CNS QP Sessional Answers

1.a) Explain the model for Network Security.
Ans.1.a)

1.b) Illustrate the encryption and decryption process using Hill Cipher for:
Plain Text : ATTACK
Keyword : BCCF
Ans.1.b)

2.a) Apply Extended Euclid algorithm to compute GCD (99,78).
Show: all the computations.
Ans.2.a)

2.b) State the different substitution encryption techniques.
Encrypt the following plaintext using Playfair cipher:
Plain Text : CHANDRAYAAN
Keyword : MONARCHY
Ans.2.b)

3.a) Differentiate between block cipher and stream cipher.
Ans.3.a)

3.b) Explain Key Calculation Procedure in Simplified DES algorithm.
Illustrate your answer by considering user input key as 00011 00111.
Ans.3.b)

4.a) What are the block cipher modes of operation of DES? Explain in detail.
Ans.4.a)

4.b) Explain in detail about DES encryption and decryption algorithm.
Ans.4.b)

5.) Give decryption the stepwise Illustration of RSA algorithm to perform encryption and procedure for following data:

Plain Text 10	:	10
Prime No.P	:	11
Pime No. Q	:	17
Parameter e	:	7

Ans.5)

6.a) Explain in detail about the working of Diffie-Hellman key exchange algorithm.
Ans.6.a)

6.b) Apply the Chinese Remainder Theorem to solve following congruent equations.

X	≡	2	(mod 3)
X	≡	3	(mod 5)
X	≡	2	(mod 7)

Ans.6.b)

7.a) Explain in detail about X.509 directory authentication service.
Ans.7.a)

7.b) Explain MD5 message digest algorithm with example.
Ans.7.b)

8.a) Explain in detail about the hash functions and their security.
Ans.8.a)

8.b) What is Kerberos? Explain briefly about it.
Ans.8.b)

9.a) What is firewall? What are its type? Explain in brief.
Ans.9.a)

9.b) Explain in detail about SQL injection?
Ans.9.b)

10.a) Discuss in detail about application gateway firewall.
Ans.10.a)

10.b) Explain in detail about PGP,
Ans.10.b)