Cryptanalysis of Vigenere Cipher

Ciphertext:

WSPGM HHEHM CMTGP NROVX WISCQ TXHKR VESQT IMMKW BMTKW CSTVL TGOPZ XGTKS CXHCX HSMGX WMNIA XPLVY GROWX LILNF JXTJI RIRVE XRTAX WETUS BITJM CKMCO TWSGR HIRGK PVDNI HWOHL DAIVX JVNUS JX

Keyword: five-letters legal English word

Cryptanalysis – finding a key:

Step 1:

Let's utilize the Python program, which is designed specifically for splitting the given ciphertext into groups, depending on the key size. This script also calculates the frequency of all letters in the groups, sorting the sequences by their frequency (sort order – *descending*), which will also be useful to determine the letters to detect the possible keyword by.

The program splits the given ciphertext to the following five groups:

1: CHWJTXBDGILNPRV
2: IMXRSEGVWAHKP
3: TOMSHLNRDEIP
4: GVKCHJNUAIPQW
5: XMSILRWAEFKOPQTYZ

In this case, left-most letter of each sequence is the most frequent one. The frequencies of the letters will be displayed in the table below. Only most frequent letters' values will be included, less frequent ones will be omitted.

Set 1	Freq.	Set 2	Freq.	Set 3	Freq.	Set 4	Freq.	Set 5	Freq.
C	4	I	5	T	8	G	5	X	6

Step 2:

Most frequent letters in Sets 1, 2, 3, 4, 5 are C, I, T, G, X respectively.

Let's check them against the most popular letters in English alphabet: E, T, N, O, R, I, A, S, which will be taken as possible plaintext options. Next, every combination of plaintext and ciphertext letters will be checked via Vigener table.

Most frequent letter in the Set 1 is C:

Ciphertext letter	Possible plaintext letter	Corresponded key-word letter **Possible first letter of the keyword**
C	E	Y
C	T	J
C	N	P
C	O	O
C	R	L
C	I	U
C	A	C
C	S	K

Most frequent letter in the Set 2 is I:

Ciphertext letter	Possible plaintext letter	Corresponded key-word letter Possible second letter of the keyword
I	E	E
I	T	P
I	N	V
I	O	U
I	R	R
I	I	A
I	A	I
I	S	Q

Most frequent letter in the Set 3 is T:

Ciphertext letter	Possible plaintext letter	Corresponded key-word letter Possible third letter of the keyword
T	E	P
T	T	A
T	N	G
T	O	F
T	R	C
T	I	L
T	A	T
T	S	B

Most frequent letter in Set 4 is G:

Ciphertext letter	Possible plaintext letter	Corresponded key-word letter Possible fourth letter of the keyword
G	E	C
G	T	N
G	N	T
G	O	S
G	R	P
G	I	Y
G	A	G
G	S	O

Most frequent letter in Set 5 is X:

Ciphertext letter	Possible plaintext letter	Corresponded key-word letter Possible fourth letter of the keyword
X	E	T
X	T	E
X	N	K
X	O	J
X	R	G
X	I	P
X	A	X
X	S	F

Step 3:
Now, let's create a table of all possible keywords by putting together the columns for the first, second, third, fourth, and fifth letters.

Corresponded key-word letter First letter	Corresponded key-word letter Second Letter	Corresponded key-word letter Third Letter	Corresponded key-word letter Fourth Letter	Corresponded key-word letter Fifth letter
Y	E	P	C	T
J	P	A	N	E
P	V	G	T	K
O	U	F	S	J
L	R	C	P	G
U	A	L	Y	P
C	I	T	G	X
K	Q	B	O	F

Step 4:
Now, let's create all possible five-letter combinations of the given letters, putting each letter from each column consequently. We're constrained by the fact that the combinations should make up legal English words.
Each word combination will be checked to see if, at least, the first words of the plaintext make sense.
Possible keywords: CEANE, CRANE, PEACE, PILOT, LEASE, CAPOT…
The answer: Deciphering the ciphertext with keyword PEACE will give a plaintext:
HOPE IS DEFINITELY NOT THE SAME THING AS OPTIMISM IT IS NOT THE CONVICTION THAT SOMETHING WILL TURN OUT WELL BUT THE CERTAINITY THAT SOMETHING MAKES SENSE REGARGLESS OF HOW IT TURNS OUT.