Floor Covering Media
Your Gateway to the Floor Covering Industry

Durable encryption method

WIKIPEDIA
The Free Encyclopedia

Vigenère cipher

The Vigenère cipher named after Blaise de Vigenère although invented by Giovan Battista Bellaso is a method of encrypting alphabetic text where each letter of the plaintext is encoded with a different Caesar cipher, whose increment is determined by the corresponding letter of another text, the key.

WIKIPEDIA
The Free Encyclopedia

Blaise de Vigenère

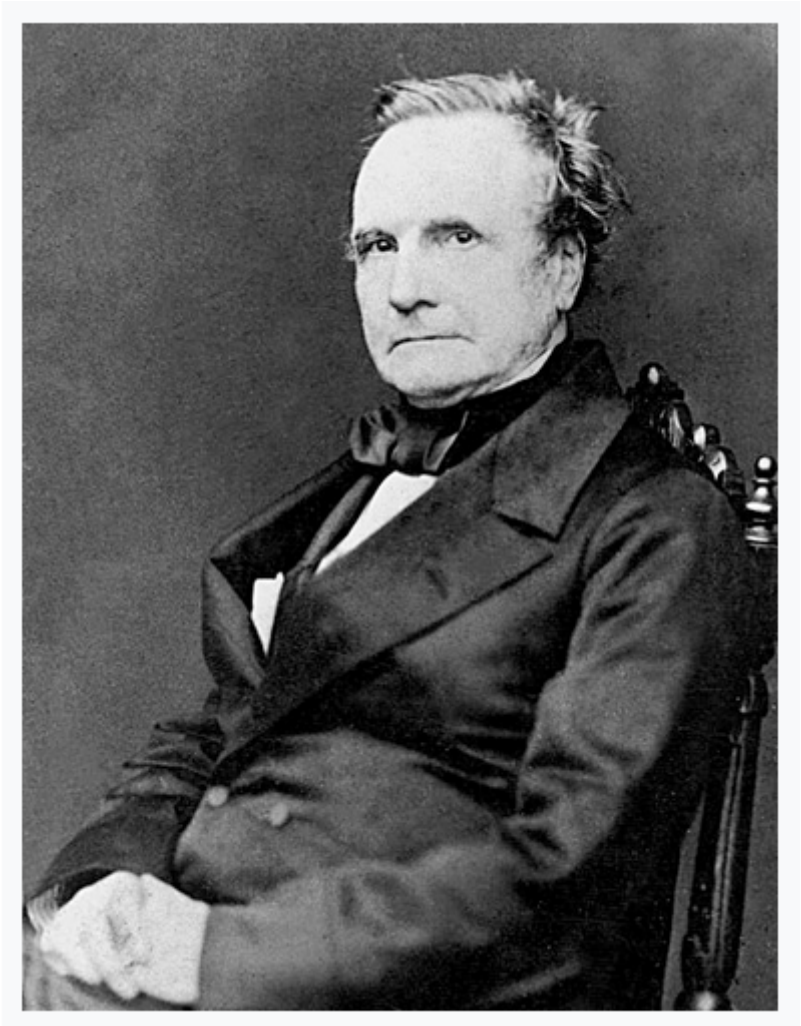
If the plaintext to be encrypted is the phrase 'attacking tonight' and the encryption key is 'OCULORHINOLARINGOLOGY', then this is the procedure: The first letter a of the plaintext is shifted by 14 positions within the alphabet (the first letter O of the key is the 14th letter of the alphabet, counting from 0), yielding o; the second letter t is shifted by 2 (because the second letter C of the key means 2) yielding v; the third letter t is shifted by 20 (U) yelding n, with wrap-around; and so on; yielding the coded message ovnlqbpvt eoeqtnh.

Giovan Battista Bellaso

If the recipient of the message knows the encryption key, he or she could decryp and recover the plaintext by reversing the above encryption process. The Vigenère cipher is a method of polyalphabetic substitution code, which was invented by Giovan Battista Bellaso in 1553. At the time, it was relatively easy to implement and for three centuries remarkably resilient to prying eyes.

Friedrich Kasiski

It was this resilience that earned it the *nickname* of *chiffrage indéchiffrable* (indecipherable cipher); an accurate *sobriquet* up until 1863 when a German infantry officer and archeologist Friedrich Kasiski devised a general method to decipher Vigenère ciphers; which was published in Die Geheimschriften und die Dechiffrir-Kunst (German for Secret writing and the Art of Deciphering).



WIKIPEDIA
The Free Encyclopedia

Kasiski examination

While it was the first published account of a particular procedure suggested for attacking polyalphabetic substitution cipers (Vigenère ciphers in particular) it is quite possible that Charles Babbage was already aware of a similar methodology that wasn't published, which relied upon noticeable gaps between repeated fragments in the ciphertext that revealed hints to the perceptive observer about the keylength, which was used to encrypt the text. This particular procedure is commonly referred to as the Kasiski examination.

More than a few people have attempted to implement encryption schemes, which are Vigenère ciphers. Obviously, this wasn't the only type of polyalphabetic cipher at the time. Circa 1467, Leon Battista Alberti documented a description of a polyalphabetic cipher that required a cumbersome metal cipher disk to switch between the cipher alphabets and only switched alphabets after several words. Writing the letter of the corresponding alphabet in the cipher text indicated the alphabet-switches.

Floor Covering Media
Your Gateway to the Floor Covering Industry

	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

The Polygraphiae (1518) credits Johannes Trithemius as the tabula recta's inventor, which is actually an important component of the Vigenère cipher. Though it could be said that Trithemius sourced the tabula recta ineffectually with a rigid even almost predictable system for switching between cipher alphabets. Learn more about the history of this cipher Wikipedia or Youtube.

Floor Covering Media publishes
press releases called Flooring Updates.

Floor Covering Media

Your Gateway to the Floor Covering Industry

Flooring Network

For those in the market and those that serve it

Floor Covering Media is
a social media network.

Floor Search

Answers to Questions About Flooring

Retrieve timely, objective news and
information at https://www.floorsearch.info.