MATH 4161 Mathematics of Cryptography **Assignment 4**
ASSIGNMENT JOE TRAN

Question 1. Given the ciphertext RB BL RP ST AP VY GY XC TX CA ZA GO BE YD QG IC CF ZM WL WH DK PL ST UW DK RC OQ AW and given the partial key

O	X	F	V	M
Y	K	W	*	N
*	T	R	L	*
Q	B	*	A	*
S	I	P	D	G

where * means that there is a letter that you have to fill in. Determine the plaintext and determine the key.

Solution. First note that the key is missing the following letters: C, E, H, U, and Z. Using the above table, we can find part of the plaintext as follows:

R	B	B	L	R	P	S	T	A	P	V	Y	G	Y	X	C	T	X	C	A
T	*	A	T	W	*	I	*	*	D	O	*	S	N	•	•	K	I	•	•

Z	A	G	O	B	E	Y	D	Q	G	I	C	C	F	Z	M	W	L	W	H
•	•	S	M	•	•	*	S	*	S	•	•	•	•	•	•	*	R	•	•

D	K	P	L	S	T	U	W	D	K	R	C	O	Q	A	W
I	*	D	R	I	*	•	•	I	*	•	•	S	*	*	*

where • denotes the letter that cannot be determined at the moment.

First observe the first four letters T*AT. One of the letters that can be used in this case is H, and so the fourth row then becomes

Q	B	H	A	*

making the first four letters THAT. Then filling out what we have,

R	B	B	L	R	P	S	T	A	P	V	Y	G	Y	X	C	T	X	C	A
T	H	A	T	W	H	I	*	H	D	O	*	S	N	•	•	K	I	•	•

Z	A	G	O	B	E	Y	D	Q	G	I	C	C	F	Z	M	W	L	W	H
•	•	S	M	•	•	*	S	*	S	•	•	•	•	•	•	*	R	F	R

D	K	P	L	S	T	U	W	D	K	R	C	O	Q	A	W
I	*	D	R	I	*	•	•	I	*	•	•	S	*	H	*

Next, observe the next five letters after THAT, WHI*H. One of the letters that can be used in this case is C, and so the third row becomes

C	T	R	L	*

making the five letters WHICH. Then filling out what we have,

R	B	B	L	R	P	S	T	A	P	V	Y	G	Y	X	C	T	X	C	A
T	H	A	T	W	H	I	C	H	D	O	*	S	N	O	T	K	I	L	Q

Z	A	G	O	B	E	Y	D	Q	G	I	C	C	F	Z	M	W	L	W	H
•	•	S	M	•	•	*	S	*	S	S	T	R	O	•	•	*	R	F	R

D	K	P	L	S	T	U	W	D	K	R	C	O	Q	A	W
I	*	D	R	I	C	•	•	I	*	•	•	S	C	H	*

Next, observe the two 3-grams WH, DK and PL, FRI*DR. Ignoring the last R for the moment, one of the letters that we can use in this situation is E, and so making the second row

Y	K	W	E	N

and thus, we have FRIEDR. Then filling what we can,

R	B	B	L	R	P	S	T	A	P	V	Y	G	Y	X	C	T	X	C	A
T	H	A	T	W	H	I	C	H	D	O	E	S	N	O	T	K	I	L	Q

Z	A	G	O	B	E	Y	D	Q	G	I	C	C	F	Z	M	W	L	W	H
•	•	S	M	A	K	E	S	*	S	S	T	R	O	•	•	E	R	F	R

D	K	P	L	S	T	U	W	D	K	R	C	O	Q	A	W
I	E	D	R	I	C	•	•	I	E	T	*	S	C	H	E

Now, observe the 2-gram QG. One of the letters that can be used in this case is U, so the fourth row becomes

Q	B	H	A	U

making the 2-gram US in plaintext. So now,

R	B	B	L	R	P	S	T	A	P	V	Y	G	Y	X	C	T	X	C	A
T	H	A	T	W	H	I	C	H	D	O	E	S	N	O	T	K	I	L	Q

Z	A	G	O	B	E	Y	D	Q	G	I	C	C	F	Z	M	W	L	W	H
*	U	S	M	A	K	E	S	U	S	S	T	R	O	•	•	E	R	F	R

D	K	P	L	S	T	U	W	D	K	R	C	O	Q	A	W
I	E	D	R	I	C	H	N	I	E	T	*	S	C	H	E

Lastly, it follows that the last remaining letter is Z, which belongs to the third row

C	T	R	L	Z

So now,

R	B	B	L	R	P	S	T	A	P	V	Y	G	Y	X	C	T	X	C	A
T	H	A	T	W	H	I	C	H	D	O	E	S	N	O	T	K	I	L	Q

Z	A	G	O	B	E	Y	D	Q	G	I	C	C	F	Z	M	W	L	W	H
L	U	S	M	A	K	E	S	U	S	S	T	R	O	N	G	E	R	F	R

D	K	P	L	S	T	U	W	D	K	R	C	O	Q	A	W
I	E	D	R	I	C	H	N	I	E	T	Z	S	C	H	E

Therefore, the plaintext is That which does not kill us makes us stronger Friedrich Nietzsche and the key is the table given by

O	X	F	V	M
Y	K	W	E	N
C	T	R	L	Z
Q	B	H	A	U
S	I	P	D	G