MATH 4161 Mathematics of Cryptography **Assignment 8**
ASSIGNMENT JOE TRAN

Question 1. Assume that you know that the word of the ciphertext ZQ!G corresponds to the plaintext PICK. Determine what (four letter English word) corresponds to the ciphertext: KVLW, and determine the key.

Solution. 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	.	!	?
$\Downarrow$	$\Downarrow$	$\Downarrow$	$\Downarrow$	$\Downarrow$	$\Downarrow$	$\Downarrow$	$\Downarrow$	$\Downarrow$	$\Downarrow$	$\Downarrow$	$\Downarrow$	$\Downarrow$	$\Downarrow$	$\Downarrow$	$\Downarrow$	$\Downarrow$	$\Downarrow$	$\Downarrow$	$\Downarrow$	$\Downarrow$	$\Downarrow$	$\Downarrow$	$\Downarrow$	$\Downarrow$	$\Downarrow$	$\Downarrow$	$\Downarrow$	$\Downarrow$
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 $k = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, where $a, b, c, d \in \mathbb{Z}_{29}$. Since the ciphertext ZQ!G corresponds to the numerical value 25-16-27-6 and the plaintext PICK corresponds to the numerical value 15-8-2-10, then we have that

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 15 \\ 8 \end{bmatrix} = \begin{bmatrix} 25 \\ 16 \end{bmatrix}$$

and

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 2 \\ 10 \end{bmatrix} = \begin{bmatrix} 27 \\ 6 \end{bmatrix}$$

Or in other words,

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 15 & 2 \\ 8 & 10 \end{bmatrix} = \begin{bmatrix} 25 & 27 \\ 16 & 6 \end{bmatrix}$$

So now right multiplying $\begin{bmatrix} 15 & 2 \\ 8 & 10 \end{bmatrix}^{-1}$ yields

$$\begin{aligned}
\begin{bmatrix} a & b \\ c & d \end{bmatrix} &= \begin{bmatrix} 25 & 27 \\ 16 & 6 \end{bmatrix} \begin{bmatrix} 15 & 2 \\ 8 & 10 \end{bmatrix}^{-1} \\
&= \begin{bmatrix} 25 & 27 \\ 16 & 6 \end{bmatrix} (134 \bmod 29)^{-1} \begin{bmatrix} 10 & -2 \\ -8 & 15 \end{bmatrix} \\
&= \begin{bmatrix} 25 & 27 \\ 16 & 6 \end{bmatrix} 18^{-1} \begin{bmatrix} 10 & 27 \\ 21 & 15 \end{bmatrix}
\end{aligned}$$

Now note that because $\gcd(18, 29) = 1$, then by Bezout's Theorem, there exists $x, y \in \mathbb{Z}$ such that

$$18x + 29y = 1$$

In particular, $x = -8$ and $y = 5$ so that

$$18(-8) + 29(5) = 1$$

so $-8 \equiv 21$ is the inverse of 18. Now,

$$\begin{aligned}
\begin{bmatrix} a & b \\ c & d \end{bmatrix} &= \begin{bmatrix} 25 & 27 \\ 16 & 6 \end{bmatrix} 21 \begin{bmatrix} 10 & 27 \\ 21 & 15 \end{bmatrix} \\
&= \begin{bmatrix} 25 & 27 \\ 16 & 6 \end{bmatrix} \begin{bmatrix} 7 & 16 \\ 6 & 25 \end{bmatrix} \\
&= \begin{bmatrix} 18 & 2 \\ 3 & 0 \end{bmatrix}
\end{aligned}$$

So now we check that the key that we have obtained is correct. Indeed,

$$\begin{bmatrix} 18 & 2 \\ 3 & 0 \end{bmatrix} \begin{bmatrix} 15 \\ 8 \end{bmatrix} = \begin{bmatrix} 25 \\ 16 \end{bmatrix}$$

and also,

$$\begin{bmatrix} 18 & 2 \\ 3 & 0 \end{bmatrix} \begin{bmatrix} 2 \\ 10 \end{bmatrix} = \begin{bmatrix} 27 \\ 6 \end{bmatrix}$$

as desired. So from here, our keyword is 18-2-3-0, which translates to SCDA. Finally, we now need to determine what KVLW is in plaintext, given our key. So, the ciphertext KVLW in numerical form is 10-21-11-22, so there exists $x, y, z, w \in \mathbb{Z}_{29}$ such that

$$\begin{bmatrix} 18 & 2 \\ 3 & 0 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} 10 \\ 21 \end{bmatrix}$$

and

$$\begin{bmatrix} 18 & 2 \\ 3 & 0 \end{bmatrix} \begin{bmatrix} y_1 \\ y_2 \end{bmatrix} = \begin{bmatrix} 11 \\ 22 \end{bmatrix}$$

In particular, $\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} 7 \\ 0 \end{bmatrix}$ and $\begin{bmatrix} y_1 \\ y_2 \end{bmatrix} = \begin{bmatrix} 22/3 \\ 53/2 \end{bmatrix}$. Now we just need to compute the values $22 \cdot 3^{-1} \bmod 29$ and $53 \cdot 2^{-1} \bmod 29$. Since $\gcd(3, 29) = 1$ and $\gcd(2, 29) = 1$, then by Bezout's Theorem, there exists $k, \ell, m, n \in \mathbb{Z}$ such that

$$3k + 29\ell = 1$$

and

$$2m + 29n = 1$$

In particular, $k = 10$, $\ell = -1$, $m = -14$ and $n = 1$. So 10 is the inverse of 3, and $-14 \equiv 15$ is the inverse of 2. Now,

$$22 \cdot 3^{-1} \bmod 29 = 22 \cdot 10 \bmod 29 = 17$$

and

$$53 \cdot 2^{-1} \bmod 29 = 53 \cdot 15 \bmod 29 = 12$$

So $\begin{bmatrix} y_1 \\ y_2 \end{bmatrix} = \begin{bmatrix} 17 \\ 12 \end{bmatrix}$. Note that now $\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} 7 \\ 0 \end{bmatrix} = \begin{bmatrix} H \\ A \end{bmatrix}$ and $\begin{bmatrix} y_1 \\ y_2 \end{bmatrix} = \begin{bmatrix} 17 \\ 12 \end{bmatrix} = \begin{bmatrix} R \\ M \end{bmatrix}$.

To find the decrypting key, we need to find the inverse of the key. Indeed,

$$\begin{aligned} \begin{bmatrix} 18 & 2 \\ 3 & 0 \end{bmatrix}^{-1} &= (18 \cdot 0 - 3 \cdot 2)^{-1} \begin{bmatrix} 0 & -2 \\ -3 & 18 \end{bmatrix} \\ &= (-6)^{-1} \begin{bmatrix} 0 & -2 \\ -3 & 18 \end{bmatrix} \\ &= 23^{-1} \begin{bmatrix} 0 & -2 \\ -3 & 18 \end{bmatrix} \end{aligned}$$

Since $\gcd(23, 29) = 1$, then there exists $\delta, \varepsilon \in \mathbb{Z}$ such that

$$23\delta + 29\varepsilon = 1$$

In particular, $\delta = -5$ and $\varepsilon = 4$, so the inverse of 23 is $-5 \equiv 24$. So then,

$$\begin{aligned}\begin{bmatrix} 18 & 2 \\ 3 & 0 \end{bmatrix}^{-1} &= 24 \begin{bmatrix} 0 & -2 \\ -3 & 18 \end{bmatrix} \\ &= \begin{bmatrix} 0 & 10 \\ 15 & 26 \end{bmatrix}\end{aligned}$$

To check that we have the deciphering key, observe that

$$\begin{bmatrix} 0 & 10 \\ 15 & 26 \end{bmatrix} \begin{bmatrix} 10 \\ 21 \end{bmatrix} = \begin{bmatrix} 7 \\ 0 \end{bmatrix}$$

and

$$\begin{bmatrix} 0 & 10 \\ 15 & 26 \end{bmatrix} \begin{bmatrix} 11 \\ 22 \end{bmatrix} = \begin{bmatrix} 17 \\ 12 \end{bmatrix}$$

as required.

To conclude:

- Plaintext of KVLW: HARM
- Enciphering Key: $\begin{bmatrix} 18 & 2 \\ 3 & 0 \end{bmatrix}$
- Deciphering Key: $\begin{bmatrix} 0 & 10 \\ 15 & 26 \end{bmatrix}$