

## Aufgabe 1:

**Sicherheitspolitiken**

Im Rahmen einer der letzten Lehrveranstaltungen wurden Sicherheitspolitiken als ein zentraler Bestandteil von Firewalls bzw. ganz allgemein von gegen Angriffe zu schützenden IT-Infrastrukturen dargestellt. Informieren sie sich über die Folien, die benannte Literatur und insbesondere das Grundschutzhandbuch des BSI<sup>1</sup> zur Wiederholung nochmals kurz über die wichtigsten, im Rahmen einer Sicherheitspolitik zu beantwortenden Fragen und bearbeiten sie die folgenden Aufgabenstellungen:

1. Führen sie für ein Rechnernetz ihrer Wahl (z.B. das Netz der FHB im WWZ) eine Strukturanalyse durch.
2. Wie ist der Schutzbedarf der einzelnen Komponenten bzw. Komponentengruppen des Netzwerks?
3. Erstellen sie gruppenorientierte Kommunikationsprofile für die Benutzer des Netzwerks.
4. Welche Komponenten des Netzes werden bereits durch Sicherheitskomponenten geschützt? Was leisten diese Komponenten? Wo besteht zusätzlicher Handlungsbedarf?
5. Überlegen sie sich für jede Schnittstelle ihres Netzes zu einem Netz mit anderem Schutzbedarf eine Sicherheitsstrategie.
6. Falls sie Firewalls einsetzen wollen: Welche Art von Filtersystem soll eingesetzt werden? Begründen sie ihre Entscheidung. Geben sie einige Filterregeln (Syntax: Deutsch) als Beispiele an.

---

<sup>1</sup>siehe <http://www.bsi.bund.de/gshb/deutsch/index.htm>

## Aufgabe 2:

### Klassische Chiffren

Auf der folgenden Seite finden sie einen längeren, verschlüsselten Text. Dieser ist mit einer klassischen Chiffre verschlüsselt. Befassen sie sich im Rahmen der folgenden Aufgabenstellungen mit dem Text:

1. Brechen sie die Chiffre, vorzugsweise auf Papier. 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), das 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?

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

Bapr hcba n zvqavtug qernel, juvyr V cbaqrerq jrn̄x naq j̄rnel,  
Bire znal n dhnvag naq phevbfh̄f ibyh̄zr bs sbetbggra yber,  
Juvyr V abqqrq, arneyl anccvat, fhqqr̄ayl gurer pn̄zr n gnccvat,  
Nf bs fb̄zr bar tragyl enccvat, enccvat ng zl punzore qb̄be.  
'Gvf fb̄zr ivfvgbe,' V zhggr̄erq, 'gnccvat ng zl punzore qb̄be -  
Bayl guvf, naq abguvat zber.'

Nu, qvfgvap̄gyl V erz̄zore vg j̄nf va gur oyr̄nx Qr̄pr̄zore,  
Naq r̄np̄u fr̄cn̄egr ql̄vat rzore jebhtug vgf tubfg hcba gur syb̄be.  
R̄nt̄reȳl V j̄vfurq gur zbeeb̄j; - invayl V unq fb̄htug gb obeeb̄j  
Sebz zl ob̄bx̄f fhepr̄n̄fr bs fb̄eeb̄j - fb̄eeb̄j sbe gur yb̄fg Yraber -  
Sbe gur ener naq enq̄vn̄ag zn̄vqra jubz gur natryf anzr̄q Yraber -  
Anzryr̄ff urer sbe rirezber.

Naq gur fvyxra fn̄q hapregn̄va ehfḡyvat bs r̄np̄u checyr phegn̄va  
Guevȳyr̄q zr - svyyr̄q zr j̄v̄gu snaḡn̄fḡvp greebef arire sryg orsber;  
Fb̄ gung ab̄j, gb fḡvȳy gur ornḡvat bs zl urneg, V fḡbb̄q er̄cr̄nḡvat  
'Gvf fb̄zr ivfvgbe rager̄nḡvat ragenapr ng zl punzore qb̄be -  
Fb̄zr yn̄gr ivfvgbe rager̄nḡvat ragenapr ng zl punzore qb̄be; -  
Guvf vg vf, naq abguvat zber,'

'Fve,' fn̄vq V, 'be Zn̄q̄nz, gehyl lb̄he sb̄etvirar̄ff V vzcyber;  
Ohg gur sn̄pg vf V j̄nf anccvat, naq fb̄ tragyl lb̄h pn̄zr enccvat,  
Naq fb̄ sn̄vagyl lb̄h pn̄zr gnccvat, gnccvat ng zl punzore qb̄be,  
Gung V fp̄nepr j̄nf fher V urneq lb̄h' - urer V bcrar̄q j̄v̄qr gur qb̄be; -  
Q̄nexar̄ff gurer, naq abguvat zber.

Q̄rrc vagb gung q̄nexar̄ff cr̄revat, ybat V fḡbb̄q gurer j̄baq̄revat, sr̄nevat,  
Q̄bhoḡvat, q̄ern̄zvat q̄ern̄zf ab zbegny r̄ire q̄nerq gb q̄ern̄z orsber  
Ohg gur fvyrapr j̄nf haoeb̄xra, naq gur q̄nexar̄ff tn̄ir ab gb̄xra,  
Naq gur bayl j̄beq gurer fcb̄xra j̄nf gur juvf̄cr̄erq j̄beq, 'Yraber!'  
Guvf V juvf̄cr̄erq, naq na r̄pub zhezherq on̄px gur j̄beq, 'Yraber!'  
Zr̄erȳl guvf naq abguvat zber. [...]

## Aufgabe 3:

## 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. Wie muß ein Schlüssel beschaffen sein, um eine optimale Buchstabenstreuung (also eine maximale stochastische Unabhängigkeit zwischen Klartext und Geheimtext) im Geheimtext zu erhalten?