsory. Solve any 4.

Q. 1 **Summaries and find Plain text by decrypting cipher text "XVWG" using Hill Cipher Substitution technique .**

KEY matrix →

$$\begin{bmatrix} 3 & 7 \\ 5 & 12 \end{bmatrix}$$

10

Q. 1 b) **Consider a scenario where an intruder wants to access some valuable information from an ongoing communication. What security services should be implemented in system and which mechanism can be used to achieve those security services?**

Q. 2 a) Encrypt " **academic committee will meet today** " using Playfair Cipher with Keyword "**ROYAL ENFIELD**" 10

Q. 2 b) Discuss CBC and OFB Block cipher Modes with examples. 10

Q. 3 a) If generator g=2 and n or p =11, using diffie Hellman algorithm, solve the following: 10

i) Show that 2 is primitive root of 11
ii) If A has public key 9, What is A's Private Key
iii) If B has public key 3, What is B's Private Key
iv) Calculate shared secret Key

Q. 3 b) **Elaborate International Data Encryption Algorithm (IDEA) and its key generation?** 10

Q. 4 a) Explain Digital Signature and Digital Certificate used for authentication 10

Q. 4 b) Calculate Cipher Text using RSA Algorithm for following data: Prime Numbers P=7, Q= 17. Plain Text Message M=10. Find pair of keys and Cipher text (D,C and P).

Q. 5 a) Explain Hash Based Message Authentication Code. Give Example also. 10

Q. 5 b) Describe various types of Intrusion Detection System (IDS). What are Active and Passive IDS?

1685EEF251B9899113CE47ECACEA3234

Q. 6 a) Convert given PT = $(CA)_{16}$ with Key (1011001101) using S-DES Algorithm.

Given- P10 (3,5,2,7,4,10,1,9,8,6) P4 (2,4,3,1)

P8 (6,3,7,4,8,5,10,9) IP (2,6,3,1,4,8,5,7)

E/P (4,1,2,3,2,3,4,1) IP^{-1} (4,1,3,5,7,2,8,6)

S0=

1	0	3	2
3	2	1	0
0	2	1	3
3	1	3	2

S1=

0	1	2	3
2	0	1	3
3	0	1	0
2	1	0	3

Q. 6 b) Explain concept of key management along with its distribution system.

1685EEF251B9899113CE47ECACEA3234

diffmail

Mailbox of exam_kgce2010

Subject: Correction in QP Code: 57241

From: University of Mumbai<support@muapps.in> on Tue, 27 Nov 2018 11:45:16

To: <exam_kgce2010@rediffmail.com>

University of Mumbai

Correction in 1T00717 - B.E.(COMPUTER)(Sem VII) (R-2012) (CBSGS) / 42102 - Cryptography and System Security **QP Code: 57241**

Instruction : Question 1 Compulsory, Solve Any Three Instead of Four

Q. 3 a) ii) If A has private key 9, What's A's Public Key
iii) If B has private key 3, what's B's Public Key

q.5 b) .... Marks 10
q.6 a) .... Marks 10
q.6 b) .... Marks 10

University of Mumbai
https://muapps.in
support@muapps.in
022-26534263 / 022-26534266
Mon-Fri, 10am - 5pm