Angaben zur Person:

Name: Huber

Vorname/n: Valentin

Alter: 21

E-Mail: valentinchuber@gmail.com

Geschlecht: M

Derzeitige Tätigkeit: Informatik-Student

Geschätzte Entschlüsselungs-«Menge» (in Prozent): 100%

Vorgehensweise bei der Entschlüsselung (Stichworte genügen):

Brute-force-Versuch:

Bei gegebener Schlüssellänge kann ich die Buchstaben aus dem Ciphertext, die mit dem jeweils gleichen Buchstaben aus dem Schlüssel verschlüsselt werden als eigenen Unter-Text anschauen.

Dann kann ich eine Häufigkeitsanalyse auf die jeweiligen Unter-Texte machen. Ausserdem sollten bei jedem dieser Unter-Texte die Worthäufigkeiten ungefähr übereinstimmen. Ich kann also die Durchschnitte der Wahrscheinlichkeiten der jeweils häufigsten, jeweils zweithäufigsten, etc. Buchstaben nehmen und diese mit der Wahrscheinlichkeitsverteilung der Buchstaben in der deutschen Sprache vergleichen.

So kann ich also schauen, bei welcher Schlüssellänge die Wahrscheinlichkeitsverteilungen am besten übereinstimmen. Damit weiss ich die Schlüssellänge. Jetzt kann ich wieder die Wahrscheinlichkeitsverteilungen der Unter-Texte nehmen und schauen, um wie viele Zeichen diese verschoben sind verglichen mit der Wahrscheinlichkeitsverteilung der deutschen Sprache.

Aus dem ergibt sich das Codewort und damit kann ich den Text entschlüsseln.

Verwendete Hilfsmittel (alle verwendeten deutlich ankreuzen):

- Wegleitung
- Kurzes, selbst geschriebenes Programm

Zum Schluss noch eine Kleine Umfrage

1. Wie schätzt du den Schwierigkeitsgrad der von uns gestellten Aufgabe ein?

Sehr einfach geht so sehr schwierig

1	2	3	4	5	6	7	8	9	10
			x						

2. Für wie sicher hältst du die Verschlüsselung?

Total unsicher ganz okay sehr sicher

1	2	3	4	5	6	7	8	9	10
	x								

3. Glaubst du, diese Art von Verschlüsslung war mal alltäglich?

Ja ~~Nein~~

4. Oder ist sie das sogar noch?

~~Ja~~ **Nein**

5. Hattest du vor dem Experiment schon mal **aktiv** mit Kryptologie bzw. Verschlüsselungen zu tun? (Nicht Gehörtes aus den Nachrichten oder ähnliches...)

Nein, noch nie ein paar Male praktisch täglich

1	2	3	4	5	6	7	8	9	10
							x		

6. Das verwendete Chiffrierverfahren ist…

a) …ganz schön praktisch und gefällt mir.
b) …in Ordnung, aber nicht wirklich meins.
c) …komplex aber sehr spannend.
d) …sehr umständlich und überhaupt nicht mein Fall.
e) …sehr spannend, ich möchte gerne mehr darüber wissen.
f) …nicht sicher und seit langer Zeit überholt durch Verfahren, bei denen bewiesen werden kann, dass sie sicher sind.