Proseminar

Cryptool 2 - Kryptoanalyse

Dominic Bublitz

31. Januar 2014

Lehrstuhl 14 Software Engineering – Prof. Dr. Jan Jürjens

betreut durch: Sebastian Pape

Dominic Bublitz

Dominic.Bublitz@udo.edu
Matrikelnummer: 148377
Studiengang: Bachelor Informatik

Werkzeugunterstützung für sichere Software
Thema: Cryptool 2 - Kryptoanalyse

Eingereicht: 31. Januar 2014

Betreuer: Sebastian Pape

Prof. Dr. Jan Jürjens Lehrstuhl 14 Software Engineering
Fakultät Informatik
Technische Universität Dortmund
Otto-Hahn-Straße 14
44227 Dortmund

Ehrenwörtliche Erklärung

Ich erkläre hiermit ehrenwörtlich, dass ich die vorliegende Arbeit selbstständig angefertigt habe. Sämtliche aus fremden Quellen direkt oder indirekt übernommenen Gedanken sind als solche kenntlich gemacht.

Die Arbeit wurde bisher keiner anderen Prüfungsbehörde vorgelegt und noch nicht veröffentlicht.

Dortmund, den 31. Januar 2014 _____

Unterschrift

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1 Einleitung

1.1 Motivation, Ziele und Nutzen

In der heutigen Zeit, wo immer mehr Nachrichten digital ausgetauscht werden und die Sicherheit der Daten immer wichtiger wird, muss es eine Möglichkeit geben diese Sicherheit zu überprüfen. Dafür wurde das Instrument der Kryptoanalyse geschaffen, welches sich eben damit beschäftigt die Sicherheit zu analysieren und Verfahren zu entwickeln, um eine Verschlüsselung möglichst effizient zu knacken.

In meiner Arbeit möchte ich daher eine paar Methoden in der Kryptoanalyse vorstellen und hinterher mit dem Cryptool 2 eine Software vorstellen, welche es ermöglicht die vorgestellten Methoden praktisch auszuprobieren.

1.2 Aufbau der Arbeit

Meine Arbeit werde ich zu beginn mit einer Einführung in die Kryptographie und Kryptoanalyse einleiten. In dem ersten Kapitel werden daher einige Grundgedanken verständlich gemacht werden und erste Fachbegriffe geklärt. Im weiteren Verlauf werden dann konkrete Methoden zur Kryptoanalyse vorgestellt und anhand von einigen Beispielen erklärt. Mit diesen Grundlagen soll anhand des Cryptool 2 eine praktische Anwendung gezeigt werden.

2 Einführung in die Kryptologie

Die Kryptologie versucht Nachrichten so zu verändern, dass ein Dritter keine Möglichkeit hat aus einer verschlüsselten Nachricht Informationen zu erhalten. Die Nachricht hat dann ein kryptisches („unklar in seiner Ausdrucksweise oder Darstellung und daher schwer zu deuten, dem Verständnis Schwierigkeiten bereitend“[1]) Aussehen und der Angreifer bzw. der eigentlich Unbefugte für diese Nachricht versucht diese dann mittels kryptoanalytischer Methoden wieder lesbar zu machen. Es gibt also zwei große Bereiche in der Kryptologie zu einem die Kryptographie und Kryptoanalyse, welche im folgenden Abschnitt näher erläutert werden.

[1] [Dud13]

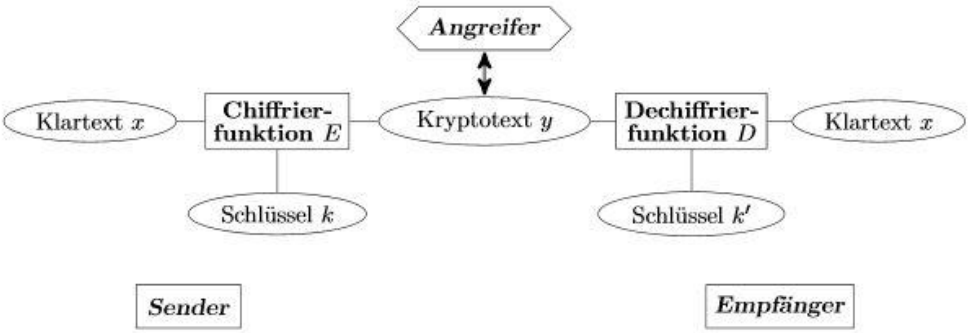

Abbildung 1 Kommunikationsschema[2]

2.1 Kryptographie

In der Kryptographie wird versucht Systeme und Verfahren zu entwickeln, die möglichst sicher sind. Die Abbildung 1 zeigt das typische Schema einer Kommunikation mit der Anwesenheit eines Angreifers der den Kryptotext y gerne entschlüsseln bzw. knacken möchte. Der Kryptotext y wurde dabei mittels der Chiffrierfunktion E erzeugt, die den Schlüssel k und den Ursprungsklartext x benötigt. Die Dechiffrierfunktion D generiert aus dem Kryptotext y und dem bekannten Schlüssel k‘ hingegen wieder den Klartext x. In der Kryptographie wird versucht die De- bzw. Chiffrierfunktionen so zu gestalten, dass ein Angreifer sehr lange braucht oder es auch gar nicht schafft den Schlüssel zu ermitteln.

Verfahren zum sichern von Informationen werden schon lange gesucht und einige klassische historische Beispiele wie die Caesar-Verschlüsselung oder die Enigma der deutschen im zweiten Weltkrieg haben viele schon gehört und wurden teilweise auch schon in Filmen behandelt z.B. „Enigma – Das Geheimnis“ oder „The Da Vinci Code – Sakrileg“.

2.2 Kryptoanalyse

Die Kryptoanalyse bemüht sich hingegen, um das Knacken eines Kryptotextes und versucht diese möglichst effizient zu lösen.

In der Kryptoanalyse wird unter anderem unterschieden zwischen mono- und polyalphabetischen Verschlüsselungen. Der Unterschied zwischen den beiden Verschlüsselungen ist, dass bei der monoalphabetischen Verschlüsselung das Eingabealphabet durch ein festes Ausgabealphabet substituiert wird und bei der polyalphabetischen Verschlüsselung durch unterschiedliche Elemente substituiert wird. Auf die Berechnung solcher Schlüssel wird im folgenden Kapitel genauer darauf eingegangen.

[2] [Köb12 S. 3]

Eines der wichtigsten Prinzipien ist das Kerckhoffsche Prinzip, welches im Wesentlichen besagt, dass der Angreifer das angewandte System kennt und nur der Schlüssel geheim gehalten werden muss.[3]

3 Methoden der Kryptoanalyse

Im folgenden Kapitel werden nun drei Methoden der Kryptoanalyse vorgestellt.

3.1 Brute-Force-Methode

Die Brute-Force-Methode versucht mit „roher Gewalt“ (aus dem engl. brute force) alle Möglichkeiten eines Schlüssels auszuprobieren. Ein Erfolg ist dann zum Beispiel erkennen, wenn ein Onlineanmeldeformular eine erfolgreiche Anmeldung zurückgibt.

Diese Methode ist sehr ineffizient, da es im worst-case bis zur letzten Kombination dauern kann bis der passende Schlüssel gefunden ist. Die Gefahr, dass der Angreifer entdeckt werden kann und der Schlüssel geändert wird ist bei dieser Methode besonders hoch.

3.2 Wörterbuch-Angriff

Beim Wörterbuch-Angriff wird eine Liste von möglichen Schlüsseln abgearbeitet, die z.B. häufige Passwörter in einem Sprachraum nutzt. Der Wörterbuch-Angriff ähnelt dem Brute-Force-Angriff sehr stark und das vorherige Beispiel kann auch in diesem Szenario angewendet werden.

Der Wörterbuch-Angriff ist schneller als der Brute-Force-Angriff, aber kann auch keinen Erfolg haben, falls der Schlüssel nicht in der Liste ist.

3.3 Statistische Analyse

Bei der statistischen Analyse wird z.B. die Häufigkeit eines gewissen Buchstabens ermittelt, um Rückschlüsse auf den Schlüssel ziehen zu können. Beispielsweise guckt man sich die Häufigkeitsverteilung der Buchstaben aus dem deutschen Alphabet an und stellt fest, dass die Buchstaben A, E, I, N, R, S und T besonders häufig vorkommen[4].

[3] vgl. [Köb12 S. 26]

[4] [Sch07 S. 45]

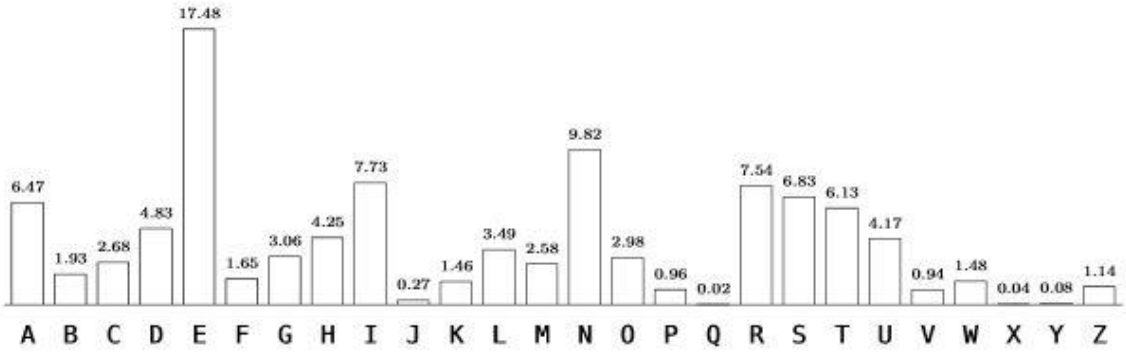

Abbildung 2 Häufigkeitsverteilung in Prozent[5]

Des Weiteren kann man diese Verteilungen auf Kombinationen ausweiten, sodass n-Gramme entstehen, dabei steht n für die Anzahl an Buchstabenkombinationen. Die wichtigsten n-Gramme sind Histogramm (n=1), Bigramm (n=2) und Trigramm (n=3).

Als Beispiel[6] dient folgender Kryptotext:

```
laoea ehoap hwvae ixobg jcbho thlob lokhe ixope vbcix ockix qoppo boapo
mohqc euogk opeho jhkpl eappj seobe ixoap opmcu
```

Tabelle 1 Absolute Häufigkeitsverteilung

x	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
H(x)	7	6	5	0	10	0	2	8	5	3	4	4	2	0	19	11	2	0	1	1	2	2	1	5	0	0

Da O und P die Buchstaben mit dem häufigsten Vorkommen sind und in Relation zur Abb. 1 setzt ist E => O und P => N. Bei dem Beispiel handelt es sich um eine einfache Substitutionschiffre, d.h. ein Buchstabe wird mit einer bestimmten Verschiebung durch einen anderen Buchstaben ersetzt. Um diese Verschiebung zu ermitteln lassen sich die Gleichungen I. b * E + c = O und II. b * N + c= P[7] aufstellen. Durch Subtraktion der ersten Gleichung I. von II. erhält man eine Kongruenz von 9*b=1 (ein Buchstabe hat dabei seinen Stellenwert im Alphabet z.B. O = 15). Daraus folgt als Schlüssel k=(3,2) und im Vergleich zur natürlichen Häufigkeit ist eine Übereinstimmung vorzufinden.

[5] [Köb12 S. 28]

[6] [Köb12 S. S.29f]

[7] Folgt aus der der Definition der affinen Chiffre [Köb12 S. 5ff.]

Tabelle 2 Vergleich Häufigkeit im Kryptotext [H(y)] und der natürlichen Häufigkeit [E(x)]

y	O	P	E	H	A	B	C	X	I	L	K	J	U	M	G	V	Q	S	T	W	R	F	N	Z	Y	D
H(y)	19	11	10	8	7	6	5	5	5	4	4	3	2	2	2	2	2	1	1	1	0	0	0	0	0	0
E(x)	17	10	7	6	8	8	6	4	3	5	4	3	3	3	1	1	1	3	0	0	2	2	1	1	0	0
x	E	N	S	T	I	R	A	H	C	D	U	L	G	M	K	P	W	O	X	Y	F	B	V	Z	Q	J

Dieses Verfahren ist erfolgreich gegen einfache Chiffren, aber findet seine grenzen bei komplexeren Stromchiffren wie der Vigenère-Chiffre. Bei Stromchiffren wird der Klartext periodisch mit dem Schlüssel verschlüsselt.

Beispiel:

Klartext: dertest Schlüssel: key

(dertest)+(keykeyk) = OJPEJQE

Um wieder Häufigkeitsanalysen verwenden zu können muss erst die Periode ermittelt werden, d.h. wann sich der Schlüssel wiederholt. Die älteste Methode ist der Kasiski-Test[8], welcher gleiche Teilfolgen ermittelt und deren Abstände zu einander. Durch eine Primfaktorzerlegung kann man einen größten gemeinsamen Teiler feststellen, welcher entweder selber die Länge des Schlüsselwortes ist oder die seiner Primfaktorzerlegung. Ein zu berücksichtigender Nachteil ist, dass es vorkommen kann, dass eine Primfaktorzerlegung sich stark von anderen Unterscheidet und man eventuell in die Irre geleitet werden kann und einen falschen Teiler bestimmt. Dies kann vorkommen wenn rein zufällige Kombinationen entstehen und von daher muss darauf geachtet werden das solche Ausnahmen ignoriert werden, damit die richtige Schlüssellänge ermittelt werden kann.

Der Friedmann-Test ist eine weitere Methode und kann die Ergebnisse des Kasiski-Tests bestätigen. Dazu wird unter anderem der Koinzedenzindex (IC) benutzt „welcher also die Wahrscheinlichkeit angibt, mit der man im Text y an zwei zufällig gewählten Positionen den gleichen Buchstaben vorfindet.“[9]. Dieser ist wie folgt definiert:

$$\mathrm{IC} = \frac{\sum_{i=A}^{Z} n_i(n_i - 1)}{N(N-1)}$$

Im Zähler wird n_i verwendet für die Häufigkeit des Vorkommens jedes einzelnen Buchstaben im Alphabet (A-Z) und im Nenner die Gesamtanzahl der Zeichen. Die daraus entstehende Zahl gibt Auskunft darüber, ob es sich um eine monoalphabetische (für die deutsche Sprache

[8] [Beu07 S. 32ff.]

[9] [Köb12 S. 34]

IC≥0,0762) oder polyalphabetische Verschlüsselung handelt. Das absolute Minimum beträgt dabei 0,0385.[10] Für die Länge l des Schlüsselwortes gilt:

$$l = \frac{(0{,}0762 - \frac{1}{26})n}{IC * (n-1) - 0{,}385n + 0{,}0762}$$

Da die Länge nun bekannt ist kann nun wieder mit Hilfe der Häufigkeitsanalyse der Schlüssel bestimmt werden und der Kryptotext entschlüsselt werden.

4 Cryptool 2

Im folgenden Kapitel werde ich das Cryptool 2 vorstellen.

4.1 Vorstellung

Das Cryptool 2 ist ein Open-Source Lehrprogramm, welches initial von der Universität Siegen entwickelt worden ist, und bietet verschiedene Möglichkeiten zur Veranschaulichung von Themen aus dem Gebiet der Kryptologie. Ich werde mich bei der Benutzung auf die Beta 10 des Cryptool 2 beziehen.

4.2 Statistische Analyse einer Vigenère Verschlüsselung

Im Cryptool 2 lässt sich die Vigenère-Verschlüsselung einfach analysieren mit Hilfe der bereits im vorherigen Kapitel vorgestellten Methode der statistischen Analyse.

Es ergibt sich folgender Aufbau:

[10] [Beu07 S. 38]

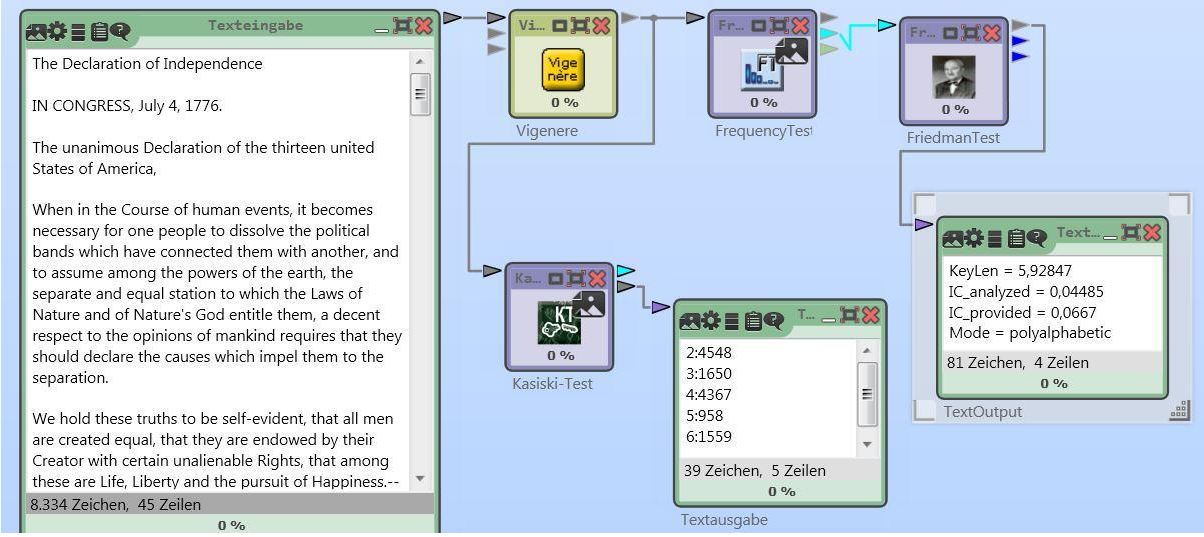

Abbildung 3 Versuchsaufbau der statistischen Analyse

Als Eingabeklartext können wir jeden beliebigen Text nutzen in diesem Fall nehmen wir die „Decleration Of Independence“ in englischer Sprache, welche in einem Textfeld eingebettet wird. Dieses wird mit dem Vigenère-Plugin verbunden und mit den Standardeinstellungen, aber mit dem Schlüssel AKEY (0, 10, 4, 24 als Zahlenfolge) betrieben. Der generierte Kryptotext wird mit dem Frequenzanalyse-Plugin auf die Buchstabenhäufigkeit analysiert und als Histogramm dargestellt.

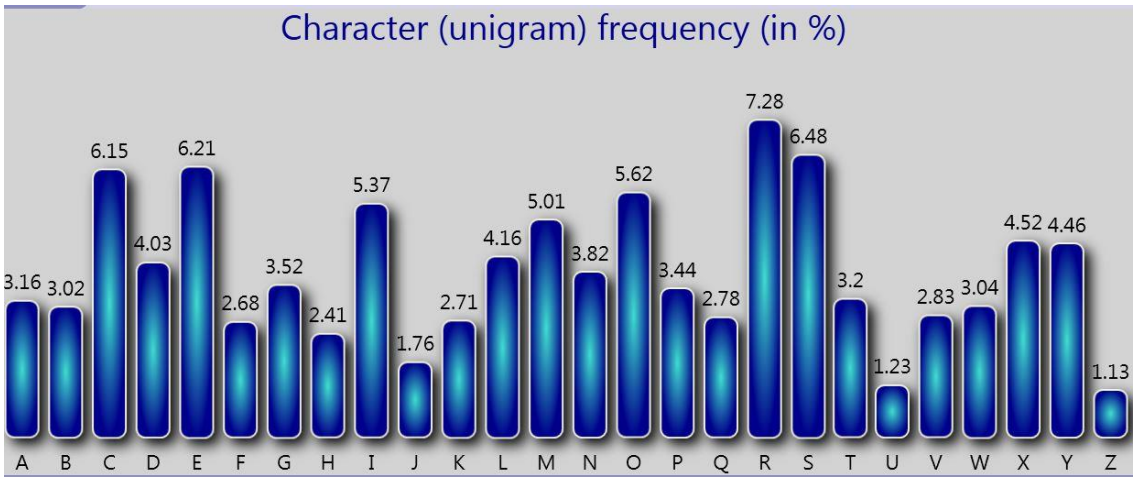

Abbildung 4 Histogramm des Kryptotextes

Der Friedman-Test wertet die ermittelte Buchstabenhäufigkeit aus und gibt für die Testdaten eine mögliche Schlüssellänge KeyLen = 5,92847, einen Koinzedenzindex in Bezug auf den Text von 0,04485 aus, welcher auf polyalphabetische Chiffre hinweist. Das Plugin hat ebenfalls

korrekt ermittelt, dass der Kryptotext in englischer Sprache vorliegt, da der errechnete Koinzedenzindex bei 0,0667 ($IC_{engl.}$ = 0,661[11]) liegt.

Zur verifizieren der Schlüssellänge wird noch ein Kasiski-Test ausgeführt, welcher eine Häufung 4-Gramme bei den Teilern zwei und vier ermittelt. Somit muss die Schlüssellänge zwei, vier oder vielfache von zwei lang sein.

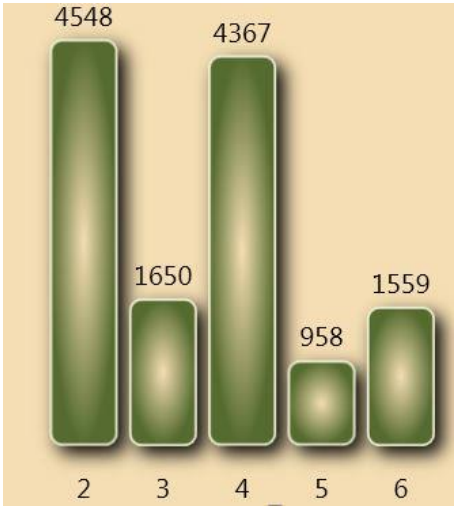

Abbildung 5 Kasiski-Test der Testdaten

Bei der Analyse stoßen wir darauf, dass manche Passagen sich ähneln z.B. die Folge „Ho“. Aus dem wissen (Kerckhoffs‘ Prinzip), dass es sich um eine Vigenère-Verschlüsselung handelt mit der Schlüssellänge vier, sind alle vier Zeichen gleich verschlüsselt. Zu beginn steht die Folge „Tri“, die bei der Überprüfung eines Trigramms der englischen Sprache z.B. „the“ entsprechen könnte. In der Annahme das also T = T verschlüsselt worden ist und das erste Zeichen des Schlüssels A ist, überprüfen wir das an anderen markanten Stellen. Die bereits genannte Folge „Ho“ und „Fe“ bieten sich an, da sie am Satzanfang stehen und wiederholt nach einem Vielfachen von vier auftreten. „Ho“ kommt nach $4 * n$ Zeichen vor und „Fe“ nach $4 * n + 1$ Zeichen vor, sodass also H=H und E=E ist. In Relation zu einander kann das engl. Wort he vermutet werden woraus folgt, dass F = H bei der Folge „Fe“ ist. Mithilfe des Vigenère-Quadrats kann ermittelt werden das Y der passende Teilschlüssel ist. Zusammenfassend ist der Schlüssel bisher als „A**Y“ ermittelt worden. Für die letzten beiden Schlüsselteile wird wieder nach Gemeinsamkeiten und Häufigkeiten gesucht, sodass letztendlich der Schlüssel wieder auf „AKEY“ zurückgeführt werden kann.

[11] [Kla04]

Vigenère-Quadrat

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

Abbildung 6 Vigenère Quadrat[12]

4.3 AES-Analyse mithilfe eines bekannten Klartextes

Zum analysieren einer modernen Verschlüsselung wähle ich AES aus und nehme an das ich einen Teil des Kryptotextes kenne. Zum Testen ist ein Szenario denkbar in dem ich meine Emails mit AES verschlüssele und immer mit meinem Namen beende. Ich schreibe zum Beispiel den Text „WieGehtesdirDominic“ mit AES (128Bit, ECB Modus) mit dem Schlüssel „00-01-02-03-04-05-06-07-08-09-0A-0B-0C-0D-0E-0F“ (der Bindestrich dient zur besseren Lesbarkeit) .

[12] [Wik14]

Da ich als Angreifer weiß, dass der Text immer mit Dominic endet überprüfe ich mit einem regulären Ausdruck, ob das verschlüsselte Muster „Dominic“ im Kryptotext vorliegt. Zu Testzwecken sei ein Teil des Schlüssels bekannt „00-01-02-03-**-**-**-**-**-09-0A-0B-0C-0D-0E-0F“. Das Schlüsselsucher-Plugin probiert jetzt alle Schlüssel aus (→ Brute-Force), in dem „Dominic“ mit den einzelnen Schlüsseln verschlüsselt wird und auf das resultierende Muster überprüft wird.

Selbst ein Heimcomputer ist dazu in der Lage eine große Menge an Schlüsseln zu berechnen und auszuprobieren.

Tabelle 3 Laufzeit verschiedener Konfigurationen

Konfiguration	Zeit	CPU	OpenCL[13]
PC mit CPU und Grafikkarte	ca. 3 Min.	ca. 19 Mill.	ca. 20 Mrd.
PC nur mit CPU (i5, 4 Kerne)	ca. 7 Min.	ca. 10 Mill.	
Laptop mit CPU und Grafikkarte	ca. 6 Min	ca. 10 Mill.	ca. 10 Mrd.
Laptop nur mit CPU (i7, 8 Kerne)	ca. 9 Min.	ca. 8 Mill.	

Es fällt deutlich auf, dass die Grafikkarte unter der Nutzung von OpenCL deutlich mehr Schlüssel ausprobieren kann als reine Prozessorleistung. Dies macht sich vor allem bemerkbar wenn weniger vom Schlüssel bekannt ist.

5 Fazit und Ausblick

5.1 Zusammenfassung

In meiner Arbeit hab ich zu beginn eine kurze Einführung in die Kryptologie und anschließend drei Methoden zur Kryptoanalyse mit dem Schwerpunkt auf die statistische Analyse vorgestellt. Im vierten Kapitel wurde das Cryptool 2 vorgestellt und mit Hilfe von zwei Beispielen eine Kryptoanalyse durchgeführt.

5.2 Ausblick

Die Kryptoanalyse wird weiterhin eine sehr wichtige Rolle haben, da es heutzutage wichtiger denn je ist sichere Systeme zu haben. Der NSA-Skandal[14] hat nicht zuletzt gezeigt, dass es wichtig Daten zu verschlüsseln und ein sicherer System zu haben, dass auch großer Rechenleistung stand hält wie sie zum Beispiel die NSA zur Verfügung hat. In der Zukunft wird eine immer größere Rechenleistung zur Verfügung stehen und die Entwicklung im Bereich der Quantencomputer wird neue Methoden zur Sicherheit bringen und die Kryptoanalyse vor neue Aufgaben stellen.

[13] Open Source Schnittstelle, um auf die Recheneinheit der Grafikkarte zu zugreifen.

[14] National Security Agency Geheimdienst der USA

Literaturverzeichnis

[Beu07] Beutelspracher, Albrecht. *Kryptologie. Eine Einführung in die Wissenschaft vom Verschlüsseln, Verbergen und Verheimlichen. Ohne alle Geheimniskrämerei, aber nicht ohne hinterlistigen Schalk, dargestellt zum Nutzen und Ergötzen des allgemeinen Publikums.* Wiesbaden : Springer Verlag, 2007.

[Cry13] Cryptool Online. [Online] 2013. [Zitat vom: 15. Dezember 2013.] http://www.cryptool-online.org.

[Dud13] Duden. [Online] 15. Dezember 2013. http://www.duden.de/rechtschreibung/kryptisch.

[Kla04] Pommerening, Klaus. Kryptologie. *Der Koinzidenzindex einer stochastischen Sprache.* [Online] 30. 11 2004. [Zitat vom: 2013. 12 16.] http://www.staff.uni-mainz.de/pommeren/Kryptologie/Klassisch/3_Koinz/KS.html.

[Köb12] Köbler, Prof. Dr. Johannes. *Einführung in die Kryptologie.* Humboldt-Universität zu Berlin, Berlin, Deutschland : s.n., 8. Februar 2012.

[Sch07] Schmeh, Klaus. *Kryptografie.* s.l. : dpunkt.verlag, 2007.

[Wik14] Wikipedia. *Polyalphabetische Substitution.* [Online] [Zitat vom: 28. Januar 2014.] http://de.wikipedia.org/wiki/Polyalphabetische_Substitution.