Vigenère – Verschlüsselung

Der französische Diplomat und Kryptograf Blaise de Vigenère (1523 – 1596) entwickelte mit seinem Verfahren die Möglichkeit, dass einem Klartextbuchstaben mehrere Geheimtextbuchstaben zugeordnet werden können.   
Eine Möglichkeit ist es, für jeden Buchstaben des Schlüsselwortes eine eigene Caesar-Scheibe zu benutzen (oder die Scheibe jeweils zu verstellen)

Schlüssel: INFOINFOIN  
Klartext: GUTGEMACHT  
Geheimtext: OHYUMZFQPG

1. Prüfe das Beispiel!

Das Beispiel ist richtig!

1. Entschlüssle die Nachricht Apmicqsvpetwluwuyrwpk mit dem Schlüssel Schule.

Informatikistspannend

1. Um den Aufwand mit den Caesar-Scheiben zu reduzieren wird das Vigenére-Quadrat verwendet, womit Ver- und Entschlüsseln schneller erfolgt. Benutze die Vorlage und Verschlüssele einen von dir gewählten Text.
2. Der Geheimtext goudipq wurde verschlüsselt. Beweise, dass sowohl paarmal als auch Rostock aus dem Geheimtext zu entschlüsseln ist.

Beispiel:

Schlüssel: Packung roumwpf   
Klartext: Rostock paarmal  
Geheimtext: goudipq goudipq

Nenne einen weiteren Klartext, der sich aus dem Geheimtext rekonstruieren lässt. Beurteile die Sicherheit dieses Verfahrens.

Schlüssel: forzqlm  
Klartext: badesee  
Geheimtext: goudipq

* Sicherheit ist bei einer 1:1 Beziehung von Schlüssel und Klartext sehr hoch!