Beurteilen der Sicherheit von Substitutionsverfahren

Aufgabe 1: Ergänzen Sie in der Tabelle, ob für die angegebenen Verfahren ein Brute-Force-Angriff bzw. ein Angriff mithilfe einer Häufigkeitsanalyse möglich ist und wie die Sicherheit der Verfahren jeweils erhöht werden kann.

	Brute-Force-Angriff	Angriff mithilfe einer Häufigkeitsanalyse	Möglichkeiten zur Erhöhung der Sicherheit
Substitution nach dem Prinzip des Caesar-Verfahrens			
Monoalphabetische Substitution mit beliebiger Zuordnungstabelle			
Polyalphabetische Substitution mit einem Schlüsselwort nach dem Prinzip von Vigenère			

Aufgabe 2: Untersuchen Sie die Sicherheit der folgenden Verfahren, indem Sie sie jeweils in die Tabelle aus Aufgabe 1 einordnen. Gehen Sie dabei jeweils davon aus, dass für einen Geheimtext bekannt ist, mit welchem Verfahren er verschlüsselt wurde, aber nicht mit welchem Schlüssel.

Verfahren A: Die 26 Zeichen des Alphabets und das Leerzeichen werden zufällig in drei Tabellen der Größe 3x3 eingetragen. Die Zeilen und Spalten werden mit beliebigen Zeichen beschriftet. Jedes Klartextzeichen wird dann durch die beiden Zeichen ersetzt, mit denen die Zeile und die Spalte in der jeweiligen Tabelle beschriftet sind.

	+	?	*
+	D	N	I
?	R		A
*	O	Z	V

	!	-	#
!	B	U	P
-	J	C	F
#	S	W	L

	$	%	&
$	G	K	E
%	Q	T	M
&	X	H	Y

Beispiel:

Klartext	S	A	F	A	R	I		I	M		U	R	W	A	L	D
Geheimtext	#!	?*	-#	?*	?+	+*	??	+*	%&	??	!-	?+	#-	?*	##	++

Aus dem Klartext SAFARI IM URWALD wird der Geheimtext #!?*-#?*?++*??+*%&??!-?+#-?*##++.

Verfahren B: Die Klartextzeichen werden zunächst mithilfe einer beliebigen Zuordnungstabelle ersetzt. Für jedes Geheimtextzeichen wird anschließend noch eine Caesar-Verschiebung durchgeführt.

Beispiel: Ersetzung mithilfe der folgenden Zuordnungstabelle:

klar	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
geheim	Q	L	E	P	B	J	H	U	S	D	N	Y	A	Z	T	I	W	C	O	G	V	K	M	F	X	R

Klartext	S	A	F	A	R	I		I	M		U	R	W	A	L	D
Geheimtext1	O	Q	J	Q	C	S		S	A		V	C	M	Q	Y	P

Anschließend Caesar-Verschiebung um 7.

Geheimtext1	O	Q	J	Q	C	S		S	A		V	C	M	Q	Y	P
Geheimtext2	V	X	Q	X	J	Z		Z	H		C	J	T	X	F	W

Aus dem Klartext SAFARI IM URWALD wird der Geheimtext VXQXJZ ZH CJTXFW.

Verfahren C: Das Verfahren C verwendet als Schlüssel zwei Zahlen x und y zwischen 1 und 26. Die Klartextzeichen werden mithilfe des Caesar-Verfahrens verschlüsselt. Die Zahl x legt dabei fest, um wie viele Zeichen im Alphabet das erste Klartextzeichen verschoben wird. Die folgenden Zeichen werden jeweils um eine Stelle mehr verschoben. Nachdem die ersten y Zeichen verschlüsselt wurden, wird der nächste Block von y Zeichen wieder nach dem gleichen Prinzip verschlüsselt. Das (y+1) Zeichen wird also wieder um x Zeichen verschoben.

Beispiel: Schlüssel x = 3 und y = 5

Klartext	S	A	F	A	R	I		I	M		U	R	W	A	L	D
Verschiebung um	3	4	5	6	7	3		4	5		6	7	3	4	5	6
Geheimtext	V	E	K	G	Y	L		M	R		A	Y	Z	E	Q	J

Aus dem Klartext SAFARI IM URWALD wird der Geheimtext VEKGYL MR AYZEQJ.

Verfahren D: Die Verschlüsselung erfolgt mithilfe der Rotoren, die Sie im Gruppenpuzzle zu Substitutionsverfahren kennengelernt haben.

Aufgabe 3:

a) Entwerfen Sie ein eigenes Verschlüsselungsverfahren.

b) Untersuchen Sie, ob ein Geheimtext, der mit Ihrem Verfahren erstellt wurde, …
   [1] … bei Kenntnis des Schlüssels eindeutig entschlüsselt werden kann.
   [2] … mithilfe eines Brute-Force-Angriffs geknackt werden kann.
   [3] … mithilfe einer Häufigkeitsanalyse geknackt werden kann.

c) [*]Implementieren Sie Ihr Verschlüsselungsverfahren. Zerlegen Sie das Verfahren dazu in geeignete Teilschritte und überlegen Sie, mit welchen algorithmischen Strategien sich diese umsetzen lassen. Passen Sie das Verfahren ggf. so an, dass Ihnen eine Implementierung möglich ist.

[*] Aufgabe zur Verknüpfung von Kryptologie und Algorithmik, die auch zu einem größeren Projekt ausgestaltet werden kann.