Die Vigenère-Verschlüsselung wurde im 16. Jahrhundert erfunden und nach dem französischen Blaise de Vigenère benannt. Sie galt lange Zeit als unlösbar und konnte erst 300 Jahre später zum ersten Mal geknackt werden.

So funktioniert die Vigenère-Verschlüsselung:
Wie auch bei der Cäsar-Verschlüsselung werden die Buchstaben entlang des Alphabets verschoben. Anstatt jedoch jeden Buchstaben um die gleiche Anzahl zu verschieben und so *einen* Cäsar-Schlüssel zu erhalten, benutzt man zum Beispiel 6 Cäsar-Schlüssel. So wird jeder sechste Buchstabe mit dem gleichen Cäsar-Schlüssel kodiert.
Für die geheime Nachricht CRYPTOCROC und 6 Cäsar-Schlüssel, zum Beispiel G, E, H, E, I, M, ergibt sich dann:

Nachricht	C	R	Y	P	T	O	C	R	O	C
Cäsar-Schlüssel	G	E	H	E	I	M	G	E	H	E
Verschlüsselung	I	V	F	T	B	A	I	V	V	G

Den Vigenère-Schlüssel erhält man indem du deine Cäsar-Schlüssel aneinander reihst. Hier ist also der Vigenère-Schlüssel GEHEIM.

Beispiel:
Der Satz “ich bin der cryptocroc” mit dem Schlüssel GEHEIM wird zu “ogo fqz jiy gzkvxvgzai”

Wie sicher ist die Vigenère-Verschlüsselung?
Die Sicherheit hängt ab von der Länge des Vigenère-Schlüssels. Desto länger dieser ist, desto sicherer wird deine Nachricht.
Auch die Vigenère-Verschlüsselung kann man mit einer Häufigkeitsanalyse knacken; dies ist nur deutlich schwerer als bei der monoalphabetischen oder der Cäsar-Verschlüsselung.