One-Time-Pad (OTP)[1]

a) Der Geheimtext lautet: F O N M Z R

Welcher der folgenden Klartexte könnte mit der Vigenère-Tabelle verschlüsselt worden sein?

T E L L E R, M E S S E R, F E R I E N

Nachricht:

Schlüssel:

Geheimtext: F O N M Z R

b) *Denke dir einen längeren Klartext aus (max. 1024 Zeichen). Wähle einen mindestens genauso langen Schlüssel (max. 1024 Zeichen). Verschlüssele deinen Klartext mit dem Vigenère-Verfahren. (z.B. mit CrypTool)*

c) Kann deine Sitznachbarin / dein Sitznachbar deinen in (b) erzeugten Geheimtext knacken? Begründe.

1 Teilweise übernommen aus: *http://www.inf-schule.de/kommunikation/kryptologie/historischechiffriersysteme/station_onetimepad/version:1* (21.4.18)