

MysteryTwister C3

THE CRYPTO CHALLENGE CONTEST

MODIFIED VIGENÈRE CIPHER

Author: Encrypted Puzzle

December 2021

Introduction (1/2)

The Vigenère cipher is a polyalphabetical cipher that uses a known Tabula Recta of twenty-six alphabets and a keyword.

A detailed description of the Vigenère cipher can be found at :
https://en.wikipedia.org/wiki/Vigenere_cipher

The main weakness of the Vigenère cipher is the repeating nature of the keyword. If the correct keyword length is guessed or calculated, the encrypted text can be treated as interwoven Caesar ciphers. These are easily broken individually.

Introduction (2/2)

The version of the Vigenère cipher I have devised for this challenge has been designed to increase the security of this cipher. The principle is to use mixed instead of ordered alphabets (like the monoalphabetic substitution). There is a different mixed alphabet for each key number.

The mixed alphabets are created from keywords which are taken from an easily memorized phrase.

On the following pages you can find an example, using the phrase:
Cats eat mice

Example (1/3)

The keywords for the mixed alphabets are:

CATS

EAT

MICE

Note, one and two letter words in the phrase would be ignored.

The phrase above creates three different mixed alphabets.

The Tabula Recta created is:

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

Example (2/3)

Instead of a keyword for the encryption process the alphabets are simply numbered 1, 2, 3 and the normal alphabet is placed across the top of the Tabula Recta:

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

Example (3/3)

The Plaintext is: ATTACK AT DAWN PLS

The encryption process is:

Key number	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3
Plaintext	A	T	T	A	C	K	A	T	D	A	W	N	P	L	S
Ciphertext	C	S	T	C	T	J	C	S	E	C	W	N	N	K	S

Challenge (1/2)

Your task is to decrypt the following ciphertext. The plaintext is in English.

ZKCRP	TQQNO	WYWSQ	CIKWM	JQFBT	PLSDG	QTYNH
ZMBDN	MIEBQ	JCLSL	NRJKQ	SLOEK	GEDQG	KBBSP
OYSBF	DJCNK	JYWOZ	QQYKL	RZDRT	KNNKE	

Challenge (2/2)

The solution consists of the following 3 words:

1. The last name of the subject
2. What mode of transportation is the subject using?
3. The subject's destination

Please enter the solution in uppercase letters with spaces between the words.

Example:

If the three words are 1. Smith, 2. car, 3. London
you have to enter: SMITH CAR LONDON