UNIVERSITY OF PETROLEUM AND ENERGY STUDIES

END Semester Examination, April 2017

Program Name: B.Tech(CSE)	**Semester – VIII Sem**
Course Name : Network Security and Cryptography	**Max. Marks : 100**
Course Code : CSEG-423	**Duration : 3 Hrs**
No. of page/s:02	

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

1. Discuss any one Substitution Technique and list its merits and demerits.
2. Explain the general block diagram of RSA algorithm. Encrypt and decrypt the message M="CS" using RSA algorithm for the following parameters; p=7; q=11; e=17;
3. Explain the format of PGP signature packet with diagram
4. Explain the architecture of CMAC

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

5. Explain how the encryption key is expanded to produce keys for the 10 rounds in AES
6. Describe the important criteria of a cryptographic hash function. Calculate the minimum and maximum number of padding bits that can be added to a message in SHA-512. Justify your answer.
7. 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 R_1 and R_2 .
8. How does PGP provide confidentiality and authentication service for e-mail and file storage applications? Draw the block diagram and explain its components.

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

9. A).Explain the round structure of SHA-512 with block diagram. **(10 Marks)**

   B). Define the goal of each phase in the handshake protocol of SSL. Justify your answer with necessary diagrams **(10 Marks)**
10. A). Explain the DES key generation algorithm with diagram. **(10 Marks)**

    B). Explain the block diagram of HMAC and it security features. **(10 Marks)**

11. Perform S-DES on the following data: **(20 Marks)**

Plaintext: $(F2)_{16}$, 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: --------------------------

UNIVERSITY OF PETROLEUM AND ENERGY STUDIES

End Semester Examination, April, 2017

Program Name: B.Tech(CSE) **Semester – VIII Sem**
Course Name : Network Security and Cryptography **Max. Marks : 100**
Course Code : CSEG-423 **Duration : 3 Hrs**
No. of page/s:01

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

1. Explain the extended Euclid's algorithm to find all the multiplicative inverse of Z_8 and Z_{11}
2. Apply the conditional functions on E, F G buffers of SHA-512 which contains 0x9,0xA, and 0xF respectively. Find the leftmost digit of the result
3. Write down the block diagram of double transposition cipher.
4. Write an algorithm for RSA key generation, encryption and decryption.

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

5. Explain any five types of attacks on RSA algorithm
6. In AES, how the encryption key is expanded to produce keys for the 10 rounds
7. Discuss about the objectives of HMAC and it security features.
8. Explain the Vigenere Cipher method and encrypt the message "school of computer science " using the key "CLOUD"

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

9. A). Briefly explain Deffie Hellman key exchange with an example. **(10 Marks)**
   B). Discuss clearly Secure Hash Algorithm (SHA-512) block diagram **(10 Marks)**
10. A) In a public-key system using RSA you intercept the cipher text C = 10 sent to a user whose public key is e = 5, n = 35. Compute the plain text M. **(10 Marks)**
    B). Encode the message "this is a test" using Radix-64 encoding scheme: **(10 Marks)**
11. A) Write and explain the digital signature algorithm **(10 Marks)**
    B) Write a short note on; **(2x5=10** Marks)
    i). Security attacks (ii). Security services