Roll No: --------------------------

UNIVERSITY OF PETROLEUM AND ENERGY STUDIES

End Semester Examination, December 2017

Program: B.Tech (SoCSE) (MFT+IFM)	**Semester – VII**
Subject (Course): Network Security & Cryptography	**Max. Marks : 100**
Course Code : CSEG423	**Duration : 3 Hrs**
No. of page/s: 2	

Section-A: Answer all the questions and each question carries equal marks (4x5=20 Marks)

1. Explain the format of PGP signature packet with diagram
2. Illustrate the architecture of CMAC
3. Explain the general block diagram of RSA algorithm.
4. Describe IP Sec and its architecture.

Section-B: Answer all the questions each question carries equal marks (4x10=40 Marks)

5. Discuss any one Substitution Technique and list its merits and demerits.
6. Briefly explain Deffie Hellman key exchange. In the Diffie Hellman protocol, (p,g) = (43,3). Alice and Bob choose their random secret to be 8 and 37 respectively. Compute the value of the symmetric key. Also, determine the value of $R1$ and $R2$.
7. What is the difference between stream cipher and block cipher?
8. Find the Hill cipher for the following message using the key matrix K.
   Message = “SCHOOL_OF_COES ” and K={3,4,7,8; 4,5,7,6; 6,4,3,4; 3 ,2, 6, 7}

Section-C: Answer any two questions each question carries equal marks (2x20=40)

9. A. Explain the DES key algorithm with diagram. (10 marks)
   B. Explain the digital signature and its applications. (10 marks)

10. Explain the block diagram of HMAC and its security features. (20 marks)

Or

Perform S-DES on following data: (20 marks)
Plain text : $(F2)_{16}$, Initial key : 1011100110
IP: 2 6 3 1 4 8 5 7
EP-4/8: 4 1 2 3 2 3 4 1
P4: 2 4 3 1
P10: 3 5 2 7 4 10 1 9 8 6

P8: 6 3 7 4 8 5 10 9

S1 = 1 0 3 2
3 2 1 0
0 2 1 3
3 1 3 2

S2 = 0 1 2 3
2 0 1 3
3 0 1 0
2 1 0 3

Roll No: --------------------------

UPES

UNIVERSITY OF PETROLEUM AND ENERGY STUDIES

End Semester Examination, December 2017

Program: B.Tech (SoCSE) (MFT+IFM)	**Semester – VII**
Subject (Course): Network Security & Cryptography	**Max. Marks : 100**
Course Code : CSEG423	**Duration : 3 Hrs**
No. of page/s: 1	

Section-A: Answer all the questions and each question carries equal marks (4x5=20 Marks)

1. What do you mean by Feistel cipher?
2. Explain any one substitution technique with its merits and demerits.
3. Describe Cipher Block Chaining Mode
4. Explain the DDoS attack and how it influence network security?

Section-B: Answer all the questions each question carries equal marks (4x10=40 Marks)

5. What is the difference between HMAC and CMAC?
6. Using the DSS scheme, let q=59, p=709 and d=14. Find the values of e_1 and e_2. Choose r = 13. Find the value of S_1 and S_2 if $h(M) = 100$.
7. Explain how encryption key is expanded to produce keys for the 10 rounds in AES
8. Explain the extended Euclid's algorithm to find the multiplicative invers of an integer number. Find the multiplicative inverse of 23 in Z_{102}

Section-C: Answer any two questions each question carries equal marks (2x20=40)

9. Compare and contrast the Record protocol in SSL and TLS. (20 marks)
10. A. Explain how message authentication and hash function contribute for network security. (10 marks)

    B. Explain the round structure of SHA-512 with block diagram. (10 marks)

Or

Find the result of Majority(x, y, z) if (20 marks)

x= 1234 5678 ABCD 2345 34564 5678 ABCD 2468
y=2234 5678 ABCD 2345 34564 5678 ABCD 2468
z=3234 5678 ABCD 2345 34564 5678 ABCD 2468