VIT®
Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

# School of Computer Science and Engineering

**Winter Semester 2024-2025**

**Laboratory Mid-Term Assessment Test**

**SLOT L47+L48**

**Programme Name &Branch : B.Tech & Computer Science and Engineering**

**Course Name & code: Cryptography and Network Security Lab & BCSE309P**

**Class Number (s): VL2024250504969**

**Faculty Name (s): Dr.V.ILAYARAJA**

**Exam Duration: 1hour and 30 Mins** **Maximum Marks: 20** **Date: 12.03.25**

## Instructions:

1. Duration – 1 hour 30 minutes **(05:45 PM to 07:15 PM).** Complete your Exam before 7.15 PM, because next LAB slot students will be waiting outside to write their exams. But, You have to be there in the Lab at **05.35 pm. Don't bring your cell phone, all electronic items and bags to the Lab.**
2. Wear your ID card. Switch off your mobile and put it in your bag.
3. Question number is given in the top right hand side corner of the Answer paper distributed.
4. A. Evaluation components (20 Marks):

    a. Algorithm (5 marks) :
    b. Code (10 marks) :
    c. Output (5 marks) :
    Total (20 marks) :

    **Write this in the first page of your answer sheet.**

5. Take screenshot of

    a. Your complete source code

b. Output (Given input and output must be in a same screenshot)

6. Align all these 2 components (a & b) in the word document and **File name must be your reg. no. (Full reg. no with capital). Inside this document also, should have your register no, name, Slot name, Q.no, Question and followed by above said contents (a & b). (Note: Convert into pdf and you can upload the pdf)**

7. Now, you can upload your pdf document in **the given upload folder.**

**8. Screenshot must be readable one.**

9. You have to write only "Algorithm steps & Output" in the Answer sheet. **No need to write program.**

10. If you end up with error also, you have to take a screenshot of error program and the error information.

11. Documents uploaded after 07.15 PM will not be evaluated.

12. Upload only once. If multiple uploads are found, then your file becomes invalid for evaluation.

**13. If any kind of malpractice is identified, mark will be 0.**

**14. Don't ask any doubts in a Question Paper during your exam time. Other than login issue, don't ask anything. Otherwise your time will be wasted. Treat this as FAT theory.**

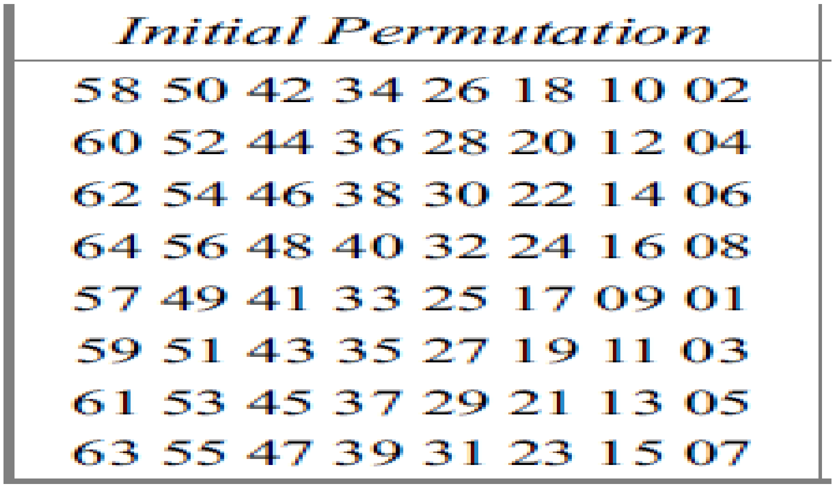
**15. You can use any language to implement an experiment, but you should not use any of the library functions. You have to write only code for each operation.**

## Questions List

1. Use the RSA algorithm to find n, ϕ(n), d if p=7, q=11, e=13 and encrypt the plaintext "5" and "63" and also decrypt it.

2. Decrypt the message "gatlmzclrqtx" using playfair cipher with the key "monarchy".

3. In DES, Show the results of the following hexadecimal data after passing it through the initial permutation box. Show the results in hexadecimal.
   0110 1023



| Initial Permutation | | | | | | | |
|---|---|---|---|---|---|---|---|
| 58 | 50 | 42 | 34 | 26 | 18 | 10 | 02 |
| 60 | 52 | 44 | 36 | 28 | 20 | 12 | 04 |
| 62 | 54 | 46 | 38 | 30 | 22 | 14 | 06 |
| 64 | 56 | 48 | 40 | 32 | 24 | 16 | 08 |
| 57 | 49 | 41 | 33 | 25 | 17 | 09 | 01 |
| 59 | 51 | 43 | 35 | 27 | 19 | 11 | 03 |
| 61 | 53 | 45 | 37 | 29 | 21 | 13 | 05 |
| 63 | 55 | 47 | 39 | 31 | 23 | 15 | 07 |

4. Answer the following questions about S-boxes in DES:
   a. Show the result of passing 110111 through S-box 3.
   b. Show the result of passing 001100 through S-box 4.
   Show these results in both binary and decimal.

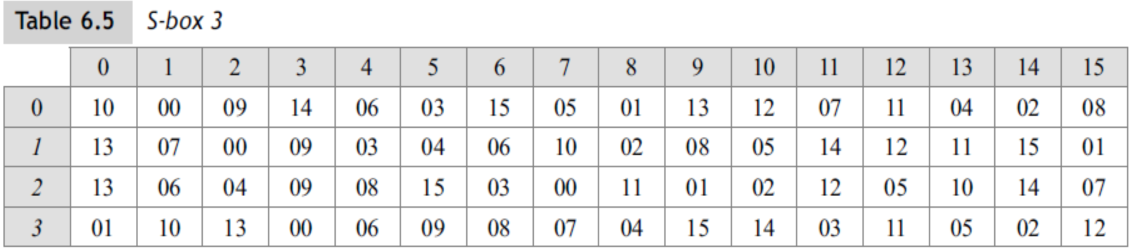


**Table 6.5** *S-box 3*

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 10 | 00 | 09 | 14 | 06 | 03 | 15 | 05 | 01 | 13 | 12 | 07 | 11 | 04 | 02 | 08 |
| *1* | 13 | 07 | 00 | 09 | 03 | 04 | 06 | 10 | 02 | 08 | 05 | 14 | 12 | 11 | 15 | 01 |
| *2* | 13 | 06 | 04 | 09 | 08 | 15 | 03 | 00 | 11 | 01 | 02 | 12 | 05 | 10 | 14 | 07 |
| *3* | 01 | 10 | 13 | 00 | 06 | 09 | 08 | 07 | 04 | 15 | 14 | 03 | 11 | 05 | 02 | 12 |

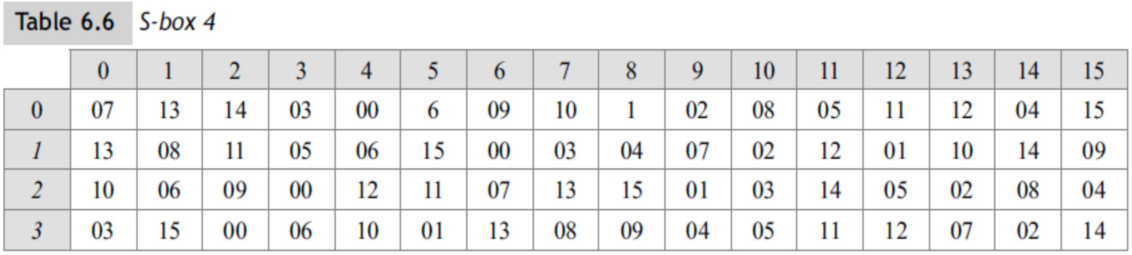


**Table 6.6** *S-box 4*

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 07 | 13 | 14 | 03 | 00 | 6 | 09 | 10 | 1 | 02 | 08 | 05 | 11 | 12 | 04 | 15 |
| *1* | 13 | 08 | 11 | 05 | 06 | 15 | 00 | 03 | 04 | 07 | 02 | 12 | 01 | 10 | 14 | 09 |
| *2* | 10 | 06 | 09 | 00 | 12 | 11 | 07 | 13 | 15 | 01 | 03 | 14 | 05 | 02 | 08 | 04 |
| *3* | 03 | 15 | 00 | 06 | 10 | 01 | 13 | 08 | 09 | 04 | 05 | 11 | 12 | 07 | 02 | 14 |

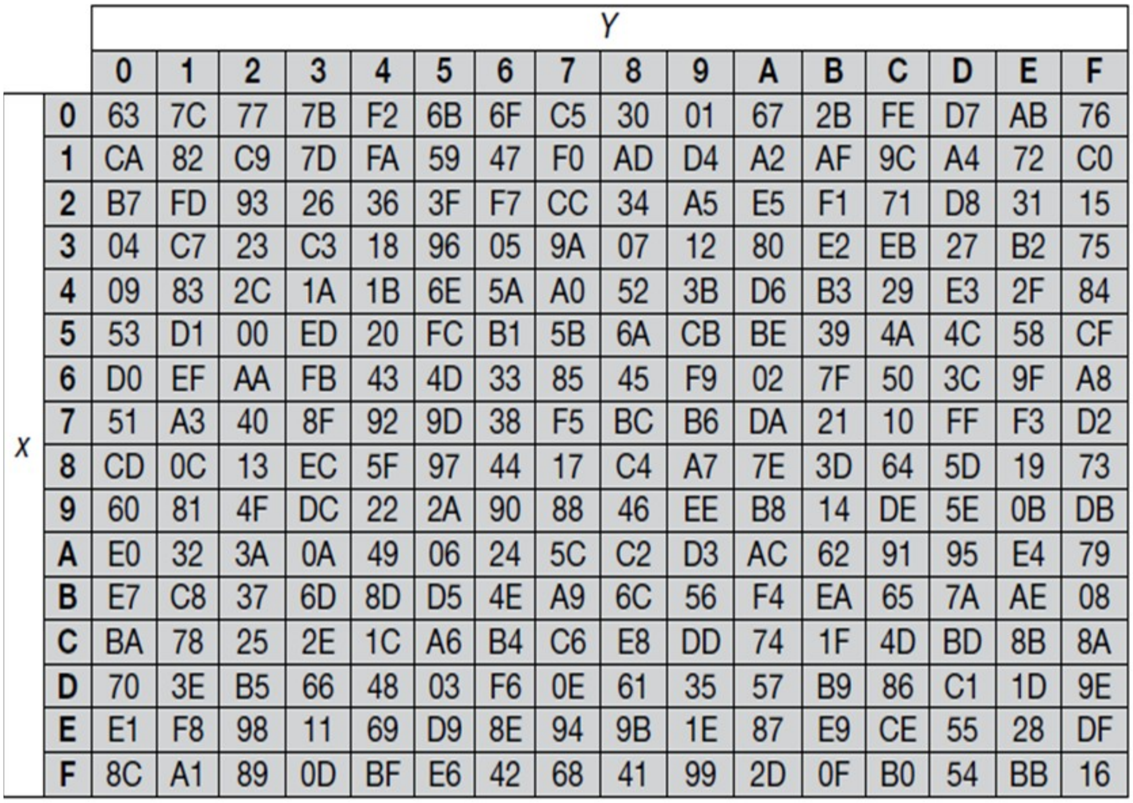
5. Use a Hill cipher to decrypt the message "apadjtftwlfj" using the key. (Key should be 2 X 2 matrix)
   Key:
   7 8
   11 11

6. Find the 10th round key of AES 128 using the following 9th round key which is given in hexadecimal, S-Box table and round constant 36. (Note: No need to declare all the values of S-box, manually find the answer for sub word and proceed further)

**9th Round Key**

| | | | |
|---|---|---|---|
| BF | 45 | A1 | F7 |
| E2 | 59 | 64 | F1 |
| BF | FA | 80 | CB |
| 90 | B2 | B4 | D8 |

S-Box Table



| | | Y | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F |
| X | 0 | 63 | 7C | 77 | 7B | F2 | 6B | 6F | C5 | 30 | 01 | 67 | 2B | FE | D7 | AB | 76 |
| | 1 | CA | 82 | C9 | 7D | FA | 59 | 47 | F0 | AD | D4 | A2 | AF | 9C | A4 | 72 | C0 |
| | 2 | B7 | FD | 93 | 26 | 36 | 3F | F7 | CC | 34 | A5 | E5 | F1 | 71 | D8 | 31 | 15 |
| | 3 | 04 | C7 | 23 | C3 | 18 | 96 | 05 | 9A | 07 | 12 | 80 | E2 | EB | 27 | B2 | 75 |
| | 4 | 09 | 83 | 2C | 1A | 1B | 6E | 5A | A0 | 52 | 3B | D6 | B3 | 29 | E3 | 2F | 84 |
| | 5 | 53 | D1 | 00 | ED | 20 | FC | B1 | 5B | 6A | CB | BE | 39 | 4A | 4C | 58 | CF |
| | 6 | D0 | EF | AA | FB | 43 | 4D | 33 | 85 | 45 | F9 | 02 | 7F | 50 | 3C | 9F | A8 |
| | 7 | 51 | A3 | 40 | 8F | 92 | 9D | 38 | F5 | BC | B6 | DA | 21 | 10 | FF | F3 | D2 |
| | 8 | CD | 0C | 13 | EC | 5F | 97 | 44 | 17 | C4 | A7 | 7E | 3D | 64 | 5D | 19 | 73 |
| | 9 | 60 | 81 | 4F | DC | 22 | 2A | 90 | 88 | 46 | EE | B8 | 14 | DE | 5E | 0B | DB |
| | A | E0 | 32 | 3A | 0A | 49 | 06 | 24 | 5C | C2 | D3 | AC | 62 | 91 | 95 | E4 | 79 |
| | B | E7 | C8 | 37 | 6D | 8D | D5 | 4E | A9 | 6C | 56 | F4 | EA | 65 | 7A | AE | 08 |
| | C | BA | 78 | 25 | 2E | 1C | A6 | B4 | C6 | E8 | DD | 74 | 1F | 4D | BD | 8B | 8A |
| | D | 70 | 3E | B5 | 66 | 48 | 03 | F6 | 0E | 61 | 35 | 57 | B9 | 86 | C1 | 1D | 9E |
| | E | E1 | F8 | 98 | 11 | 69 | D9 | 8E | 94 | 9B | 1E | 87 | E9 | CE | 55 | 28 | DF |
| | F | 8C | A1 | 89 | 0D | BF | E6 | 42 | 68 | 41 | 99 | 2D | 0F | B0 | 54 | BB | 16 |

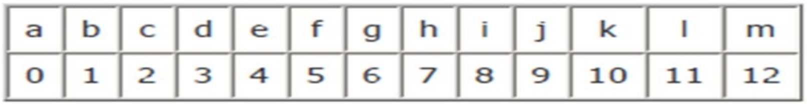
7.

Alice and Bob use the Diffie-Hellman key exchange technique with a common prime q = 71 and its primitive root=7

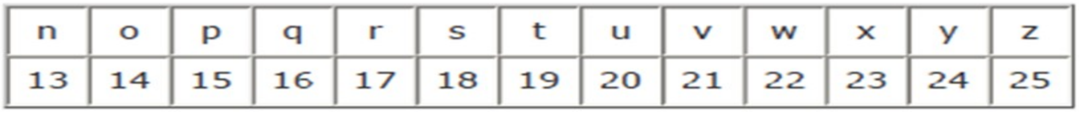
i. If Bob has public key $Y_B = 4$, what is Bob's pvt key $X_B$?

ii. If Alice has public key $Y_A = 51$, what is the shared key K with Bob.

8. Use the RSA algorithm to find n, ϕ(n), d if p=109, q=127, e=17 and Encrypt the message "math is fun" using 00 to 25 for letters A to Z and 26 for the space and also decrypt it.
9. Encrypt the plaintext "MATRIX" using the Vigenère cipher with the key "CODE". Refer the following table for this question.



| a | b | c | d | e | f | g | h | i | j | k | l | m |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |



| n | o | p | q | r | s | t | u | v | w | x | y | z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

10.

Alice and Bob use the Diffie – Hellman key exchange technique with a common prime P = 227 and primitive root g = 14.

a) If Alice has a private key $X_a$ = 227, find her public key $Y_a$?

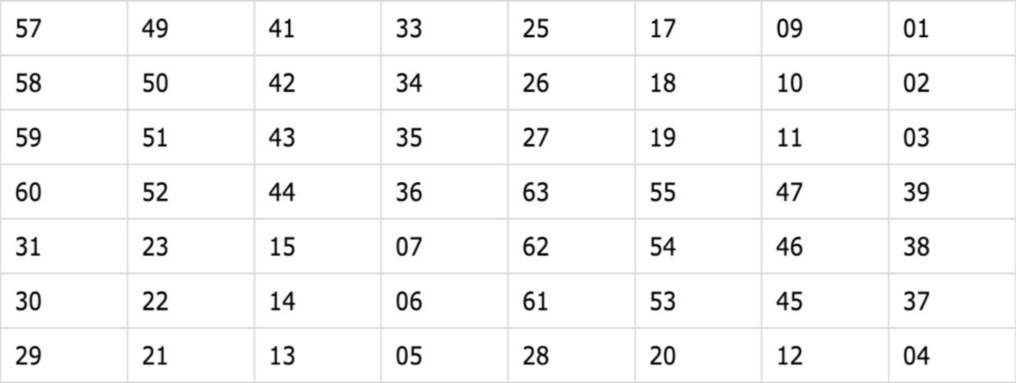
b) If Bob has a private key $X_b$ = 170, find her public key $Y_b$?

c) What is the shared secret key between Alice and Bob?

## SET-A

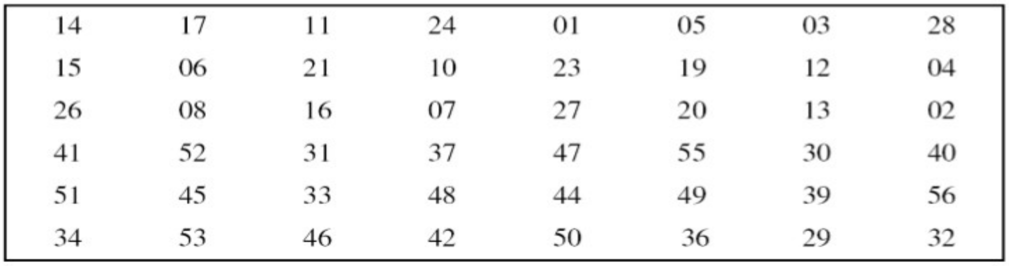
1. Write a C/C++/JAVA /Python program to implement the following: A person wants to share a plaintext “123456ABCD132536” to his friend in the opposite side through social network. He/she uses Data Encryption Standard (DES) algorithm for session encryption during his communication and assume that he/she uses, the key as “ AABB 0918 2736 CCDD”. Show the key generated for the first two rounds.

Parity Drop Table



| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 57 | 49 | 41 | 33 | 25 | 17 | 09 | 01 |
| 58 | 50 | 42 | 34 | 26 | 18 | 10 | 02 |
| 59 | 51 | 43 | 35 | 27 | 19 | 11 | 03 |
| 60 | 52 | 44 | 36 | 63 | 55 | 47 | 39 |
| 31 | 23 | 15 | 07 | 62 | 54 | 46 | 38 |
| 30 | 22 | 14 | 06 | 61 | 53 | 45 | 37 |
| 29 | 21 | 13 | 05 | 28 | 20 | 12 | 04 |

Compression Box Table



| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 14 | 17 | 11 | 24 | 01 | 05 | 03 | 28 |
| 15 | 06 | 21 | 10 | 23 | 19 | 12 | 04 |
| 26 | 08 | 16 | 07 | 27 | 20 | 13 | 02 |
| 41 | 52 | 31 | 37 | 47 | 55 | 30 | 40 |
| 51 | 45 | 33 | 48 | 44 | 49 | 39 | 56 |
| 34 | 53 | 46 | 42 | 50 | 36 | 29 | 32 |

2. Suppose you are asked to implement a cryptography application that requires converting Hexadecimal numbers to binary and binary to decimal. Write a C/C++/JAVA/Python program for this purpose.

SET-B

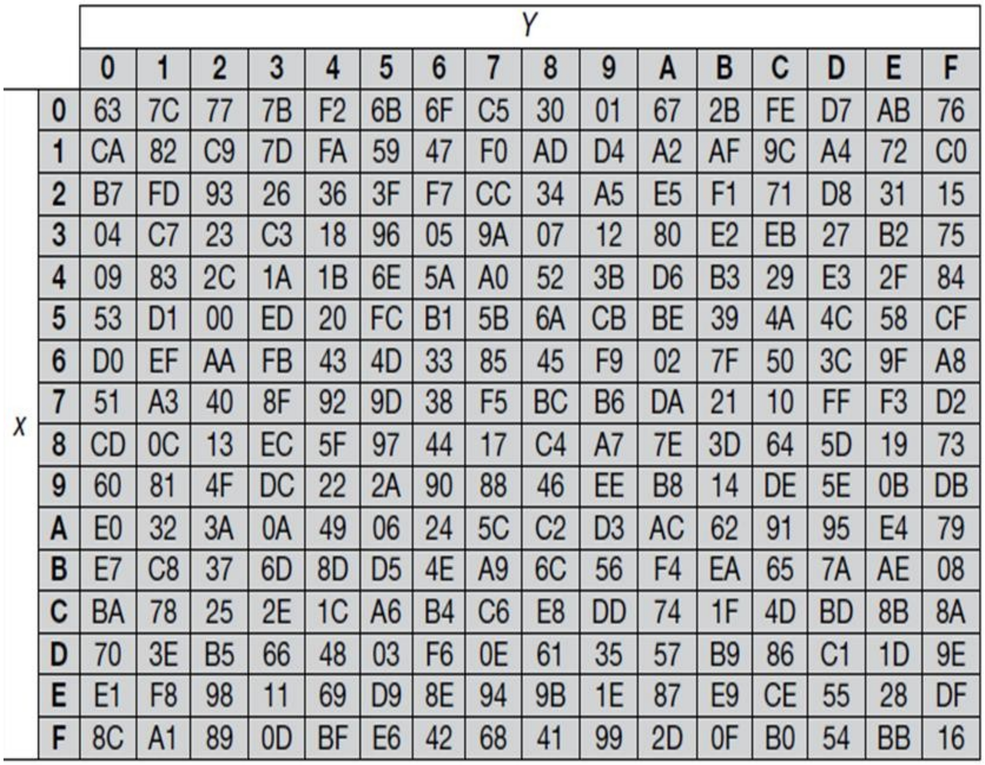
1. Write a C/C++/JAVA/Python code to implement the following:

Find the third round key of AES 128 using the following second round key which is given in hexadecimal, S-Box table and round constant 04.

Second Round Key

| | | | |
|---|---|---|---|
| 56 | C7 | 76 | A0 |
| 08 | 1A | 43 | 3A |
| 20 | B1 | 55 | F7 |
| 07 | 8F | 69 | FA |

S-Box Table



| | | Y | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F |
| | 0 | 63 | 7C | 77 | 7B | F2 | 6B | 6F | C5 | 30 | 01 | 67 | 2B | FE | D7 | AB | 76 |
| | 1 | CA | 82 | C9 | 7D | FA | 59 | 47 | F0 | AD | D4 | A2 | AF | 9C | A4 | 72 | C0 |
| | 2 | B7 | FD | 93 | 26 | 36 | 3F | F7 | CC | 34 | A5 | E5 | F1 | 71 | D8 | 31 | 15 |
| | 3 | 04 | C7 | 23 | C3 | 18 | 96 | 05 | 9A | 07 | 12 | 80 | E2 | EB | 27 | B2 | 75 |
| | 4 | 09 | 83 | 2C | 1A | 1B | 6E | 5A | A0 | 52 | 3B | D6 | B3 | 29 | E3 | 2F | 84 |
| | 5 | 53 | D1 | 00 | ED | 20 | FC | B1 | 5B | 6A | CB | BE | 39 | 4A | 4C | 58 | CF |
| | 6 | D0 | EF | AA | FB | 43 | 4D | 33 | 85 | 45 | F9 | 02 | 7F | 50 | 3C | 9F | A8 |
| | 7 | 51 | A3 | 40 | 8F | 92 | 9D | 38 | F5 | BC | B6 | DA | 21 | 10 | FF | F3 | D2 |
| X | 8 | CD | 0C | 13 | EC | 5F | 97 | 44 | 17 | C4 | A7 | 7E | 3D | 64 | 5D | 19 | 73 |
| | 9 | 60 | 81 | 4F | DC | 22 | 2A | 90 | 88 | 46 | EE | B8 | 14 | DE | 5E | 0B | DB |
| | A | E0 | 32 | 3A | 0A | 49 | 06 | 24 | 5C | C2 | D3 | AC | 62 | 91 | 95 | E4 | 79 |
| | B | E7 | C8 | 37 | 6D | 8D | D5 | 4E | A9 | 6C | 56 | F4 | EA | 65 | 7A | AE | 08 |
| | C | BA | 78 | 25 | 2E | 1C | A6 | B4 | C6 | E8 | DD | 74 | 1F | 4D | BD | 8B | 8A |
| | D | 70 | 3E | B5 | 66 | 48 | 03 | F6 | 0E | 61 | 35 | 57 | B9 | 86 | C1 | 1D | 9E |
| | E | E1 | F8 | 98 | 11 | 69 | D9 | 8E | 94 | 9B | 1E | 87 | E9 | CE | 55 | 28 | DF |
| | F | 8C | A1 | 89 | 0D | BF | E6 | 42 | 68 | 41 | 99 | 2D | 0F | B0 | 54 | BB | 16 |

b. Find GCD, variables S and T by construct a table for the following inputs using

Extended Euclidean Algorithm. 291, 41.

SET-C

1. Write a C/C++/JAVA/Python code to implement the following: Consider the ElGamal signature scheme with p = 467, α = 2 and Xa = 127. Perform detailed signing and verification procedures for the hash of the message h(M) = 100 and K = 213.

2. Suppose you are asked to implement a cryptography application that requires converting decimal number to binary and binary to hexadecimal. Write a C/C++/JAVA/Python program for this purpose.

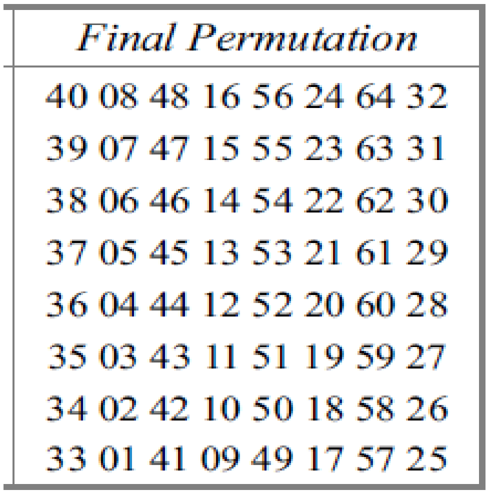
## **Questions List**

1. In a Diffie-Hellman Key Exchange, Alice and Bob have chosen prime value q = 17 and primitive root = 5. If Alice's private key is 4 and Bob's private key is 6, what is the public key of both users and secret key they exchanged?

2. Jennifer creates a pair of keys for herself. She chooses p = 397, q = 401. Find her n and ϕ(n). She then chooses e = 343 and find d value. Show how Ted can send a message "NO" to Jennifer if he knows e and n values. Do the encryption and decryption process using RSA
**(Note: He has to change each character to a number, Use 00 to A……25 to Z format. So, each character coded as two digits and he then concatenates these two digits and then gets a four digit number and do the further process)**

3. Encipher the message "instruments" using playfair cipher with the key "monarchy".

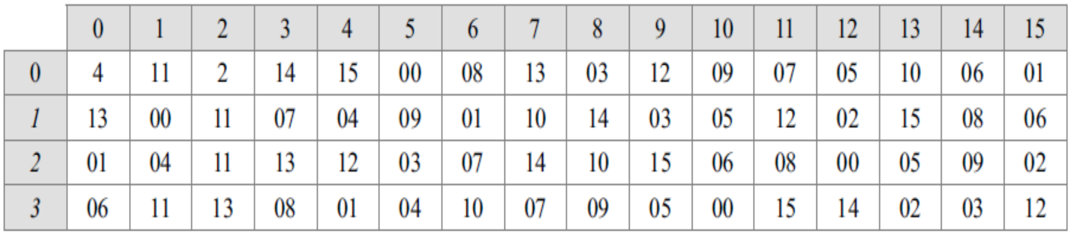
4. In DES, Show the results of the following hexadecimal data after passing it through the final permutation box. Show the results in hexadecimal.
1066 0099



| *Final Permutation* |
|---|
| 40 08 48 16 56 24 64 32 |
| 39 07 47 15 55 23 63 31 |
| 38 06 46 14 54 22 62 30 |
| 37 05 45 13 53 21 61 29 |
| 36 04 44 12 52 20 60 28 |
| 35 03 43 11 51 19 59 27 |
| 34 02 42 10 50 18 58 26 |
| 33 01 41 09 49 17 57 25 |

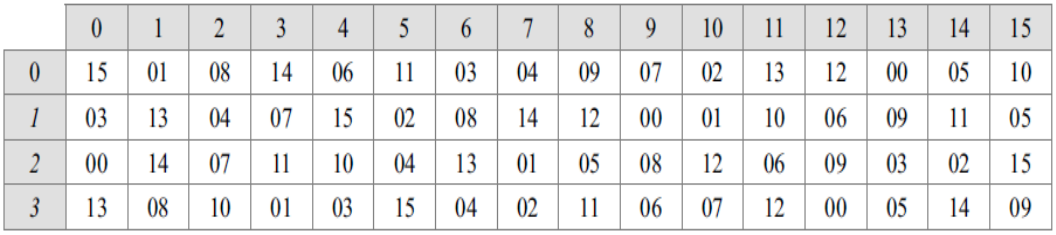
5. Answer the following questions about S-boxes in DES:
a. Show the result of passing 000000 through S-box 7.
b. Show the result of passing 111111 through S-box 2.
Show these results in both binary and decimal.

**Table 6.9** *S-box 7*



| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 4 | 11 | 2 | 14 | 15 | 00 | 08 | 13 | 03 | 12 | 09 | 07 | 05 | 10 | 06 | 01 |
| *1* | 13 | 00 | 11 | 07 | 04 | 09 | 01 | 10 | 14 | 03 | 05 | 12 | 02 | 15 | 08 | 06 |
| *2* | 01 | 04 | 11 | 13 | 12 | 03 | 07 | 14 | 10 | 15 | 06 | 08 | 00 | 05 | 09 | 02 |
| *3* | 06 | 11 | 13 | 08 | 01 | 04 | 10 | 07 | 09 | 05 | 00 | 15 | 14 | 02 | 03 | 12 |

**Table 6.4** *S-box 2*



| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 15 | 01 | 08 | 14 | 06 | 11 | 03 | 04 | 09 | 07 | 02 | 13 | 12 | 00 | 05 | 10 |
| *1* | 03 | 13 | 04 | 07 | 15 | 02 | 08 | 14 | 12 | 00 | 01 | 10 | 06 | 09 | 11 | 05 |
| *2* | 00 | 14 | 07 | 11 | 10 | 04 | 13 | 01 | 05 | 08 | 12 | 06 | 09 | 03 | 02 | 15 |
| *3* | 13 | 08 | 10 | 01 | 03 | 15 | 04 | 02 | 11 | 06 | 07 | 12 | 00 | 05 | 14 | 09 |

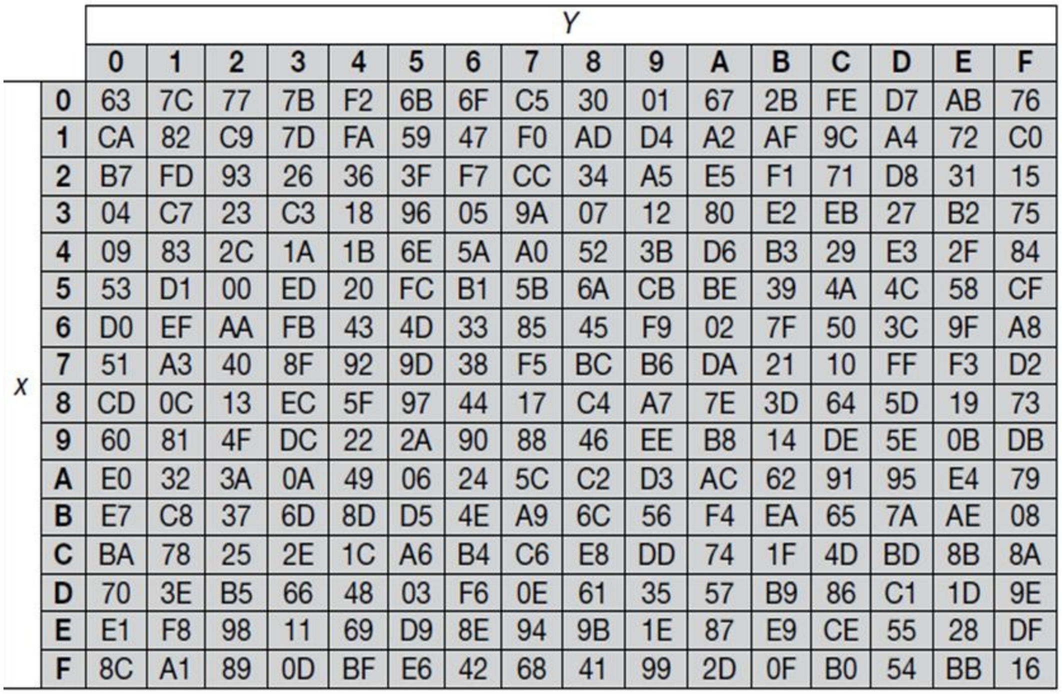
6. Use a Hill cipher to encipher the message “shortexample” using the key. (Key should be 2 X 2 matrix)
   Key:
   7 8
   11 11

7. Find the 9th round key of AES 128 using the following 8th round key which is given in hexadecimal, S-Box table and round constant 1B. **(Note: No need to declare all the values of S-box, manually find the answer for sub word and proceed further)**

8th Round Key

| | | | |
|---|---|---|---|
| 8E | FA | E4 | 56 |
| 51 | BB | 3D | 95 |
| EF | 45 | 7A | 4B |
| 21 | 22 | 06 | 6C |

S-Box Table

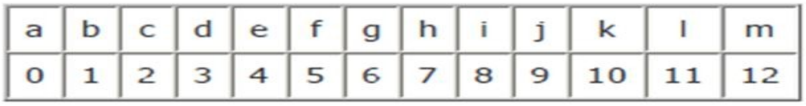


| | | Y | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | **0** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **A** | **B** | **C** | **D** | **E** | **F** |
| | **0** | 63 | 7C | 77 | 7B | F2 | 6B | 6F | C5 | 30 | 01 | 67 | 2B | FE | D7 | AB | 76 |
| | **1** | CA | 82 | C9 | 7D | FA | 59 | 47 | F0 | AD | D4 | A2 | AF | 9C | A4 | 72 | C0 |
| | **2** | B7 | FD | 93 | 26 | 36 | 3F | F7 | CC | 34 | A5 | E5 | F1 | 71 | D8 | 31 | 15 |
| | **3** | 04 | C7 | 23 | C3 | 18 | 96 | 05 | 9A | 07 | 12 | 80 | E2 | EB | 27 | B2 | 75 |
| | **4** | 09 | 83 | 2C | 1A | 1B | 6E | 5A | A0 | 52 | 3B | D6 | B3 | 29 | E3 | 2F | 84 |
| | **5** | 53 | D1 | 00 | ED | 20 | FC | B1 | 5B | 6A | CB | BE | 39 | 4A | 4C | 58 | CF |
| | **6** | D0 | EF | AA | FB | 43 | 4D | 33 | 85 | 45 | F9 | 02 | 7F | 50 | 3C | 9F | A8 |
| | **7** | 51 | A3 | 40 | 8F | 92 | 9D | 38 | F5 | BC | B6 | DA | 21 | 10 | FF | F3 | D2 |
| *x* | **8** | CD | 0C | 13 | EC | 5F | 97 | 44 | 17 | C4 | A7 | 7E | 3D | 64 | 5D | 19 | 73 |
| | **9** | 60 | 81 | 4F | DC | 22 | 2A | 90 | 88 | 46 | EE | B8 | 14 | DE | 5E | 0B | DB |
| | **A** | E0 | 32 | 3A | 0A | 49 | 06 | 24 | 5C | C2 | D3 | AC | 62 | 91 | 95 | E4 | 79 |
| | **B** | E7 | C8 | 37 | 6D | 8D | D5 | 4E | A9 | 6C | 56 | F4 | EA | 65 | 7A | AE | 08 |
| | **C** | BA | 78 | 25 | 2E | 1C | A6 | B4 | C6 | E8 | DD | 74 | 1F | 4D | BD | 8B | 8A |
| | **D** | 70 | 3E | B5 | 66 | 48 | 03 | F6 | 0E | 61 | 35 | 57 | B9 | 86 | C1 | 1D | 9E |
| | **E** | E1 | F8 | 98 | 11 | 69 | D9 | 8E | 94 | 9B | 1E | 87 | E9 | CE | 55 | 28 | DF |
| | **F** | 8C | A1 | 89 | 0D | BF | E6 | 42 | 68 | 41 | 99 | 2D | 0F | B0 | 54 | BB | 16 |

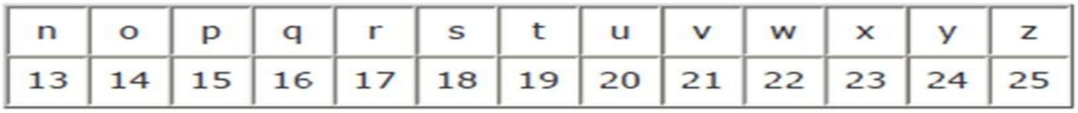
8. Alice and Bob use the Diffie–Hellman key exchange technique with a common prime q = 29 and a primitive root a = 10.
i. If Alice has a private key ${}_A$ = 15, find his public key ${}_A$.
Xii. If Bob has a private key ${}_B$ ¥27, find his public key ${}_B$.
Xiii. Find the shared secret key Ybetween Alice and Bob?

9. Use the RSA algorithm to find n, ϕ(n), d if p=107, q=113, e=13 and Encrypt the message “this is tough” using 00 to 25 for letters A to Z and 26 for the space and also decrypt it.

10. Encrypt the plaintext "SECRET" using the Vigenère cipher with the key "CODE". Refer the following table for this question.



| a | b | c | d | e | f | g | h | i | j | k | l | m |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |



| n | o | p | q | r | s | t | u | v | w | x | y | z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |