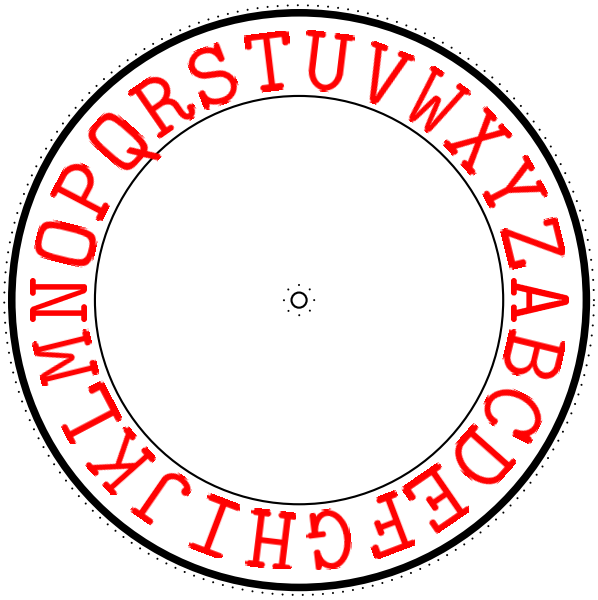
ABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZ

ABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZ

Cäsar, Vigenère, Vernam

Für alle drei Verschlüsselungsverfahren musst du die beiden Streifen und die beiden Scheiben an den punktierten Linien ausschneiden, in der Mitte der Scheiben ein Loch hineinpieksen und drehbar verbinden. (Deine Eltern haben bestimmt eine Rundkopf- oder Musterbeutelklammer, mit der man große Briefumschläge zumacht.) Die Streifen kann man einfach nebeneinanderlegen.

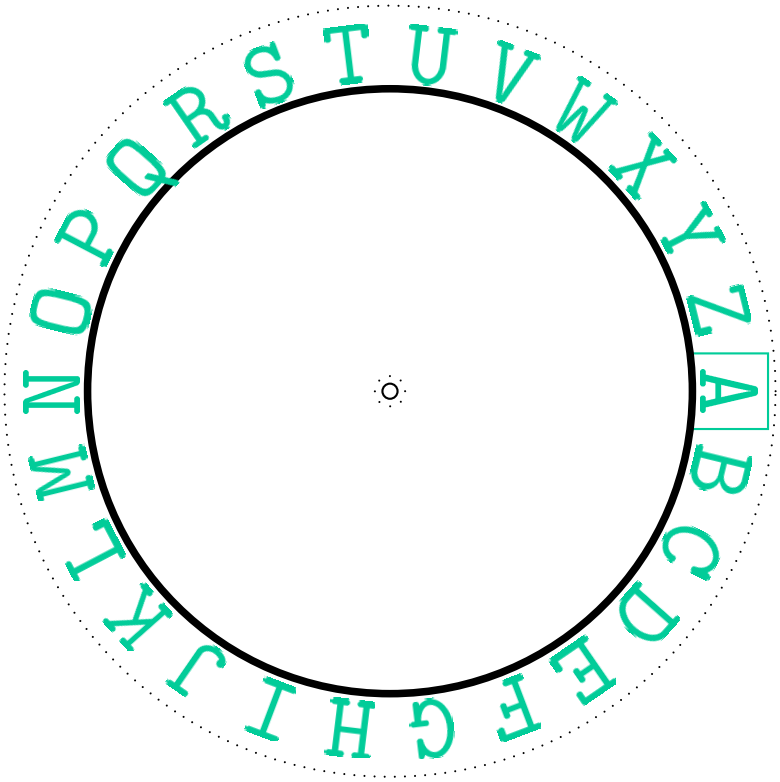


Die Cäsar-Chiffre. Wähle einen *Buchstaben* als Schlüssel. Cäsar selbst soll meistens den dritten Nachfolger verwendet haben, das wäre bei uns der Schlüsselbuchstabe D. Stelle nun die Scheibe so ein, dass der roten Schlüsselbuchstabe beim grünen A steht. Um zu verschlüsseln, lies für jeden Buchstaben deines Klartextes am entsprechenden grünen Klartextbuchstaben den zuigehörigen roten Geheimtextbuchstaben ab und schreib ihn auf. Zum Entschlüsseln der Nachricht machst du dasselbe nur umgekehrt: aus roten Buchstaben werden grüne.

Beispiel: Mit dem Schlüsselbuchstaben D wird aus dem Klartext KINDERUNI der Geheimtext NLQGHUXQL. Dazu stellst Du das grüne A auf das rote D ein. Dann liest nach und nach bei den grünen Buchstaben die roten ab.

Die Vigenère-Chiffre. Wähle ein *Wort* als Schlüssel. Das ist deutlich besser als nur ein Buchstabe. Zum Verschlüsseln schreibe die Nachricht am Besten auf. Und direkt darunter mehrmals den Schlüssel und zwar so oft, dass genauso viele Buchstaben dastehen wie in der Nachricht. Wie bei Cäsar stellst du die Scheibe mit dem grünen A auf den ersten Buchstaben des Schlüsselworts ein. Dann liest Du bei deinem ersten grünenn Klartextbuchstaben den roten Geheimtextbuchstaben ab. Für den zweiten Klartextbuchstaben nimmst Du den zweiten Buchstaben aus dem Schlüsselwort. Und so weiter… Zum Entschlüsseln macht man es einfach umgekehrt. Probier einfach mal, ob Du das Beispiel im Kasten ver- und entschlüsseln kannst.

```
VIGENEREISTBESSERALSCAESAR
SCHULESCHULESCHULESCHULESC
NKNYYIJGPMEFWUZYCEDUJUPWST
```



Die Vernam-Chiffre. Das ist das sicherste Verschlüsselelungsverfahren überhaupt. Es ist sogar das einzige, für das man beweisen kann, dass es sicher ist. Es funktioniert genauso wie die Vigenère-Chiffre, aber hier muss das Schlüsselwort erstens völlig zufällig sein, also irgendeine sinnlose Folge von Buchstaben, und zweitens muss es genauso lang wie die Nachricht sein und drittens darf es nur ein einziges Mal verwendet werden.

Knacken? Sicherheit bedeutet, dass man eine Chiffre nur schwer oder gar nicht knacken kann, ohne den Schlüssel zu kennen. Die Cäsar-Chiffre ist leicht zu knacken, da man ja nur 26 Möglichkeiten ausprobieren muss. Die Vigenère-Chiffre ist schon wesentlich sicherer, immerhin hat es etwa dreihundert Jahre gedauert bis er geknackt wurde. Bei der Vernam-Chiffre kann man beweisen, dass sie unknackbar ist.

©2009 Michael Nüsken, Bonn