

## Aufgabe 1:

**Klassische Chiffren**

Auf der folgenden Seite finden sie einen längeren, verschlüsselten Text. Dieser ist mit einer klassischen Chiffre verschlüsselt; es wird vermutet, daß der zugehörige Klartext in englischer Sprache verfasst ist. Befassen sie sich im Rahmen der folgenden Aufgabenstellungen mit dem Text:

1. Brechen sie die Chiffre, egal wie. Entschlüsseln sie die ersten paar Zeilen des Chiffrates. Erläutern sie ihren Lösungsweg.
2. Entwickeln sie ein kleines Programm (egal wie, sie müssen's erklären können), dass ihnen die lästige Arbeit der Buchstabensuche abnimmt und es ihnen ermöglicht, den Rest des Textes zu entschlüsseln.
3. Um was für eine Chiffre handelt es sich? Welche Schlüssellänge hat das Verfahren?
4. Was ist das tolle an dem gewählten Schlüssel?

Rqtne Nyyna Cbr: Gur Enira  
[Svefg choyvfurq va 1845]

Bapr hcba n zvqavtug qernel, juvyr V cbaqrerq jrnx naq jrncl,  
Bire znal n dhnvag naq phevbhf ibyhxr bs sbetbggra yber,  
Juvyr V abqqrq, arneyl anccvat, fhqgrayl gurer pnzr n gnccvat,  
Nf bs fbzr bar tragyl enccvat, enccvat ng zl punzore qbbe.  
'Gvf fbzr ivfvgbe,' V zhggrerq, 'gnccvat ng zl punzore qbbe -  
Bayl guvf, naq abguvat zber.'

Nu, qvfgvapgyl V erzrzore vg jnf va gur oyrnx Qrprzore,  
Naq rnpu frcnegr qlvat rzore jebhtug vgf tubfg hcba gur sybbe.  
Rntreyll V jvfurq gur zbeebj; - invayl V unq fbhtug gb obeebj  
Sebz zl obbxf fheprnfr bs fbeebj - fbeebj sbe gur ybfg Yraber -  
Sbe gur ener naq enqvnag znvqra jubz gur natryf anzrq Yraber -  
Anzryrff urer sbe rirezber.

Naq gur fvyxra fnq hapregnva ehfgyvnt bs rnpu checyr phegnva  
Guevyyrq zr - svyyrq zr jvgu snagngvp greebef arire sryg orsber;  
Fb gung abj, gb fgvy gur orngvat bs zl urneg, V fgbbq ercngvat  
'Gvf fbzr ivfvgbe ragerngvat ragenapr ng zl punzore qbbe -  
Fbzr yngr ivfvgbe ragerngvat ragenapr ng zl punzore qbbe; -  
Guvf vg vf, naq abguvat zber,'

'Fve,' fnvq V, 'be Znqnz, gehyl lbhe sbetvirarff V vzcyber;  
Ohg gur snpg vf V jnf anccvat, naq fb tragyl lbh pnzr enccvat,  
Naq fb snvagyl lbh pnzr gnccvat, gnccvat ng zl punzore qbbe,  
Gung V fpnepr jnf fher V urneq lbh' - urer V bcrarq jvqr gur qbbe; -  
Qnexarff gurer, naq abguvat zber.

Qrrc vagb gung qnexarff crrevat, ybat V fgbbq gurer jbaqrevat, srnevat,  
Qbhogvat, qernzvat qernzf ab zbegny rire qnerq gb qernz orsber  
Ohg gur fvyrapr jnf haoebxra, naq gur qnexarff tnir ab gbxra,  
Naq gur bayl jbeq gurer fcbxra jnf gur juvfcrerq jbeq, 'Yraber!'  
Guvf V juvfcrerq, naq na rpub zhezherq onpx gur jbeq, 'Yraber!'  
Zreryl guvf naq abguvat zber. [...]

## Aufgabe 2:

## Die Vigenère-Chiffre

Verglichen mit dem trivialen Verschlüsselungsalgorithmus in Aufgabe 1 bietet die Vigenère-Chiffre eine wesentlich höhere Sicherheit. Warum ist das so?

1. Verschlüsseln sie den Text „angriff im morgengrauen“ einmal mit der Chiffre aus Aufgabe 1 und einmal mit dem Vigenère-Verfahren unter Verwendung des Schlüssels „STRENGGEHEIM“.
2. Vergleichen sie die Ergebnisse hinsichtlich der Verteilung der Buchstaben im Klartext bzw. im Chifftrat. Zu welchen Resultaten kommen sie?
3. Wie groß ist der Schlüsselraum der Vigenère-Chiffre?
4. Optional: Implementieren sie das Ver- und Entschlüsseln eines Textes mit einem frei wählbaren Schlüssel mit der Vigenère-Chiffre. Probieren sie die Verschlüsselung eines Textes mit mehreren Schlüsseln. Wie muß ein Schlüssel beschaffen sein, um eine optimale Buchstabenstreuung im Geheimtext zu erhalten?

## Aufgabe 3:

## Solitaire

Im Internet finden sie auf den Webseiten des berühmten Sicherheitsexperten und Cryptologen Bruce Schneier die Beschreibung des Verschlüsselungsverfahrens *Solitaire*<sup>1</sup>. Solitaire basiert auf der Verwendung von Spielkarten zur Erzeugung eines Schlüsselstromes. Klären sie hierzu die folgenden Fragen:

1. Was koennte u.U. dagegen sprechen, daß ein „Agent“ einen Computer oder sein Mobiltelefon (oder was auch immer) verwendet um Nachrichten zu verschlüsseln? Wozu braucht man Solitaire?
2. Wie groß ist der Schlüsselraum des Verfahrens? Ist das gut oder schlecht?
3. Probieren sie das Verfahren aus (Kartenspiele gibt's bei ihrem Dozenten)!
4. Wozu dient die ganze komplizierte Abheberei zur Erzeugung des Schlüsselstromes? Ginge das auch einfacher?

---

<sup>1</sup>Siehe <http://www.schneier.com/solitaire.html>.