Bei der Cäsar-Verschlüsselung gibt es gerade mal 25 mögliche Verschlüsselungen, weswegen diese durch Ausprobieren sehr leicht zu knacken ist. Um die Verschlüsselung sicherer zu machen wurde die monoalphabetische Verschlüsselung erfunden. Hier gibt es 403.291.461.126.605.635.584.000.000, also mehr als 400 Quadrillionen Möglichkeiten!

So funktioniert die monoalphabetische Verschlüsselung:
Anstatt wie bei der Cäsar-Verschlüsselung das Alphabet zu verschieben, wird jeder Buchstabe durch einen anderen, beliebigen ersetzt. Zum Beispiel:

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

Die Buchstabenfolge mit dem du die jeweiligen Buchstaben aus dem Alphabet ersetzt heißt Schlüssel. In dem Beispiel ist der Schlüssel POIUZTREWQASDFGHJKLYXCVBNM.

Beispiel:
Der Satz “ich bin der cryptocroc” mit dem Schlüssel QWERTZUIOPLKJHGFDSAYXCVBNM wird zu “oei woh rts esnfygesge”

Wie sicher ist die monoalphabetische Verschlüsselung?
Sie ist sicherer als die Cäsar-Verschlüsselung, da es viel mehr Möglichkeiten gibt eine Nachricht zu verschlüsseln. So kommt man nicht weit durch bloßes Ausprobieren.
Jedoch ist auch die monoalphabetische Verschlüsselung nicht sicher, da sie mit einer Häufigkeitsanalyse schnell geknackt werden kann.