MATH 4161 Mathematics of Cryptography **Assignment 2**
ASSIGNMENT JOE TRAN

Question 1. Given the ciphertext UWHRA DRVBI VPQVG MHGBY OBBTP ZLMJO, and given that

(1) The length of the key is 4.
(2) The 13th letter is U.
(3) The 22nd letter is T.
(4) The 24th letter is P.

Decipher the text into plaintext, and determine the keyword.

Solution. Because the length of the key is 4, then we will rewrite the ciphertext as

UWHR ADRV BIVP QVGM HGBY OBBT PZLM JO

Because the 13th letter is U, then we know that $Q \mapsto U$, so by the Vigenere square, this means that $Q + W = U$. So W is part of the keyword. Then, we have the row of letters corresponding to row W given by

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

and as we see from the table, $Q \mapsto U$, which corresponds to row W. This also means that, W is our first letter of the keyword.

Next, because the 22nd letter is T, then we know that $B \mapsto T$, so by the Vigenere square, this means that $B + I = T$, so I is part of the keyword. Then we have the row of letters corresponding to row I 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
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H

as we see from the table, $B \mapsto T$, which corresponds to row I. This also means that I is our second letter of the keyword.

Next, since the 24th letter is P, then we know that $T \mapsto P$, so by the Vigenere square, this means that $T + E = P$. So P is part of the keyword. Then we have the row of letters corresponding to row E 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
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D

and as we see from the table, $T \mapsto P$, which corresponds to row E. Furthermore, E is the last letter of our keyword.

So our key up to this point is $WIxE$, where x is the missing letter we require. Now with the given tables above, let us transform the ciphertext to what we can so far.

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

At this stage, we can start to see the string that is appearing from the keyword that we have formed. We now conjecture that the third letter is U, meaning that $H \mapsto U$, so by the Vigenere sqaure, this means that $H + N = U$, so N is part of the keyword. Then we have the row of letters corresponding to row N 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
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M

Finishing the above table,

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

Therefore, our plaintext is YOUN EVER FAIL UNTI LYOU STOP TRYI NG and our key is WINE.