Name:

Enrolment No:

UNIVERSITY OF PETROLEUM AND ENERGY STUDIES

End Semester Examination, December 2019

Course: Cryptography and Network Security **Semester:VII**

Program: B.Tech(CSE+ BAO+BFSI+CCVT+ECOM-RA+TI+MT+OS&OSS+IT+OGI+HCI+MC+IOT)

Time 03 hrs.

Course Code:CSEG423 **Max. Marks: 100**

Instructions:

SECTION A

S. No.		**Marks**	**CO**
Q 1	How many keys in an organization with 100 employee will be required for securing the communication between every possible pair of employees in case the of: 1. Symmetric key cryptography 2. Public Key Cryptography	**2+2**	**CO1,CO3**
Q 2	A Cryptographer argued that in conventional bitmap image steganography instead of using the LSB(Least Significant Bit), The algorithm should use the MSB(Most Significant Bit). Point out what is wrong with the given idea.	**4**	**CO3**
Q 3	What are active and passive attacks? Explain various types of active and passive attacks.	**4**	**CO2,CO1**
Q 4	What are the services provided by IPsec?	**4**	**CO3**
Q 5	Show that for a Caesar cipher, encrypting with key (K) is same as decrypting with key (K - 26).	**4**	**CO2**

SECTION B

Q 6	Design a scenario in which X.509 Standard is applicable.	**10**	**CO4**
Q 7	Explain the feature requirement of a Kerberos system in terms of following aspects: 1. Security 2. Reliability 3. Transparency 4. Scalability	**10**	**CO2**
Q 8	Consider an Algorithm DoS_Avoid for a Web service provider. The Algorithm will deny a request from an IP X if no. of request from that IP is greater than a user provided threshold within a given Timeframe. Explain how this strategy is applicable to DoS attack but not DDoS Attack.	**10**	**CO4**

<table>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td>Q 9</td><td>In an RSA cryptosystem, a user A uses two prime numbers p = 13 and q =17, compute the private keys of user A. If the public key of A is 35. Also encrypt the plain text 88 with the given configuration.

<b>OR</b>

Attacker X thinks that he has developed an algorithm Factor() which can perform factorization in polynomial time. If his claim is real what is the implication of it.</td><td><b>10</b></td><td><b>CO2</b></td></tr>
<tr><td colspan="4"><b>SECTION-C</b></td></tr>
<tr><td>Q 10</td><td>Use 8 bit DES on the data given below and
i. Generate round keys for each round and
ii. Output of the round 1

Plaintext: 01110010 Cipher key: 1010000010 Straight P box 2 4 3 1

IP: 2 6 3 1 4 8 5 7 Expansion P box: 4 1 2 3 2 3 4 1

S-boxes:
<table>
<tr><th></th><th>0</th><th>1</th><th>2</th><th>3</th></tr>
<tr><td><b>0</b></td><td>1</td><td>0</td><td>3</td><td>2</td></tr>
<tr><td><b>1</b></td><td>3</td><td>2</td><td>1</td><td>0</td></tr>
<tr><td><b>2</b></td><td>0</td><td>2</td><td>1</td><td>3</td></tr>
<tr><td><b>3</b></td><td>3</td><td>1</td><td>3</td><td>2</td></tr>
<tr><td colspan="5">S box 1</td></tr>
</table>
<table>
<tr><th></th><th>0</th><th>1</th><th>2</th><th>3</th></tr>
<tr><td><b>0</b></td><td>0</td><td>1</td><td>2</td><td>3</td></tr>
<tr><td><b>1</b></td><td>2</td><td>0</td><td>1</td><td>3</td></tr>
<tr><td><b>2</b></td><td>3</td><td>0</td><td>1</td><td>0</td></tr>
<tr><td><b>3</b></td><td>2</td><td>1</td><td>0</td><td>3</td></tr>
<tr><td colspan="5">S Box 2</td></tr>
</table>

Straight P box for key generator 3 5 2 7 4 10 1 9 8 6

Compression P box for key generator 6 3 7 4 8 5 10 9

[Hint: P-box is used to transpose the input bits eg. If P-box is 2 4 3 1 and input bits are 1011 then output will be 0111]</td><td><b>10+10</b></td><td><b>CO4,CO2</b></td></tr>
<tr><td>Q 11</td><td>Describe a mechanism to achieve integrity, authentication and non-repudiation in public key cryptography using Digital Signature with proper diagrams.</td><td><b>20</b></td><td><b>CO1,CO2</b></td></tr>
</table>

	OR Write brief notes on the following: a. Requirements of MAC b. Requirements of Digital Signature functions c. Difference between Non-Repudiation and Integrity check. d. Using MAC with Symmetric key encryption		