**Vigenère and Gronsfeld Cipher**

**Introduction**

The Vigenère Cipher is a polyalphabetic substitution cipher. The method was originally described by Giovan Battista Bellaso in his 1553 book La cifra del. Sig. Giovan Battista Bellaso; however, the scheme was later misattributed to Blaise de Vigenère in the 19th century, and is now widely known as the Vigenère cipher.

Blaise de Vigenère actually invented the stronger [Autokey cipher](http://en.wikipedia.org/wiki/Autokey_cipher) in 1586.

The Vigenère Cipher was considered le chiffre ind hiffrable (French for the unbreakable cipher) for 300 years, until in 1863 Friedrich Kasiski published a successful attack on the Vigenère cipher. Charles Babbage had, however, already developed the same test in 1854. Gilbert Vernam worked on the vigenere cipher in the early 1900s, and his work eventually led to the one-time pad, which is a provably unbreakable cipher.

**The Algorithm**

The 'key' for a vigenere cipher is a key word. e.g. 'FORTIFICATION'

The Vigenere Cipher uses the following tableau (the 'tabula recta') to encipher the plaintext:

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

---------------------------------------------------

A 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

B 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 A

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

D D 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

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

F 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 E

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

H H 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

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

J 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 I

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

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

M M 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

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

O 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 N

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

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

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

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

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

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

V V 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

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

X 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 W

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

Z Z 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

To encipher a message, repeat the keyword above the plaintext:

FORTIFICATIONFORTIFICATIONFO

DEFENDTHEEASTWALLOFTHECASTLE

Now we take the letter we will be encoding, 'D', and find it on the first column on the tableau. Then, we move along the 'D' row of the tableau until we come to the column with the 'F' at the top (The 'F' is the keyword letter for the first 'D'), the intersection is our ciphertext character, 'I'.

So, the ciphertext for the above plaintext is:

FORTIFICATIONFORTIFICATIONFO

DEFENDTHEEASTWALLOFTHECASTLE

ISWXVIBJEXIGGBOCEWKBJEVIGGQS

**Variants**

There are several ciphers that are very similar to the vigenere cipher.

The Gronsfeld cipher is exactly the same as the vigenere cipher, except numbers are used as the key instead of letters. There is no other difference. The numbers may be picked from a sequence, e.g. the Fibonacci series, or some other pseudo-random sequence.

The gronsfeld cipher is cryptanalysed in the same way as the vigenere algorithm, however the autokey cipher will not be broken using the kasiski method since the key does not repeat. The best way to break the autokey cipher is to try and guess portions of the plaintext or key from the ciphertext, knowing they must both follow the frequency distribution of english text. Guessing how the plaintext begins is the easiest way of cracking the cipher.

To encipher your own messages in python, you can use the [pycipher](http://www.practicalcryptography.com/miscellaneous/pycipher/installing-pycipher/) module. To install it, use pip install pycipher. To encipher messages with the Vigenere cipher (or another cipher, see [here for documentation](http://pycipher.readthedocs.org/en/latest/)):

>>>from pycipher import Vigenere

>>>Vigenere('HELLO').encipher('defend the east wall of the castle')

'KIQPBKXSPSHWEHOSPZQHOINLGAPP'

>>>Vigenere('HELLO').decipher('KIQPBKXSPSHWEHOSPZQHOINLGAPP')

'DEFENDTHEEASTWALLOFTHECASTLE'

For the Gronsfeld cipher:

>>>from pycipher import Gronsfeld

>>>Gronsfeld([4,5,3,2,9]).encipher('defend the east wall of the castle')

'HJIGWHYKGNEXWYJPQRHCLJFCBXQH'

>>>Gronsfeld([4,5,3,2,9]).decipher('HJIGWHYKGNEXWYJPQRHCLJFCBXQH')

'DEFENDTHEEASTWALLOFTHECASTLE'

**Cryptanalysis**

See [Cryptanalysis of the Vigenere Cipher](http://practicalcryptography.com/cryptanalysis/stochastic-searching/cryptanalysis-vigenere-cipher/) for a guide on how to break this cipher by hand, and [here](http://practicalcryptography.com/cryptanalysis/stochastic-searching/cryptanalysis-vigenere-cipher-part-2/) for how to do it automatically.

When trying to break the Vigenere cipher, the first step is to determine the key length. [This](http://practicalcryptography.com/cryptanalysis/stochastic-searching/cryptanalysis-vigenere-cipher/) page describes how to use the Index of Coincidence to determine the key length. Once this is known, we can start trying to determine the exact key. This is usually done using the Chi-squared test to find the correct offset for each letter.

**References**

* [1] [Wikipedia](http://en.wikipedia.org/wiki/Vigen%C3%A8re_cipher) has a good description of the encryption/decryption process, history and cryptanalysis of this algorithm
* [2] Kahn, D (1973) The CodeBreakers. Macmillan: New York
* [3] <http://www.trincoll.edu/depts/cpsc/cryptography/vigenere.html> has a good description of the algorithm along with cryptanalysis.
* Simon Singh's 'The Code Book' is an excellent introduction to ciphers and codes, and includes a section on ADFGVX ciphers.
* Singh, Simon (2000). The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography. ISBN 0-385-49532-3.