Das Geheimnis des römischen Kaisers Caesar - Lösung

2. *Georg der Gangster* hat im Internet folgende vermutlich mit dem Caesar-Verfahren verschlüsselte Nachricht abgefangen: KEJPWVBGECGUCT

   a. Versuche, den Code auch ohne Kenntnis des Abstands zwischen KTA und GTA zu knacken!

      Durch systematisches Ausprobieren sämtlicher möglichen Abstände mit den ersten Zeichen der Nachricht führt beim Abstand 4 zum Erfolg, die Nachricht beginnt mit ICH …

      Die entschlüsselte Nachricht lautet: ICH NUTZE CAESAR

   b. Wie sicher ist die Verschlüsselung nach dem Caesar-Verfahren? Begründe deine Antwort!
      Hinweis: Wie viele verschiedene Geheimtextalphabete gibt es mit diesem Verfahren?

      Das Verfahren ist sehr unsicher. Durch Ausprobieren aller 25 möglichen Schlüssel mit den ersten Zeichen der Nachricht lässt sich eine mit dem Caesar-Verfahren verschlüsselte Nachricht mit vertretbarem Aufwand entschlüsseln.

3. Angenommen, die Buchstaben des Geheimtextalphabets werden in beliebiger Reihenfolge zugeordnet, z.B. :

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

   Wie würde sich diese Veränderung auf die Sicherheit der Verschlüsselung auswirken?
   Hinweis: Wie viele verschiedene Geheimtextalphabete gibt es mit diesem Verfahren?

   Das Verfahren ist wesentlich sicherer. Durch die beliebige Reihenfolge der Zeichen gibt es viel mehr mögliche Geheimtextalphabete. Die genaue Anzahl möglicher Geheimtextalphabete beträgt 26! („26 Fakultät“): Für die Wahl des ersten Zeichens stehen 26 Zeichen zur Verfügung. Für die Wahl des nächsten Zeichens verbleiben 25 mögliche Zeichen, allein für die Festlegung der ersten beiden Zeichen gibt es also 26*25 mögliche Kombinationen. Für das nächste Zeichen können die 26*25 Kombinationen mit einem von 24 weiteren Zeichen kombiniert werden usw. Für 26 Zeichen entstehen so 26 * 25 * 24 * ... * 3 * 2 * 1 = 26! = 403.291.461.126.605.635.584.000.000 Kombinationen. Ein systematisches Ausprobieren aller Schlüssel ist so nicht mehr möglich!