Übung 2

**We received the following ciphertext which was encoded with a shift cipher:**

**UKGIGP YKTF FGT FGUUGP CTOGG KP CNNGP TCGPIGP XQO INGKEJGP IGKUV DGUGGNV KUV**

1. **Perform an attack against the cipher based on a letter frequency count: How many letters do you have to identify through a frequency count to recover the key? What is the cleartext?**

Der Buchstabe „E“ kommt bei deutschen Wörtern am häufigsten vor. Mit der Annahme, dass es sich um eine deutschen Text handelt, wird der Buchstabe gesucht, der im Ausgangstext am häufigsten vorkommt. Der Buchstabe „G“ kommt mit 15 Mal am häufigsten vor. Es kann davon ausgegangen werden, dass „G“ im verschlüsselten Text einem „E“ im Klartext entspricht. Von „G“ auf „E“ muss man im Alphabet zwei Buchstaben zurückgegen, weshalb der Schlüssel 2 sein muss. Somit ergibt sich folgender Zusammenhang:

A picture containing text, bunch, lots, day

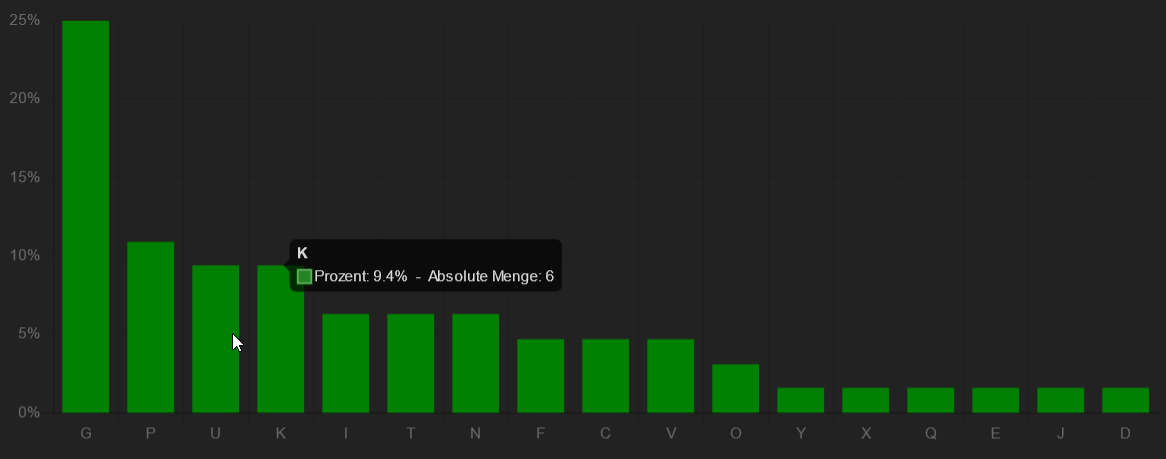
Description automatically generated

Kontrolliert werden kann das Ganze mit [Cryptool](https://www.cryptool.org/de/cto/caesar):

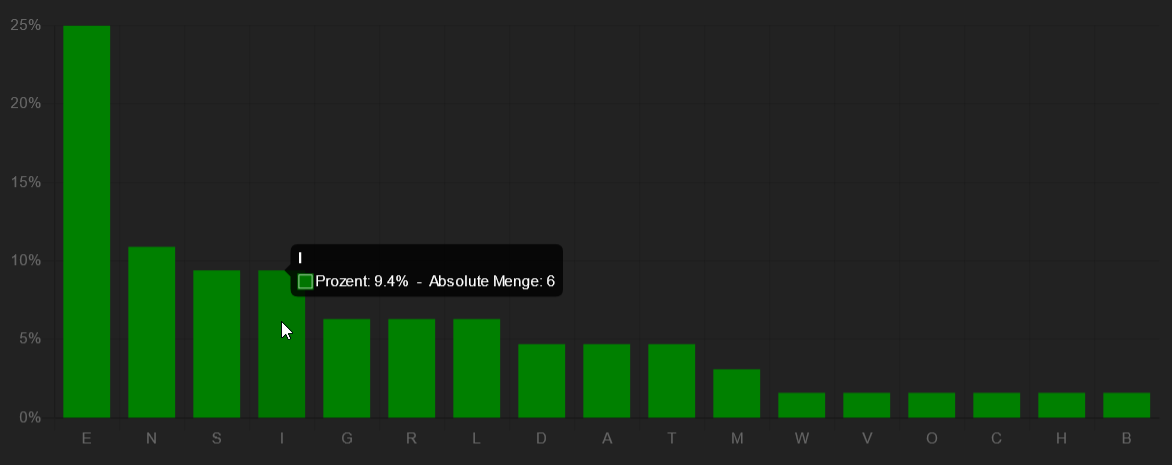
SIEGEN WIRD DER DESSEN ARMEE IN ALLEN RAENGEN VOM GLEICHEN GEIST BESEELT IST

1. **Was passiert bei der Caesar-Verschluesselung mit dem Histogram?**

**verschlüsselter Text:**

****

**Klartext:**



Es zeigt sich, dass die Diagramme genau gleich aussehen. Allerdings sind die Buchstaben genau um den Schlüssel von 2 nach „hinten“ verschoben, weshalb bei der grafischen Häufigkeitsanalyse der Buchstabe **I** im Klartext genau gleich oft vorkommt wie der Buchstabe **K** im verschlüsselten Text.

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 genau um den Schlüssel verschoben