Paper / Subject Code: 42102 / Cryptography and System Security

1T00717 - B.E.(COMPUTER)(Sem VII) (R-2012) (CBSGS) / 42102 - Cryptography and System Security

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 → 3 7 5 12

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"
- Q. 2 b) Discuss CBC and OFB Block cipher Modes with examples.
- Q. 3 a) If generator g=2 and n or p=11, using diffie Hellman algorithm, solve the following:
 - 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?
- 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?

Paper / Subject Code: 42102 / Cryptography and System Security

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

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)

- Paragram and the second of t

CALL OF THE STREET, ST

The state of the s

e a n<mark>diference</mark> por problem of also of

2. 38对数件数据数据 10 G 以下,在10 C /2

tudit sooiki

the the threshold makes by the second

The state of the second of the

of which is a special nice

eleg**os** i grene de la co Como la Como de la como

Constituted broken in a second

Complete transfer and a contract of the

E/P (4,1,2,3,2,3,4,1)

IP-1 (4,1,3,5,7,2,8,6)

S0=		1.62	r serie
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.

und Mark is a ser explored black of the kind of the **kind of the kind of the kind of the kind** (and the **kind of the kind of**