Vigenère- und Hill-Chiffre

Biografie Vigenère Blaise de Vigenère wurde am 15.04.1523 in Saint-Pourçain geboren. Im Rahmen seiner Tätigkeit als Diplomat in Rom kam er mit der Kryptographie in Kontakt, der er sich ab 1570 - nach seinem Ausscheiden aus dem diplomatischen Dienst - vollständig widmete. Er starb im Jahr 1596.

Abbildung 1: Blaise de Vigenère

Biografie Hill Lester Sanders Hill wurde am 19.01.1890 in New York City geboren. Er beendete sein Studium an der Columbia University im Jahr 1913. Im Laufe seines Lebens lehrte er an verschiedenen Universitäten, unter anderem der University of Montana, Princeton und Yale, wo er 1926 seine Dissertation „Properties of Certain Aggregate Functions“ schrieb. Zudem war er im ersten Weltkrieg in der US Naval Reserve, seine Beiträge wurden allerdings erst nach seinem Tod veröffentlicht. Der Großteil seiner Arbeit ist bis heute nicht veröffentlicht worden, da er nach wie vor als streng vertraulich eingestuft ist.

Biografie Kasiski Friedrich Wilhelm Kasiski wurde am 29.11.2805 in Westpreußen geboren. Er war Infanteriemajor und beschäftigte sich zudem mit Kryptographie. Er starb am 22.05.1881 in Neustettin.

Biografie Friedman William F. Friedman wurde am 24.09.1891 in Kishinev, Russland, geboren und kam bereits 1892 in die Vereinigten Staaten. Nach seinem Studium an der Cornell University lehrte er zunächst, wurde dann aber von dem exzentrischen „Colonel“ George Fabyan für die Genetik-Abteilung geworben, welches Labore für private Forschung in Illinois betrieb. Dort entwickelte sich seine Neigung für die Kryptologie und er wurde in kurzer Zeit zum Abteilungsleiter der Chiffrenabteilung. Auch Friedman arbeitete im und nach dem ersten Weltkrieg für die Armee und die Nationale Sicherheit, wo er ebenfalls schnell aufstieg. Seine wahrscheinlich größte Leistung war der von ihm gegangene Schritt von der traditionellen Kryptologie hin zu modernen Methoden unter Verwendung der Mathematik, insbesondere der Statistik. Am 2. November 1969 starb William F. Friedman in Washington, D.C. [1]

Abbildung 2: William F. Friedman

[1] aus: Cryptological Mathematics, Robert E. Lewand - SK170 L669

Historischer Überblick Europa im 15. und 16. Jahrhundert: Die monoalphabetische Chiffre ist entziffert und professionelle Kryptoanalytiker entziffern täglich die vertraulichen Briefe, welche durch Europa verschickt werden. Zudem entwickelt sich die Telegrafie zu einem wichtigen Übermittlungsverfahren von Informationen. Leon Battista Alberti (**1404*), ein florentiner Mathematiker, Maler, Komponist, Dichter, Philosoph und Architekt, äußerte als erster die Idee, mehrere Alphabete beim Codieren zu kombinieren. Dieser Gedanke wurde anschließend noch von Johannes Trithemius (**1492, deutscher Abt*) und Giovanni Porta (**1525, ital. Wissenschaftler*) weitergeführt, bis schließlich Blaise de Vigenère (**1525*) aus der Idee ein ausgefeiltes System machte und auch veröffentlichte. Dennoch wurden bis ins 18. Jahrhundert hinein weiterhin Varianten der monoalphabetischen Verschlüsselung verwendet, zum Beispiel die `Grande Chiffre` von Ludwig XIV, entwickelt von den Rossignols. Insbesondere die Varianten der homophonen Verschlüsselung sollten die Häufigkeitsanalyse zunichte machen, aber indem man nicht die Häufigkeit von Buchstaben, sondern die von Buchstabenverbindungen untersuchte, war diese Verschlüsselung nicht von Erfolg gekrönt. Als die Telegrafie ausgereift war griff man letztlich doch auf die Vigenère-Verschlüsselung zurück, welche `le chiffre indéchiffrable` genannt wurde.

Übungsaufgaben Vigenère-Chiffre:

1. Aller Anfang ist leicht: Dieser Text wurde mit dem Schlüsselwort `SINGH` verschlüsselt:
   `YMFZLJVJGYZMHZLFWPNTGZTKU`

2. Für Profis: Welche Länge hat wohl das Schlüsselwort für den folgenden Text?

```
EVLMMHVHWZ BWNXZVEXXA OGOWWMUYKE JKANLFDZNY EVHLUIFYGW
OEUFWOSLNL VJNKMHNUKN JVFUWSLYAE UZGZSOQYGD BEXHTTVCGW
SKOZWOUOGV TVCGWNMYKK URHWWSNUKW JEGNKUVLWW SJCMLMZWAC
FZNWWSCUGY NLNNFESYLU IVCWWOYYBL NRHAGFINXA IEFHTFEGTF
IFYKLFZBGH SVCLWORFLW JEYGNJVLYM FJMBYFEHTL IRHWWONYBK
FEYKOBIYBF XRBKWTYOGV FAOPWMJIXZ SCCVZVEXMJ FLYBFFJWAG
FEYLWFCUNU IJWAWOBNXK FZHAWSICGS MCYGKULYVC FECAEWFFEW
TMYKLSROXF FIEHFOKYBZ OJWAADBYGK PXUKRVDZEW JJWAWSUYKW
ECYAMOUNKM HUUGFFZHXF IRYGYFBIKT JDGNFENIKA OUYKEFKTZW
SUULKDYIXF HVBTULKYKA OUZEWJJWAK DYUYXMVCLU IROVZTTBPW
JEYYDFZMVZ QRWDLFNCXD JVVEADYOGV MFWDWOUXTK GVNMYFIIVZ
FEXXJCIOMM TSYKMFYLMW LVCGWOBHHU IVHNFEIOAA HLHWKJTBXJ
NZNLLPZMVZ FIQNWSUYMJ VXYKFBTBAS VJYWAFBILL CRLXTVVLWW
EFWAMOKYKV FEBNFEVHPA SUAXXVEXXF BLWAWJEYFW OXYOGOCOFH
FEBNFEVHPA FLHMWSLHLY FDYBFFBIXL FINTYEZYUW OVCWZBIXXK
DYQXJFEIXL FIXBWPYHXK JEHYMFIMBL UCCVZFWLXM EVHBETZHGW
OIUNKDYCAJ MVVXFWVLZW VUYGNFIMVZ XFLXFIRNMW OJCVZTFFVZ
FIUVCFIAXY FEXXFCIOMM TUYKLSVONF ENUVCFIGBL TVCGWNBIKT
JDGTMMVHBU IKAXOJTBXF WFHWWNGZTV EVLIXMZWAL VEXXAOVMMS
HVMTDTVLDS NMIFXMVCLU IVLNFEJYBF FELNWDBQXY ORBFFBTBAS
VJYWSXRLWW SGFHWUQFBU IMIGSMCYGN FIMVZXFLGW OSYLLJVHNW
CVLYSMCYGV BNUKVJYGWW SBIKTNZNWW NWFXATTBXF UICLKFEXTX
```

```
JVFXFALVHV FEXBWMVWDW SJNXFCZMLW OLHWXSRMLT FXCXJJXOXT
FIXBWCVOMW XRLYKJTBWA FXUGRFYOGY SZAXEFLNXT SLNNKTRBTF
GRHZKEVGLU IROLHJVFSM NZNIZJCILG QYCLUIVLLW FCYGJVYXHU
IRFLWSJUAV BJMLGMTBXJ NRMLWOJUXE UCCVZFYOGV FJWAEBLMMW
OLHWXSRMLW OUUGSIDUNU IVLTFEVLFS ICTXAUKYBD VEXLHFZMMW
TVFUKUVCGW TTBHWQJYGC FLFFGSRFTM DYXNEFZHUJ VKOLSVTBWM
ELZKATJNLG SLZMOFYGNW UZAWWSDIKS MZMMBBSIXK FJVXATGCXD
LRHGNFIZNW IIYGMOUUVZ HCYBUIRFEW OJUXMHVNBW SVHGADYNZS
OQOGVHRLOG MCEHENVHBK UUYKLVXYGV IRZMWILHWW SWLBKTK
```

Hill-Chiffre:

1. Nicht viel schwerer: Der folgende Text wurde mit der folgenden Matrix verschlüsselt: $\begin{pmatrix} 5 & 6 \\ 2 & 3 \end{pmatrix}$ `SOKLSHKPNSOORCPLANFO`
2. Zu diesem Text der Hinweis: Es geht um Käse! (ä=ae)
   `MESUDTECWCSBWCHQSUDTJEQUDGT`
   `WKMADVFYKUNUVRAORIGMTKCUVECWCU`
   `ILWKAKMADTYICKQRAORIGMTKCUVECWCE`

Vigenère-Quadrat

	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

Figure 4 - Vigenère Table

Notation Wir halten uns in unserem Vortrag so weit es geht an die Notation des Stinson:

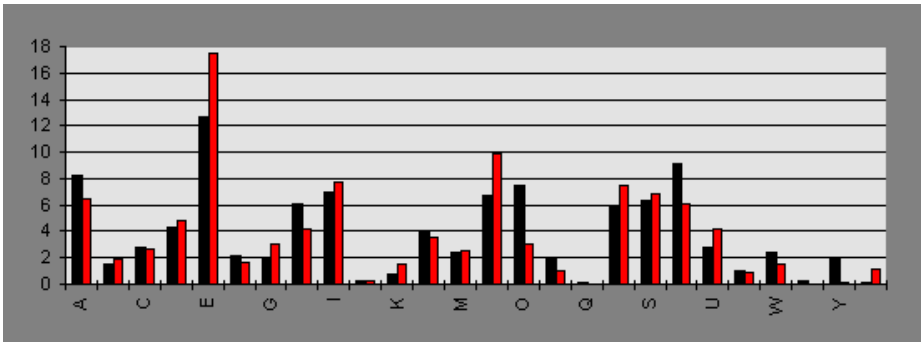
Ein Kryptosystem ist ein Tupel $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$, welches folgenden Konditionen genügt:

1. $\mathcal{P}$ ist eine endliche Menge möglicher Klartexte
2. $\mathcal{C}$ ist eine endliche Menge möglicher Geheimtexte
3. $\mathcal{K}$, der Schlüsselraum, ist eine endliche Menge möglicher Schlüssel
4. Für jedes $K \in \mathcal{K}$ gibt es eine Verschlüsselungsregel *(encryption rule)* $e_K \in \mathcal{E}$ und eine entsprechende Entschlüsselungsregel *(decryption rule)* $d_K \in \mathcal{D}$. Jedes $e_K : \mathcal{P} \to \mathcal{C}$ und $d_K : \mathcal{C} \to P$ sind Funktionen derart, dass $d_K(e_K(x)) = x$ für jedes Klartextelement $x \in \mathcal{P}$

Bei der Umwandlung des Alphabets in Zahlen modulo 26 soll folgende Tabelle gelten:

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Häufigkeitstabelle



Englische Sprache = schwarz
Deutsche Sprache = rot

Einteilung bekannter Verfahren

1. Die uns bisher bekannten Chiffrierverfahren unterteilt man in mono- und polyalphabetische Chiffren je nachdem ob jeder Buchstabe immer gleich chiffriert wird oder ob nach einem gewissen System zwischen den Alphabeten gewechselt wird. Die Caesar-Chiffre ist **monoalphabetisch**, die Vigenère-Chiffre hingegen ist **polyalphabetisch**.
2. Verschlüsselt man jeden Buchstaben einzeln, so nennt man das Verfahren **monographisch**. Ein Beispiel dafür ist die Vigenère-Chiffre. Chiffriert man ganze Buchstabengruppen zusammen, beispielsweise in der Hill-Chiffre, so spricht man von **polygraphischer** Verschlüsselung.

Quellen

1. Beutelspacher, Albrecht : Kryptologie : eine Einführung in die Wissenschaft vom Verschlüsseln, Verbergen und Verheimlichen - 3., behutsam verb. Aufl. . - Braunschweig [u. a.] : Vieweg, 1993.
SK 170 B569

2. Lewand, Robert Edward : Cryptological mathematics - Washington : Math. Assoc. of America, 2000. - ISBN: 0-88385-719-7
SK 170 L669

3. Singh, Simon : Geheime Botschaften : die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet - Darmstdt : Wiss. Buchges., 2000. - ISBN: 3-534-14978-5

4. Stinson, Douglas R. : Cryptography : theory and practice - 2. ed. . - Boca Raton [u.a.] : Chapmann & Hall [u.a.], 2002. - ISBN: 1-58488-206-9.
SK 170 S859