Vigenére knacken

Das Knacken der Vigenére-Verschlüsselung ist nicht so einfach wie bei der Caesar-Verschlüsselung, jedoch ähnlich, da auch hier eine Häufigkeitsanalyse stattfindet. Die Schwierigkeit ist aber, auf das Schlüsselwort zu kommen. Hier gibt es Möglichkeiten, die das Ermitteln des Schlüsselwortes überaus schwierig gestalten. Zunächst sollen jedoch einfache Schlüsselwörter betrachtet werden, um das Vorgehen einmal grundlegend zu verstehen.

Es sind drei Schritte notwendig, um die Verschlüsselung zu knacken:

1. Wiederkehrende Buchstabenfolgen im verschlüsselten Text werden gesucht.
2. Anschließend wird hiermit die Länge des Schlüsselwortes ermittelt.
3. Letztlich erfolgt dann die Bestimmung des Schlüsselwortes.

Wie aber auch schon bei der Häufigkeitsanalyse bei Caesar, fällt das Knacken leichter, wenn der Geheimtext sehr lang ist. Also wenn man eine große Datengrundlage benutzt.

Schritt 1: Wiederkehrende Buchstabenfolgen suchen

Der Geheimtext wir zunächst auf wiederkehrende Buchstabenfolgen untersucht. Diese sollten im Idealfall eine Mindestlänge von drei Buchstaben haben und innerhalb des Textes markiert werden. Die Buchstabenfolgen zeigen mit hoher Wahrscheinlichkeit, die gleichen Buchstaben des Geheimalphabets, mit dem verschlüsselt wurde. Das bedeutet, dass häufig vorkommende Buchstabenfolgen innerhalb des Geheimtextes auf häufig vorkommende Buchstabenfolgen (z. B. ein, der, die, das, sch …) aus der deutschen Sprache beruhen.

```
ETYJANSDUVYECVPRIDEIIYPMNQLGHPCXEIERINSXIXXIRLMIRPDAICOIIYQECSPVWP
YRETYWOWNLETYJANSIREPBTQZPGPYZOYMYCSDXAMPRBPDMTKEHIPTQMPCAIPOIRVZQ
MPYSBOTISPCIIYQECSEIXEYYNPTRFLNLZFVRANVINTDXWTCHSTNLZPTKEYLFECOMED
PVETYJANSITPIXIDEWINSIRPTRFLNLECKYKYLGKPYELDLRDPCIETYJANSITPIXEPTR
ETYJANSIRDNLLFPWSPWQANSXEDLYCSPMNQLGHPCIIYPRETYJANSINEPBTKFONLNOEY
ZFETYJANSSDPCRINSXETYJANSHIPDIRPTRFLNLEEPBTHTVDOTGHDTGHPCJOCOIRY
```

Schritt 2: Länge des Schlüsselwortes ermitteln

Nun wird für jede Buchstabenfolge ermittelt, wie groß der Abstand vom ersten Buchstaben der Buchstabenfolge zum erneuten Auftreten der Folge ist. Zum Beispiel wäre für XYZ der Abstand innerhalb von AA**XYZ**AAAA**XYZ**AAAAAA**XYZ**AA einmal Sieben und einmal Neun.

Aus der Tatsache, dass wiederkehrende Buchstabenfolgen innerhalb des Geheimtextes auf gleichen Buchstabenfolgen innerhalb des Klartextes zurückzuschließen sind, ergibt sich, dass die Länge des Schlüsselwortes ein Teiler des oben erwähnten Abstandes sein muss.

Das bedeutet, dass nun für jeden Abstand geschaut werden muss, welche Teiler dieser besitzt und welcher Teiler für alle Buchstabenfolgen in Frage kommen. Orientierung kann hier der ggT (größte gemeinsame Teiler) der einzelnen Abstände bieten. Wenn ein oder mehere Teiler gefunden wurden, dann wird die Länge des Schlüsselwortes einem davon entsprechen. Wenn mehrere Teiler in Frage kommen, muss Schritt 3 gegebenenfalls mehrfach durchgeführt werden, bis das Schlüsselwort ermittelt wurde.

Buchstabenfolge	Abstand vom ersten Buchstaben zum ersten Buchstaben	ggT der Abstände pro Buchstabenfolge
ETYJANS	$76 = 2^2 * 19$, $124 = 2^2 * 31$, $48 = 2^4 * 3$, $60 = 2^2 * 3 * 5$, $24 = 2^2 * 3$, $16 = 2^4$	2^2
IIY	$36 = 2^2 * 3^2$, $88 = 2^3 * 11$, $160 = 2^6 * 5$	2^2
NLE	$152 = 2^3 * 19$, $140 = 2^2 * 5 * 7$	2^2
PTRFL	$64 = 2^6$, $140 = 2^2 * 5 * 7$	2^2

Schritt 3: Schlüsselwort ermitteln

Da nun bekannt ist, wie Lang das Schlüsselwort ist, kann eine Häufigkeitsanalyse angewendet werden. Dafür wird der Text in Abschnitte von der Länge des Schlüsselwortes unterteilt. Da bei Vigenére der erste, zweite, dritte usw. Buchstabe eines solchen Abschnitts immer mit dem ersten, zweiten, dritten usw. Geheimalphabet verschlüsselt wurde, muss nun ermittelt werden, welcher Buchstabe innerhalb dieser Menge an Buchstaben am häufigsten vorkommt. Angenommen für den ersten Buchstaben des Schlüsselwortes ergibt sich, dass X am häufigsten verschlüsselt wurde, dann ist der Buchstabe gesucht, mit dem das E auf X abgebildet wird.

```
ETYJ ANSD UVYE CVPR IDEI IYPM NQLG HPCX EIER INSX IXXI RLMI RPDA
ICOI IYQE CSPV WPYR ETYW OWNL ETYJ ANSI REPB TQZP GPYZ OYMY CSDX
AMPR BPDM TKEH IPTQ MPCA IPOI RVZQ MPYS BOTI SPCI IYQE CSEI XEYY
NPTR FLNL ZFVR ANVI NTDX WTCH STNL ZPTK EYLF ECOM EDPV ETYJ ANSI
TPIX IDEW INSI RPTR FLNL ECKY KYLG KPYE LDLR DPCI ETYJ ANSI TPIX
EPTR ETYJ ANSI RDNL LFPW SPWQ ANSX EDLY CSPM NQLG HPCI IYPR ETYJ
ANSI NEPB TKFO NLNO EYZF ETYJ ANSS DPCR INSX ETYJ ANSH IPDI RPTR
FLNL EEPB THTV DOTG HDTG HPCJ OCOI RY
```

Buchstabe des Schlüsselwortes	Vorkommende Buchstaben mit ihrer Häufigkeit	Vermuteter Buchstabe des Schlüsselwortes
1. Buchstabe	**E** = 18, I = 14, A = 11, R = 8, …	E $\xrightarrow{A}$ E
2. Buchstabe	**P** = 24, N = 13, T = 12, Y = 9, …	E $\xrightarrow{L}$ P
3. Buchstabe	**Y** = 15, S = 12, P = 11, T = 10, …	E $\xrightarrow{U}$ Y
4. Buchstabe	**I** = 19, R = 12, J = 9, X = 8, …	E $\xrightarrow{E}$ I

In dem aufgeführten Beispiel ergibt sich also, dass das Schlüsselwort „ALUE“ sein soll. Das dieses Verfahren nicht immer auf anhieb den richtigen Schlüssel ergibt, lässt sich dann erkennen, wenn man versucht mit diesem Schlüsselwort zu ermitteln. Das eigentlich Schlüsselwort lautete nämlich „ALLE“ und das Verfahren zum Knacken der Verschlüsselung hätte sicherlich besser geklappt, wenn die Nachricht länger ist.

Entschlüsselt man nun den Text ergibt sich:

EINFACH ZU KNACKEN IST EIN EINFACHER TEXT NICHT IMMER ABER ES WIRD EINFACHER WENN EIN SOLCH EINFACHER TEXT FOLGEN VON BUCHSTABEN BESITZT DIE IMMER WIEDERKOMMEN

OB DIESER EINFACH TEXT NUN EINFACH ZU KNACKEN IST WIRD SICH ZEIGEN

ABER DIESER EINFACHE TEXT IST SICHER EINFACHER ZU KNACKEN ALS ANDERE EINFACHE TEXTE

EIN EINFACHER SCHLUESSEL MACHT ES AUCH EINFACHER EINEN EINFACHEN TEXT ZU KNACKEN

OB EINFACH ODER NICHT EINFACH DIESER EINFACHE TEXT WIRD DICH SICHER FORDERN

Aufgabe 1

Knacke die Verschlüsselung anhand des folgenden Textes und entschlüssle die ersten Zeilen des Geheimtextes[1]:

PWTMYTBADKDGPWPFYWFGUESOTLUPNVYWAPKCSOOJWWASTLSUZUSJMJBBRS
TIMGPYSXOJWWASMMZQLCHJQWGYDHKOJWWASTMFPADWIPVKLHONZWPDPWRA
AGQPRKNJCNPKGPJJLTHYOWOHPGYJWCUEKUZLGAOWKHOGPESMZMRWPBKVFV
ZTQNLAGSFSMVWTDPWRAAGQPRKNJCNPTGTKEOMSGVLYVCHKBVKLOFOBLGNC
IVXWPLYBZAAEOOWKEWEODZKZOGPWGOMSWMPWTIFFLCTUTYGUOSLZSILYOH
EWEODSRVVYHSFAVVHHWGIPTGHYHCWJVLERGJWKPDHGJWTUTQNBXGZEUKTW
IAZPPMOGPWGJQWGYDHKNJCNPSOVWTZPFOMNQUQFGOWPYTQNBAIVOSXNSNZ
NVHMSPAHCXBWVDTFJRWFLASXAGPHYHCWJVLEOANWKUPTXIYGUFFSQLLHZR
KZFGPYTXIYGUOWKVAEOEAOBBCVOSXVWKUMSGVLYVCHKBOGYOSTSGGUYSTA
APKYWIPLBBRSRIKULYJUVWKUPFHMDKLMWMMFRLCGUVKQSWAGVVWYNVLZSI
LYROMKKJSBAZSWMOWKHMILSCKZAIRPWZHMGPYSXLWTNCIVXWPIPNOMZGUS
SXIMUIPYUUEGUKICMDEOPFMZMRWPGOMYGOZSXBOKLGWKTWHYLUKVEWZDAG
VEKUOSYBWPZDHKTDGUFBJEWNJSSLZSILYYUMFPAPAGVKVLWZKV

Tipp: Von den interessanten Buchstabenfolgen wurde das erste Vorkommen bereits markiert. In Schritt 2 sollte nicht nur auf den ggT geachtet werden, sondern eher auf alle vorkommenden Teiler.

Buchstabenfolge	Abstand vom ersten Buchstaben zum ersten Buchstaben	ggT der Abstände pro Buchstabenfolge
OJWWAS		

[1] QUELLE: http://medienwissenschaft.uni-bayreuth.de/inik/email_nur_fuer_dich/3_verschluesseln/3.2_Vigenere/AB%20Vigenere%20knacken.pdf

TXIYGU		
YHCWJVLE		
QPRKNJ		
AEO		
PWT		

Buchstabe des Schlüsselwortes	Vorkommende Buchstaben mit ihrer Häufigkeit	Vermuteter Buchstabe des Schlüsselwortes
1. Buchstabe		E →
2. Buchstabe		E →
3. Buchstabe		E →

Das Schlüsselwort lautet: _____

Die ersten Zeilen des Klartextes lauten:

_____

_____

_____

_____