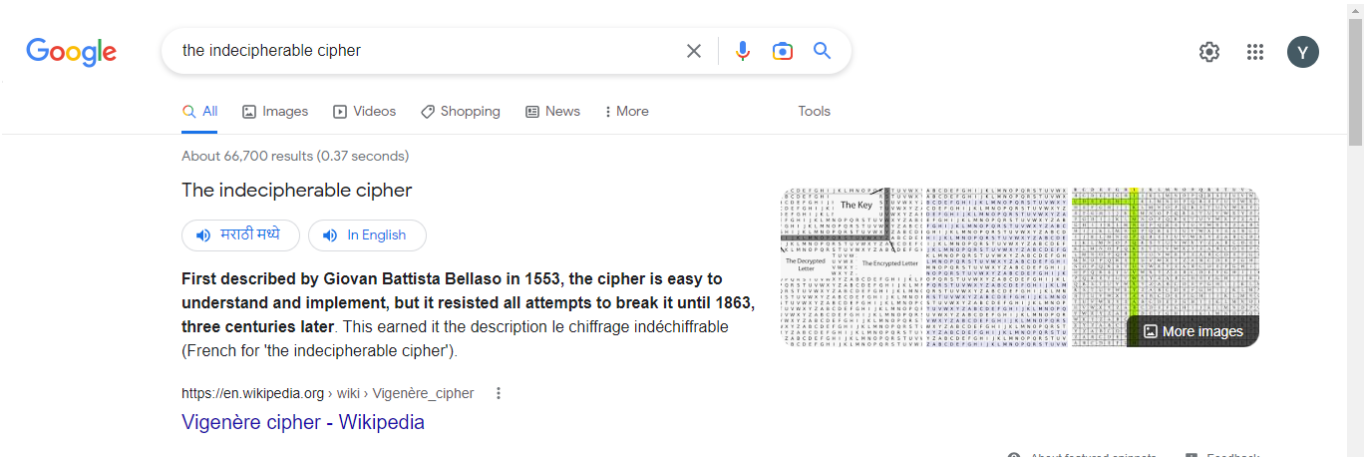
Writeup For Indicepherable Cipher

Name: Indicepherable Cipher
DescriptionOur crypto specalist Mr.Kasiski is currently anvailable, so help us decode this string
String: j3qrh4kgz3iptmyqxcw0zkm8i5xugs5lwl0lrwvirwktlqinexcw0zkmq5nqvpebpor5wqipqhw2ikzm4ipktzlr
Difficulty: Medium
Points: 295
Domain: Cryptography
Author: Yogesh Rathod

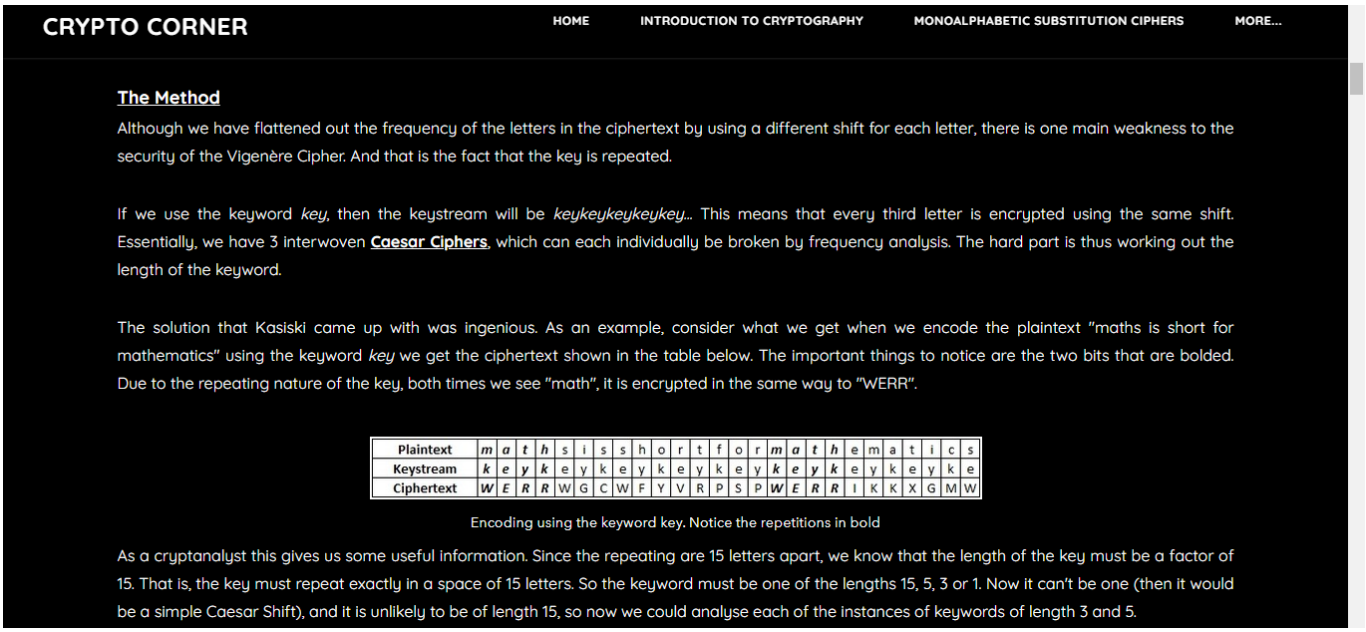
Solution:

The first thing I tried was to google the question title, that is "The indecipherable Cipher" ,and I found a wikipedia article about vigenere cipher



After reading the wikipedia page about vigenere cipher I found that it is also called as "The Indecipherable Cipher" and it is a polyalphabetic cipher and we need a key to decode the cipher. I tried to decode it using decode.fr but automatic decryption did not work and for other options to decode we need to provide a key or the length of the key to decode the string.

I tried googling again to find ways to decode vigenere cipher without a key and found this article about kasiski analysis which we can use to find the length of the key, and once we have that we can decode the string.Also the name kasiski appears in question description so we are on the right track



CRYPTO CORNER

HOME INTRODUCTION TO CRYPTOGRAPHY MONOALPHABETIC SUBSTITUTION CIPHERS MORE...

The Method

Although we have flattened out the frequency of the letters in the ciphertext by using a different shift for each letter, there is one main weakness to the security of the Vigenère Cipher. And that is the fact that the key is repeated.

If we use the keyword *key*, then the keystream will be *keykeykeykeykey...* This means that every third letter is encrypted using the same shift. Essentially, we have 3 interwoven **Caesar Ciphers**, which can each individually be broken by frequency analysis. The hard part is thus working out the length of the keyword.

The solution that Kasiski came up with was ingenious. As an example, consider what we get when we encode the plaintext "maths is short for mathematics" using the keyword *key* we get the ciphertext shown in the table below. The important things to notice are the two bits that are bolded. Due to the repeating nature of the key, both times we see "math", it is encrypted in the same way to "WERR".

Plaintext	*m*	*a*	*t*	*h*	s	i	s	s	h	o	r	t	f	o	r	*m*	*a*	*t*	*h*	e	m	a	t	i	c	s
Keystream	*k*	*e*	*y*	*k*	e	y	k	e	y	k	e	y	k	e	y	*k*	*e*	*y*	*k*	e	y	k	e	y	k	e
Ciphertext	*W*	*E*	*R*	*R*	W	G	C	W	F	Y	V	R	P	S	P	*W*	*E*	*R*	*R*	I	K	K	X	G	M	W

Encoding using the keyword key. Notice the repetitions in bold

As a cryptanalyst this gives us some useful information. Since the repeating are 15 letters apart, we know that the length of the key must be a factor of 15. That is, the key must repeat exactly in a space of 15 letters. So the keyword must be one of the lengths 15, 5, 3 or 1. Now it can't be one (then it would be a simple Caesar Shift), and it is unlikely to be of length 15, so now we could analyse each of the instances of keywords of length 3 and 5.

After reading the article I understood that we can find the length of the key used to encode the cipher by looking for substring that repeat in the cipher text and finding the distance at which they occur, The length of the key is a factor of that distance.

After analysing the cipher text I found that string "xcw0zkm" repeats and distance between its occurence is 33. So the length of the key is either 1, 11, or 33.

> j3qrh4kgz3iptmyqxcw0zkm8i5xugs5lwl0lrwvirwktlqinexcw0zkmq5nqvpebpor5wqipqhw2ikzm4ipktzlr

I also noticed that the cipher text also contains numbers, so I included them in the character set as well for decoding. I tried these lengths of key on decode.fr and found the flag for key length 11

Search for a tool

Search a tool on dCode by keywords:

e.g. type 'caesar'

Browse the full dCode tools' list

Results

Vigenere 11

(Alphabet (36) ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789)

EMINENCESHA	friedrichwilhelmkasiskiwastheonewhodesignedtheaaakasiskiexaminationtodecodevignerecipher
EMINENCASHA	friedrighwilhelmkawiskiwasthesnewhodesigredtheaaakawiskiexaminetiontodecohevignerecither
EMINENCESHE	friedrichwelhelmkasisgiwastheonewhodesignedpheaaakasisgiexaminatiktodecodevegnereciphen
8MINENCESHE	lriedrichwerhelmkasisgowastheonewsnodesignedpneaaakasisgoexaminatikttodecodevemnereciphen

VIGENERE CIPHER

Cryptography › Poly-Alphabetic Cipher › Vigenere Cipher

VIGENERE DECODER

Vigenere ciphertext

j3qrh4kgz3iptmyqxcw0zkm8i5xugs5lwl0lrwvirwktlqinexcw0zkmq5n qvpebpor5wqipqhw2ikzm4ipktzlr

PARAMETERS

Plaintext language: English

Alphabet: ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789

▶ AUTOMATIC DECRYPTION

DECRYPTION METHOD

Knowing the Key/Password: KEY

Knowing the key-length/size, number of letters: 11

Knowing only a partial key: KE?

Knowing a plaintext word: CODE

Vigenere Cryptanalysis (Kasiski's Test)

▶ DECRYPT

See also: Beaufort Cipher – Caesar Cipher

Summary

- Vigenere Decoder
- Vigenere Encoder
- How to encrypt using Vigenere cipher?
- How to decrypt Vigenere cipher?
- How to recognize Vigenere ciphertext?
- How to decipher Vigenere without knowing the key?
- How to find the key when having both cipher and plaintext?
- What are the variants of the Vigenere cipher?
- How to choose the encryption key?
- What is the running key vigenere cipher?
- What is the keyed vigenere cipher?
- What is a Saint-Cyr slide?

Feedback

flag:
vishwaCTF{friedrichwilhelmkasiskiwastheonewhodesignedtheaaakasiskiexaminationtodecodevignerecipher}