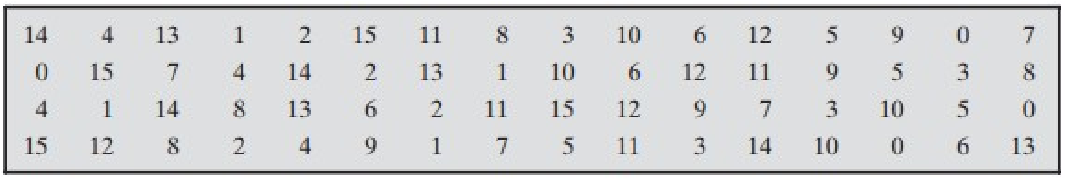
Name:

Enrolment No:

UNIVERSITY OF PETROLEUM AND ENERGY STUDIES

End Semester Examination, December 2018

Course: Cryptography and Network Security (CSEG423) **Semester:VII**
Programme: B.Tech CSE+CCVT,BAO,BFSI,ECRA,HI,IT,MFT,MI,OGI,OSS,TI
Time: 03 hrs. **Max. Marks: 100**
Instructions: Read the questions carefully

<table>
<tr><th colspan="4">SECTION A</th></tr>
<tr><td>S. No.</td><td></td><td><b>Marks</b></td><td><b>CO</b></td></tr>
<tr><td>Q 1</td><td>How many one-to-one affine Caesar ciphers are there for 26 alphabets?</td><td><b>4</b></td><td><b>CO1</b></td></tr>
<tr><td>Q 2</td><td>What will be the output value of the given S-Box(6x4) if the input is:
a. 36
b. 7

<table>
<tr><td>14</td><td>4</td><td>13</td><td>1</td><td>2</td><td>15</td><td>11</td><td>8</td><td>3</td><td>10</td><td>6</td><td>12</td><td>5</td><td>9</td><td>0</td><td>7</td></tr>
<tr><td>0</td><td>15</td><td>7</td><td>4</td><td>14</td><td>2</td><td>13</td><td>1</td><td>10</td><td>6</td><td>12</td><td>11</td><td>9</td><td>5</td><td>3</td><td>8</td></tr>
<tr><td>4</td><td>1</td><td>14</td><td>8</td><td>13</td><td>6</td><td>2</td><td>11</td><td>15</td><td>12</td><td>9</td><td>7</td><td>3</td><td>10</td><td>5</td><td>0</td></tr>
<tr><td>15</td><td>12</td><td>8</td><td>2</td><td>4</td><td>9</td><td>1</td><td>7</td><td>5</td><td>11</td><td>3</td><td>14</td><td>10</td><td>0</td><td>6</td><td>13</td></tr>
</table></td><td><b>4</b></td><td><b>CO2</b></td></tr>
<tr><td>Q 3</td><td>For each of the following equations, find an integer that satisfies the equation.
a. $5x \equiv 4 \pmod 3$
b. $7x \equiv 6 \pmod 5$</td><td><b>4</b></td><td><b>CO1</b></td></tr>
<tr><td>Q 4</td><td>In PGP, what is the probability that a user with public keys will have at least one duplicate key ID?</td><td><b>4</b></td><td><b>CO4</b></td></tr>
<tr><td>Q 5</td><td>Differentiate between chosen cipher text and chosen plain text attack.</td><td><b>4</b></td><td><b>CO1</b></td></tr>
<tr><th colspan="4">SECTION B</th></tr>
<tr><td>Q 6</td><td>Consider an automated teller machine (ATM) in which users provide a personal identification number (PIN) and a card for account access. Give examples of confidentiality, integrity, and availability requirements associated with the system</td><td><b>8</b></td><td><b>CO1</b></td></tr>
<tr><td>Q 7</td><td>Suppose that two parties A and B wish to setup a common secret key (D-H key) between themselves using the Diffie-Hellman key exchange technique. They agree on 7 as the modulus and 3 as the primitive root. Party A chooses 2 and party B chooses 5 as their respective secrets. What is their common secret key?</td><td><b>8</b></td><td><b>CO3</b></td></tr>
<tr><td>Q 8</td><td>Describe OSI Security Architecture and provide various advantages of using this architecture in context of various types of security services.
OR
Explain how would you perform in your way the various essential tasks in designing a basic security model for a system.</td><td><b>8</b></td><td><b>CO4</b></td></tr>
<tr><td>Q 9</td><td>Explain any two of the following in detail:</td><td><b>8</b></td><td><b>CO4</b></td></tr>
</table>

	a. Firewall b. Malicious Software c. VPN		
Q 10	Briefly explain IP Security Architecture.	**8**	**CO4**
SECTION-C			
Q 11	In the RSA public-key encryption scheme, each user has a public key, e, and a private key, d. Suppose Bob leaks his private key. Rather than generating a new modulus, he decides to generate a new public and a new private key. Is this safe? justify your answer with valid arguement.	**20**	**CO3**
Q 12	What are the requirements for digital signature? Briefly explain direct digital signature and arbitrated digital signatures. OR Write the digital signature algorithm. Also explain the signing and verifying functions of digital signature algorithm.	**20**	**CO4**

Name: **Enrolment No:**	UPES

UNIVERSITY OF PETROLEUM AND ENERGY STUDIES
End Semester Examination, December 2018
Course: Cryptography and Network Security(CSEG423) **Semester:VII**
Programme: B.Tech CSE+CCVT,BAO,BFSI,ECRA,HI,IT,MFT,MI,OGI,OSS,TI
Time: 03 hrs. **Max. Marks: 100**
Instructions: Read the questions carefully

	SECTION A		
S. No.		**Marks**	**CO**
Q 1	Define the term cryptography and steganography.	**4**	**CO1**
Q 2	Discuss about the parameters and design features of classical Fiestel Network.	**4**	**CO2**
Q 3	Calculate the last two digits of 17^{16}.	**4**	**CO1**
Q 4	Explain different types of firewalls.	**4**	**CO1**
Q 5	Differentiate between Passive and Active attack.	**4**	**CO1**
	SECTION B		
Q 6	Explain the CIA(Confidentiality, Integrity, Availability) in respect to postal service.	**8**	**CO1**
Q 7	In an RSA system, the public key of a given user is e = 31, n = 3599.What is the private key of this user?	**8**	**CO3**
Q 8	In PGP, what is the probability that a user with public keys will have at least one duplicate key ID?	**8**	**CO4**
Q 9	Describe OSI Security Architecture and provide its features and respective cost in context of system resources. OR Discuss the required essential features to build a robust model of network security.	**8**	**CO4**
Q 10	Briefly explain how IP Security Architecture is related to Security Policy Databases.	**8**	**CO4**
	SECTION-C		
Q 11	What are the requirements for digital signature? Briefly explain direct digital signature and arbitrated digital signatures. OR Write the digital signature algorithm. Also explain the signing and verifying functions of digital signature algorithm.	**20**	**CO4**
Q 12	With a neat schematic, explain the single round of fiestel encryption model. Also explain the concept of confusion and diffusion.	**20**	**CO2,CO3**