Roll No.:.....

National Institute of Technology, Delhi

Name of the Examination: B. Tech

Branch : CSE Semester :VIII

Title of the Course :Network Security& Cryptography Course Code : CSL466

Time: 3.0Hours **Maximum Marks: 50**

Course Matrix (CO-PO-PSO Mapping)

COs	POs													
	PO 1	PO 2	PO3	PO4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO11	PO12	PSO1	PSO2
CO1	-	-	-		-	-	-	-	-	-	-	-		
CO2	-	-	-		-	-	-	-	-	-	-	-		
CO3	-	1	2, 3	3	-	-	-	-	-	-	-	-	1, 2	3
CO4	-	-	4	4, 5	-	-	-	-	-	-	-	-	4	5

Note: Please attempt all questions

---

1. Monica breeds some pets. She does not know the exact number of pets she has. So she told that when she takes rounds, she observed some things. In the morning there are five pets in each group exceptone group which has only two pets. In the afternoon there are seven pets in each group except one group which has six pets. In the evening, there are eleven pets in each group. Monica is sure that there are fewer than 150 pets. Find out, the smallest number of pets does she have. **(6Marks)**

2. An old woman purchases a basket of some eggs from the market. While walking on the road she stops for a while and keep her basket of eggs down on the road. A horse running on the road accidentally steps on the basket and crushing all the eggs in the basket. The rider offers to pay the old woman for the damaged eggs. So, he asks her about the total number of eggs she had brought. The old woman does not remember the exact number of eggs in the basket. So she told the rider that when she had taken out two eggs at a time from the basket, there was one egg left. When she had taken out three eggs at a time from the basket, there were two eggs left. When she had taken out five at a time from the basket, there were four eggs left. Find out, the smallest number of eggs an old woman could have had in her basket? **(6 Marks)**

3. User A and B use the Diffie-Hellman Key exchange technique. They agree with a common prime $n=67$ and a primitive root $g=5$.
   a) If user A has private key $X_A = 10$, what is A's public key Y_A?
   b) If user B has private key $X_B = 24$, what is B's public key Y_B?
   c) What is the shared secret key?

   (6 Marks)

4. The parameters given are: p=3, q=19. Find out the possible public key and private for RSA algorithm. Also encrypt the message "6". **(5 Marks)**
5. Find the smallest multiple of 10 which has remainder 1 when divided by 3, remainder 6 when divided by 7 and remainder 6 when divided by 11. **(5 Marks)**
6. Find the multiplicative inverse of -74 mod 501, using the extended Euclidean algorithm. **(5 Marks)**
7. Find the value of $7^7 \bmod 9$. **(5 Marks)**
8. Find the smallest positive residue y in the following congruence.
   $7^{69} = y \bmod 23$ **(6 Marks)**
9. Explain the Index Calculus Algorithm. **(6 Marks)**

Q. No.	1	2	3	4	5	6	7	8	9
CO's	2	2	2	3	3	3, 4	3, 4	4	4

Roll No.:.....

National Institute of Technology, Delhi

Name of the Examination: B. Tech

Branch : CSE **Semester** :VIII

Title of the Course :InformationSecurity **Course Code** : CSB451

Time: 3.0Hours **Maximum Marks: 50**

Course Matrix (CO-PO-PSO Mapping)

COs	POs													
	PO 1	PO 2	PO3	PO4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO11	PO12	PSO1	PSO2
CO1	-	-	-		-	-	-	-	-	-	-	-		
CO2	-	-	-		-	-	-	-	-	-	-	-		
CO3	-	-	1, 2	2, 3	-	-	-	-	-	-	-	-	1, 2	3
CO4	-	-	4	4, 5	-	-	-	-	-	-	-	-	4	5

Note: Please attempt all questions

1.
   a. What is authentication? What are the objectives of authentication? **(3Marks)**
   b. Explain the password-based authentication method. **(3Marks)**
   c. Explain the two-factor authentication method. **(3 Marks)**

2.
   a. With respect to Kerberos, gives the three basic steps involved in authenticating a user to an end service. **(4)**
   b. Compare Kerberos with SSL. **(3Marks)**
   c. Explain the X.509 certificate. **(3 Marks)**

3. Explain the following algorithms for digital signature schemes:
   a. A key generation algorithm **(3 Marks)**
   b. A signing algorithm **(3 Marks)**
   c. A verification algorithm **(3 Marks)**

4.
   a. Explain the different header fields included in MIME. **(4Marks)**
   b. Explain the working of S/MIME. **(3 Marks)**
   c. Compare PGP with S/MIME. **(3 Marks)**

5.
   a. Which security services are provided by Encapsulating Security Payload (ESP) protocol? **(3 Marks)**
   b. What is security association in IPsec? How can it work? **(3 Marks)**
   c. How do the Authentication Header used? **(3 Marks)**
   d. Explain different types of VPN. **(3 Marks)**

Q. No.	1	2	3	4	5
CO's	2, 3	3	3,4	4	4