MATH 4161 Mathematics of Cryptography **Assignment 8.5**
BONUS JOE TRAN

Question 1. Given the ciphertext YRHOZMMVGZJRKJQ.Y?CX.GHKNQKMFZNFBAMVBYTJNM NZQNUDUWBWOXX.DXAXFBZKAKFXVDGHPMGV.USAVYNSLRIDAFUVFGFLUKEEKT.O and the first letters of the plaintext are shene verth ought shedb, determine the key and its inverse, and determine the plaintext of the rest of the characters.

Solution. Use this link `https://www.dcode.fr/matrix-inverse` to calculate inverse of a matrix with modulo.

Recall that we have the numerical representation of each letter given as follows:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	.	!	?
⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28

We first seek a key of the form $A = \begin{bmatrix} x_{11} & x_{12} & x_{13} & x_{14} \\ x_{21} & x_{22} & x_{23} & x_{24} \\ x_{31} & x_{32} & x_{33} & x_{44} \\ x_{41} & x_{42} & x_{43} & x_{44} \end{bmatrix}$, where each $x_{ij} \in \mathbb{Z}_{29}$. Since the first 16 letters of the ciphertext YRHOZMMVGZJRKJQ. corresponds to the numerical values 24-17-7-14-25-12-12-21-6-25-9-17-10-9-16-26 and the plaintext SHENEVERTHOUGHTS corresponds to the numerical values 18-7-4-13-4-21-4-17-19-7-14-20-6-7-19-18, then we have

$$\begin{bmatrix} x_{11} & x_{12} & x_{13} & x_{14} \\ x_{21} & x_{22} & x_{23} & x_{24} \\ x_{31} & x_{32} & x_{33} & x_{44} \\ x_{41} & x_{42} & x_{43} & x_{44} \end{bmatrix} \begin{bmatrix} 18 & 4 & 19 & 6 \\ 7 & 21 & 7 & 7 \\ 4 & 4 & 14 & 19 \\ 13 & 17 & 20 & 18 \end{bmatrix} = \begin{bmatrix} 24 & 25 & 6 & 10 \\ 17 & 12 & 25 & 9 \\ 7 & 12 & 9 & 16 \\ 14 & 21 & 17 & 26 \end{bmatrix}$$

$$\begin{bmatrix} x_{11} & x_{12} & x_{13} & x_{14} \\ x_{21} & x_{22} & x_{23} & x_{24} \\ x_{31} & x_{32} & x_{33} & x_{44} \\ x_{41} & x_{42} & x_{43} & x_{44} \end{bmatrix} = \begin{bmatrix} 24 & 25 & 6 & 10 \\ 17 & 12 & 25 & 9 \\ 7 & 12 & 9 & 16 \\ 14 & 21 & 17 & 26 \end{bmatrix} \begin{bmatrix} 18 & 4 & 19 & 6 \\ 7 & 21 & 7 & 7 \\ 4 & 4 & 14 & 19 \\ 13 & 17 & 20 & 18 \end{bmatrix}^{-1}$$

$$= \begin{bmatrix} 24 & 25 & 6 & 10 \\ 17 & 12 & 25 & 9 \\ 7 & 12 & 9 & 16 \\ 14 & 21 & 17 & 26 \end{bmatrix} \begin{bmatrix} 28 & 12 & 11 & 5 \\ 26 & 17 & 2 & 10 \\ 0 & 18 & 21 & 24 \\ 10 & 2 & 20 & 28 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 0 & 2 & 11 \\ 8 & 6 & 17 & 13 \\ 1 & 18 & 1 & 7 \\ 9 & 13 & 0 & 24 \end{bmatrix}$$

Now given the matrix A, we need to find A^{-1}. Indeed,

$$\begin{bmatrix} 1 & 0 & 2 & 11 \\ 8 & 6 & 17 & 13 \\ 1 & 18 & 1 & 7 \\ 9 & 13 & 0 & 24 \end{bmatrix}^{-1} = \begin{bmatrix} 25 & 5 & 10 & 24 \\ 24 & 19 & 6 & 12 \\ 15 & 4 & 19 & 12 \\ 3 & 12 & 22 & 22 \end{bmatrix}$$

Therefore, the deciphering key is $\begin{bmatrix} 25 & 5 & 10 & 24 \\ 24 & 19 & 6 & 12 \\ 15 & 4 & 19 & 12 \\ 3 & 12 & 22 & 22 \end{bmatrix}$. To verify, see that

$$\begin{bmatrix} 25 & 5 & 10 & 24 \\ 24 & 19 & 6 & 12 \\ 15 & 4 & 19 & 12 \\ 3 & 12 & 22 & 22 \end{bmatrix} \begin{bmatrix} 24 \\ 17 \\ 7 \\ 14 \end{bmatrix} = \begin{bmatrix} 18 \\ 7 \\ 4 \\ 13 \end{bmatrix} = \begin{bmatrix} S \\ H \\ E \\ N \end{bmatrix}$$

Let B_1, B_2 be the matrices given by

$$B_1 = \begin{bmatrix} 24 & 25 & 6 & 10 & 24 & 26 & 13 & 5 & 1 & 1 & 13 & 16 & 20 \\ 17 & 12 & 25 & 9 & 28 & 6 & 16 & 25 & 0 & 24 & 12 & 13 & 22 \\ 7 & 12 & 9 & 16 & 2 & 7 & 10 & 13 & 12 & 19 & 13 & 20 & 1 \\ 14 & 21 & 17 & 26 & 23 & 10 & 12 & 5 & 21 & 9 & 25 & 3 & 22 \end{bmatrix}$$

$$B_2 = \begin{bmatrix} 14 & 3 & 5 & 0 & 21 & 15 & 26 & 21 & 11 & 0 & 5 & 20 & 10 \\ 23 & 23 & 1 & 10 & 3 & 12 & 20 & 24 & 17 & 5 & 6 & 10 & 19 \\ 23 & 0 & 25 & 5 & 6 & 6 & 18 & 13 & 8 & 20 & 5 & 4 & 26 \\ 26 & 23 & 10 & 23 & 7 & 21 & 0 & 18 & 3 & 3 & 11 & 4 & 14 \end{bmatrix}$$

So doing the matrix multiplication separately,

$$AB_1 = \begin{bmatrix} 25 & 5 & 10 & 24 \\ 24 & 19 & 6 & 12 \\ 15 & 4 & 19 & 12 \\ 3 & 12 & 22 & 22 \end{bmatrix} \begin{bmatrix} 24 & 25 & 6 & 10 & 24 & 26 & 13 & 5 & 1 & 1 & 13 & 16 & 20 \\ 17 & 12 & 25 & 9 & 28 & 6 & 16 & 25 & 0 & 24 & 12 & 13 & 22 \\ 7 & 12 & 9 & 16 & 2 & 7 & 10 & 13 & 12 & 19 & 13 & 20 & 1 \\ 14 & 21 & 17 & 26 & 23 & 10 & 12 & 5 & 21 & 9 & 25 & 3 & 22 \end{bmatrix}$$

$$= \begin{bmatrix} 18 & 4 & 19 & 6 & 7 & 4 & 10 & 7 & 11 & 0 & 13 & 12 & 17 \\ 7 & 21 & 7 & 7 & 4 & 1 & 8 & 8 & 0 & 6 & 19 & 4 & 8 \\ 4 & 4 & 14 & 19 & 3 & 0 & 13 & 18 & 2 & 0 & 7 & 12 & 4 \\ 13 & 17 & 20 & 18 & 1 & 2 & 19 & 15 & 4 & 8 & 4 & 14 & 18 \end{bmatrix}$$

$$= \begin{bmatrix} S & E & T & G & H & E & K & H & L & A & N & M & R \\ H & V & H & H & E & B & I & I & A & G & T & E & I \\ E & E & O & T & D & A & N & S & C & A & H & M & E \\ N & R & U & S & B & C & T & P & E & I & E & O & S \end{bmatrix}$$

So the first part of the plaintext gives: SHE NEVER THOUGHT SHE'D BE BACK IN THIS PLACE AGAIN THE MEMORIES. Similarly, doing the matrix multiplication for A and B_2,

$$AB_2 = \begin{bmatrix} 25 & 5 & 10 & 24 \\ 24 & 19 & 6 & 12 \\ 15 & 4 & 19 & 12 \\ 3 & 12 & 22 & 22 \end{bmatrix} \begin{bmatrix} 14 & 3 & 5 & 0 & 21 & 15 & 26 & 21 & 11 & 0 & 5 & 20 & 10 \\ 23 & 23 & 1 & 10 & 3 & 12 & 20 & 24 & 17 & 5 & 6 & 10 & 19 \\ 23 & 0 & 25 & 5 & 6 & 6 & 18 & 13 & 8 & 20 & 5 & 4 & 26 \\ 26 & 23 & 10 & 23 & 7 & 21 & 0 & 18 & 3 & 21 & 11 & 4 & 14 \end{bmatrix}$$

$$= \begin{bmatrix} 14 & 17 & 11 & 14 & 14 & 13 & 2 & 18 & 19 & 4 & 5 & 19 & 13 \\ 5 & 2 & 3 & 3 & 14 & 6 & 10 & 7 & 4 & 3 & 19 & 17 & 26 \\ 7 & 7 & 7 & 5 & 3 & 1 & 0 & 4 & 15 & 14 & 7 & 0 & 18 \\ 4 & 8 & 14 & 11 & 8 & 0 & 18 & 18 & 15 & 5 & 4 & 8 & 7 \end{bmatrix}$$

$$= \begin{bmatrix} O & R & L & O & O & N & C & S & T & E & F & T & N \\ F & C & D & D & O & G & K & H & E & D & T & R & . \\ H & H & H & F & D & B & A & E & P & O & H & A & S \\ E & I & O & L & I & A & S & S & P & F & E & I & H \end{bmatrix}$$

which then gives OF HER CHILDHOOD FLOODING BACK AS SHE STEPPED OFF THE TRAIN. SH

Therefore, the plaintext is: She never thought she'd be back in this place again the memories of her childhood flooding back as she stepped off the train. with extra letters sh.