MATH 4161 Mathematics of Cryptography **Assignment 7**
ASSIGNMENT JOE TRAN

Question 1. Given the beginning of the message HOWCA NYO... and this corresponds to the first 8 letters of the ciphertext:

RGHNY GDGCM OZSNC YUQQJ DZTYR AJKVV CRDCF BFRLF PJPDF IWAVA Y

The ciphertext was encrypted by the Vernam two-tape system such the sum of the lengths of the two keys minus 1 is equal to 8. Determine the plaintext.

Solution. First, note that since the sum of the lengths of the two keys minus 1 is 8, so if x represents the length of the first key and y represents the length of the second key, then

x	y	xy
1	8	8
2	7	14
3	6	18
4	5	20

So we see here that having length 4 and length 5 for the first and second key, respectively seems candidable.

Recall the values of of the letters given by the following table:

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

Let us consider the first 20 letters of the ciphertext. Let $x = (x_1, x_2, x_3, x_4)$ and $y = (y_1, y_2, y_3, y_4, y_5)$. Then

R	G	H	N	Y	G	D	G	C	M	O	Z	S	N	C	Y	U	Q	Q	J
17	6	7	13	24	6	3	6	2	12	14	25	18	13	2	24	20	16	16	9
x_1	x_2	x_3	x_4	x_1	x_2	x_3	x_4	x_1	x_2	x_3	x_4	x_1	x_2	x_3	x_4	x_1	x_2	x_3	x_4
y_1	y_2	y_3	y_4	y_5	y_1	y_2	y_3	y_4	y_5	y_1	y_2	y_3	y_4	y_5	y_1	y_2	y_3	y_4	y_5
7	14	22	2	0	13	24	14												
H	O	W	C	A	N	Y	O												

Without loss of generality, let us assume that $x_1 = 0$. Then the table above becomes

R	G	H	N	Y	G	D	G	C	M	O	Z	S	N	C	Y	U	Q	Q	J
17	6	7	13	24	6	3	6	2	12	14	25	18	13	2	24	20	16	16	9
x_1	x_2	x_3	x_4	x_1	x_2	x_3	x_4	x_1	x_2	x_3	x_4	x_1	x_2	x_3	x_4	x_1	x_2	x_3	x_4
0				0				0				0				0			
y_1	y_2	y_3	y_4	y_5	y_1	y_2	y_3	y_4	y_5	y_1	y_2	y_3	y_4	y_5	y_1	y_2	y_3	y_4	y_5
7	14	22	2	0	13	24	14												
H	O	W	C	A	N	Y	O												

To find the other values in the table, we need to use the formula:

$$\text{plaintext number} + x_i + y_j = \text{ciphertext number mod } 26 \qquad (*)$$

For example, if we want to find y_1, since the plaintext number of H is 7, x_1 is 0, and ciphertext number of R is 17, then

$$\begin{aligned} 7 + 0 + y_1 &= 17 \bmod 26 \\ y_1 &= 10 \bmod 26 \\ y_1 &= 10 \end{aligned}$$

and so every y_1 in the above table is now 10. So

R	G	H	N	Y	G	D	G	C	M	O	Z	S	N	C	Y	U	Q	Q	J
17	6	7	13	24	6	3	6	2	12	14	25	18	13	2	24	20	16	16	9
x_1	x_2	x_3	x_4	x_1	x_2	x_3	x_4	x_1	x_2	x_3	x_4	x_1	x_2	x_3	x_4	x_1	x_2	x_3	x_4
0				0				0				0				0			
y_1	y_2	y_3	y_4	y_5	y_1	y_2	y_3	y_4	y_5	y_1	y_2	y_3	y_4	y_5	y_1	y_2	y_3	y_4	y_5
10					10					10					10				
7	14	22	2	0	13	24	14												
H	O	W	C	A	N	Y	O												

Now let us have a look for x_2 on the 6th position. Since the plaintext number is 13, $y_1 = 10$, and ciphertext number is 6, and so

$$\begin{aligned} 13 + x_2 + 10 &= 6 \bmod 26 \\ x_2 &= -17 \bmod 26 \\ x_2 &= 9 \end{aligned}$$

and therefore, updating the table gives us

R	G	H	N	Y	G	D	G	C	M	O	Z	S	N	C	Y	U	Q	Q	J
17	6	7	13	24	6	3	6	2	12	14	25	18	13	2	24	20	16	16	9
x_1	x_2	x_3	x_4	x_1	x_2	x_3	x_4	x_1	x_2	x_3	x_4	x_1	x_2	x_3	x_4	x_1	x_2	x_3	x_4
0	9			0	9			0	9			0	9			0	9		
y_1	y_2	y_3	y_4	y_5	y_1	y_2	y_3	y_4	y_5	y_1	y_2	y_3	y_4	y_5	y_1	y_2	y_3	y_4	y_5
10					10					10					10				
7	14	22	2	0	13	24	14												
H	O	W	C	A	N	Y	O												

Now let us have a look at y_2 on the 2nd position. Since the plaintext number is 14, $x_1 = 9$ and the ciphertext number is 6, then

$$\begin{aligned} 14 + 9 + y_2 &= 6 \bmod 26 \\ y_2 &= 9 \end{aligned}$$

So updating the table,

R	G	H	N	Y	G	D	G	C	M	O	Z	S	N	C	Y	U	Q	Q	J
17	6	7	13	24	6	3	6	2	12	14	25	18	13	2	24	20	16	16	9
x_1	x_2	x_3	x_4	x_1	x_2	x_3	x_4	x_1	x_2	x_3	x_4	x_1	x_2	x_3	x_4	x_1	x_2	x_3	x_4
0	9			0	9			0	9			0	9			0	9		
y_1	y_2	y_3	y_4	y_5	y_1	y_2	y_3	y_4	y_5	y_1	y_2	y_3	y_4	y_5	y_1	y_2	y_3	y_4	y_5
10	9				10	9				10	9				10	9			
7	14	22	2	0	13	24	14												
H	O	W	C	A	N	Y	O												

Then by repeating the same process until we fill all of the numbers,

R	G	H	N	Y	G	D	G	C	M	O	Z	S	N	C	Y	U	Q	Q	J
17	6	7	13	24	6	3	6	2	12	14	25	18	13	2	24	20	16	16	9
x_1	x_2	x_3	x_4	x_1	x_2	x_3	x_4	x_1	x_2	x_3	x_4	x_1	x_2	x_3	x_4	x_1	x_2	x_3	x_4
0	9	22	3	0	9	22	3	0	9	22	3	0	9	22	3	0	9	22	3
y_1	y_2	y_3	y_4	y_5	y_1	y_2	y_3	y_4	y_5	y_1	y_2	y_3	y_4	y_5	y_1	y_2	y_3	y_4	y_5
10	9	15	8	24	10	9	15	8	24	10	9	15	8	24	10	9	15	8	24
7	14	22	2	0	13	24	14												
H	O	W	C	A	N	Y	O												

And thus, $x = (0, 9, 22, 3)$ and $y = (10, 9, 15, 8, 24)$ are our keys.

Now using (*), our goal is to find the plaintext from the ciphertext, so for the remainder of the assignment, we need to compute all

$$\text{plaintext number} = \text{ciphertext number} - x_i - y_i \bmod 26$$

For example, for the 9th position's letter, we have ciphertext number 2, $x_1 = 0$ and $y_4 = 8$. So then

$$\text{plaintext number} = 2 - 0 - 8 = -6 \bmod 26 = 20$$

and 20 in the plaintext corresponds to U.

Similarly, for the 10th position's letter, we have ciphertext number 12, $x_2 = 9$ and $y_5 = 24$, so

$$\text{plaintext number} = 12 - 9 - 24 = -21 \bmod 26 = 5$$

and 5 in the plaintext corresponds to F.

By doing the same for the remaining of the letters, we should be able to obtain the plaintext:

How can you find Will Smith in the snow following the fresh prints