Stochastische Kryptoanalyse: Homophone Verschlüsselung

Ziele

Lernziele

Viele mono- und polyalphabetische Verschlüsselungen lassen sich durch die Häufigkeitsanalyse knacken. In dieser Unterrichtssequenz soll eine Methode gezeigt werden, welche dies erschwert oder unmöglich macht, ohne auf komplexere Methoden wie das Verfahren «One-Time-Pad» oder das Public-Key-Verschlüsselungsverfahren zurückzugreifen.

Eine monoalphabetische Verschlüsselung ist einfach zu dechiffrieren. Eine polyalphabetische hingegen homogenisiert die Häufigkeit der Buchstaben so, dass sie mit einer einfachen stochastischen Kryptoanalyse nicht entschlüsselt werden kann. Diese Chiffrierung ist in der Umsetzung sehr komplex und aufwändig. Es gilt einen Mittelweg zu finden. Das Verfahren sollte schwerer zu entschlüsseln sein als die monoalphabetische Verschlüsselung, in der Anwendung sollte es jedoch einfacher sein als die polyalphabetische Verschlüsselung. Die Lernenden lernen, neue Parameter für die stochastische Kryptoanalyse einzusetzen. Eine einfache Häufigkeitsanalyse reicht nicht mehr für das Entschlüsseln der Chiffre.

Voraussetzung

Bekannte Konzepte und Begriffe

Kryptosystem – Schlüssel – Chiffrierung: Ver (Klartext, Schlüssel) = Geheimtext - Dechiffrierung: Ent (Geheimtext, Schlüssel) = Klartext – Verschlüsselung – Entschlüsselung – Kryptotext – Klartextalphabet

Die zwei wichtigsten Chiffrierungsmethoden (Transposition und Substitution) sind bekannt. Das Prinzip einer monoalphabetischen und polyalphabetischen Geheimschrift ist bekannt.

Die Begriffe «relative Häufigkeit», «mittlere Häufigkeit» und «Häufigkeitsanalyse» sind den Lernenden bekannt aus dem Mathematikunterricht.

Die Lernenden kennen die Begriffe «Monogramme», «Bigramme», «Trigramme», «Tetragramme» und «Reverse» aus dem Sprachunterricht.

Einstiegsrätsel

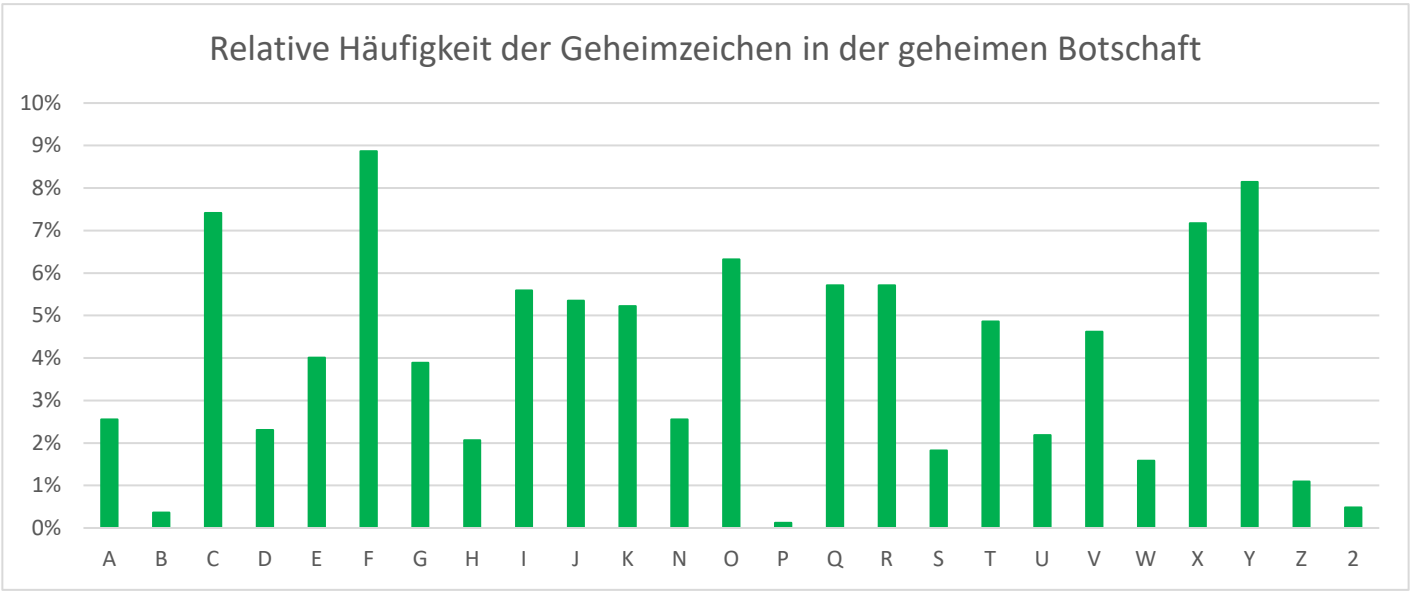
Rätsel

Im folgenden Text wurde der Buchstabe E durch 3 Zeichen ersetzt. Die Wörter im Klartext der Länge drei mit einem „N“ in der Mitte sind häufig ein UND. Die Häufigkeit des Vorkommens eines Buchstabens im deutschen Alphabet steht Ihnen zur Verfügung (Anhang). Es wurden keine Umlaute verwendet.

Führen Sie die Häufigkeitsanalyse durch und versuchen Sie, die geheime Botschaft zu entschlüsseln.

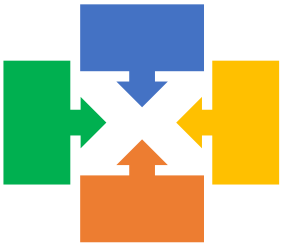
TOFJX CQUKX XHYQEI OIYT DVCCJY 2V OIY YGCAQKHHEIJF OEI UTWT
ROY TOF AGYW DOC KOFJD AVEITF VFR KOFJY ZSQXEIK NJOF
WYOFUT ROTXKX AGJYWEITF WOCCK 2VY UYGXXDVCCJY IOFQVX
XOT OXC AYQFA VFR XEINQEI VFR NOYR XOEI RQYVKWJY ZYKVJF PQ
RQX DGKEICJ OEI UTYFK CVF XQUCJ YGCAQKHHEITF 2V OIYJY DVCCKY
ROJ UYGXXDVCCKY NGIFCT RYQVXXJF OD NQSR KOFJ IQSWK XCVFRT
BGD RGYZ JFCZTYFC QSX YGCAQKHHEIJF RTF NQSR WKCYQC
WJUTUFKCJ OIY RTY NGSZ YGCAQJHHEIKF NVXXCT FOEIC RQXX JY
WGKXT NQY VFR ZVJYEICKCJ XOEI FOEIC BGY OID UVCTF CQU
YGCAQKHHEIJF XHYQEI TY XEIGKFJF RQFA NGSZ NG NOSSXC RV RTFF
IOF XG ZYVKI YGCAQJHHEITF 2VY UYGXXDVCCKY NQX CYQJUXC RV
RQ OF RTOFKD AGJYWEIKF AVEITF VFR NJOF RQDOC XOEI ROK
UYGXXDVCCTY RQYQF XCQJYAKF AQFF NG NGIFC RTFF RJOFK
UYGXXDVCCJY FGEI TOFK UVCJ BOTYCKSXCVFRJ NTOCKY OD NQSR
VFCJY RTF RYKO UYGXXJF TOEIKF XCJIC OIY IQVX XQUCT
YGCAQKHHEIJF RTY NGSZ RQEICK RQX AOFR NOYR DOY FGEI WJXXTY
XEIDKEAJF QSX ROT QSCK RV DVXXC ROY JOFTF HSQF QVXRKFAJF
RQXX RV WTORK JYNOXEITF AQFFXC

Tipp: Nutzen Sie die folgende Tabelle, die angibt, welche Zeichen in welcher Häufigkeit in der geheimen Botschaft vorkommen.



- Welche Strategie haben Sie gewählt?
- Welche Rolle hat dabei die Häufigkeitsanalyse gespielt?
- Welche Buchstaben haben Sie am schnellsten gefunden?
- Ist eine solche Verschlüsselung sinnvoll? Ist sie sicher?
- Könnte man diese Verschlüsselung automatisieren?

Homophone Verschlüsselung



Die homophone Verschlüsselung* (von altgriechisch ὅμος hómos „gleich“ und φωνή phoné „Stimme“ = „gleich klingend“) ist eine bereits im 17. Jahrhundert weit verbreitete monoalphabetische Verschlüsselungsmethode, bei der im Gegensatz zur einfachen monoalphabetischen Substitution die Klartextzeichen auch durch mehrere Geheimtextzeichen substituiert werden können.

Die wesentliche Schwäche der einfachen monoalphabetischen Substitution ist, dass jeder Klartextbuchstabe stets nur durch ein einziges Geheimtextzeichen verschlüsselt wird. Der so entstehende Geheimtext ist deshalb anfällig für statistische Angriffsmethoden. Beispielsweise genügt eine simple Häufigkeitszählung der Zeichen des Geheimtextes, um den in den meisten Sprachen am häufigsten vorkommenden Buchstaben E (Häufigkeit im Deutschen etwa 17.7 %) schnell zu identifizieren.

Diesem Angriff wirkt die homophone Verschlüsselung entgegen, indem sie mehrere Substitute für häufiger verwendete Buchstaben, wie zum Beispiel E oder N, erlaubt. Die homophone Verschlüsselung stellt somit eine kryptographische Verbesserung der einfachen monoalphabetischen Substitutionsverfahren dar und ist dabei immer noch leichter zu handhaben als eine polyalphabetische Substitution, bei der mehrere unterschiedliche Geheimalphabete zum Einsatz kommen.

Wie bei allen monoalphabetischen Substitutionsverfahren wird auch bei der homophonen Verschlüsselung nur ein einziges festes Substitutionsalphabet zur Ver- und Entschlüsselung verwendet. Um das Ziel, nämlich die Einebnung der unterschiedlichen Häufigkeiten der Klartextbuchstaben zu erreichen, kann man beispielsweise jedem Buchstaben des Alphabets so viele Geheimtextzeichen zuordnen, wie diese seiner relativen Häufigkeit in Prozent entsprechen, was ein Geheimtextalphabet von 100 Zeichen ergibt.

Für die homophone Chiffrierung gelten also folgende Regeln:

- Einem Klartext-Buchstaben wird nicht mehr nur ein Zeichen, sondern werden manchmal gleich eine Menge von Zeichen zugeordnet.
- Die Zuordnung muss eindeutig sein. Dasselbe Zeichen darf nicht für mehrere Buchstaben verwendet werden.
- Das Alphabet der Chiffre wird also mehr Zeichen enthalten als das Klartextalphabet.
- Die Häufigkeit der Zeichen in den Geheimtexten soll möglichst ausgeglichen sein.

* Quelle: https://de.wikipedia.org/wiki/Homophone_Verschl%C3%BCsselung

Beispiel

Bildet man nun die 26 Buchstaben des Alphabets auf 100 Geheimzeichen ab, im einfachsten Fall auf die Zahlen 00 bis 99, und zwar so, dass dem A fünf Geheimzeichen, dem B zwei, dem C drei, dem D fünf zugeordnet werden, und so weiter, so tritt im Geheimtext jede (Geheim-)Zahl mit einer mittleren Häufigkeit von 1 % auf. Eine Häufigkeitsanalyse der Einzelzeichen ergibt nun keine Ansatzpunkte mehr für die Entzifferung. Um den Text dennoch zu knacken, muss der Angreifer nun raffiniertere Methoden anwenden. Hierzu kann er anstelle von einzelnen Zeichen (Monogrammen) die Analyse auf Bigramme (Zeichenpaare), Trigramme oder Tetragramme ausweiten. Mögliche Angriffspunkte sind charakteristische Bigramme wie CH, CK oder QU sowie die Reversen EN und NE oder ER und RE. Hierzu benötigt er jedoch deutlich längere Texte. Hinreichend kurze, homophon verschlüsselte Texte (weniger als achtzig Buchstaben) sind gegen unbefugte Entzifferung recht gut geschützt.

Buchstabe	Geheimtext	Buchstabe	Geheimtext
A	10 21 52 59 71	N	30 35 43 62 63 67 68 72 77 79
B	20 34	O	02 05 82
C	28 06 80	P	31
D	04 19 70 81 87	Q	25
E	09 18 33 38 40 42 53 54 55 60 66 75 85 86 92 93 99	R	17 36 51 69 74 78 83
F	00 41	S	15 26 45 56 61 73 96
G	08 12 97	T	13 32 90 91 95 98
H	07 24 47 89	U	29 01 58
I	14 39 46 50 65 76 88 94	V	37
J	57	W	22
K	23	X	44
L	16 03 84	Y	48
M	27 11 49	Z	64

Aus der Geschichte

Mit der Verwendung homophoner Chiffren startete man einen der ersten Versuche, die statistische Analyse von Geheimtexten zu erschweren. Eine der bekanntesten historischen Anwendungen homophoner Verschlüsselungen ist die «Beale-Chiffre»*aus dem 19. Jahrhundert.

Diese besteht aus drei Teilen, von denen bis heute nur einer gebrochen werden konnte. Auch wenn die anderen beiden Teile wahrscheinlich eine Fälschung sind - die historischen Forschungsergebnisse erscheinen diesbezüglich sehr vage beziehungsweise nicht überzeugend - der zweite Teil der Chiffre als homophone Verschlüsselung gelöst werden. Dabei verwendete der Autor die Unabhängigkeitserklärung der USA als Schlüssel und suchte für jeden Klartextbuchstaben ein Wort mit demselben Anfangsbuchstaben in der Unabhängigkeitserklärung. Anschliessend ersetzte er den Buchstaben durch die Stelle des Wortes in der Unabhängigkeitserklärung. Da viele Worte in dieser mit demselben Buchstaben anfangen, entspricht dies einer homophonen Chiffre.

*Quelle: Günther, Christoph G.: A Universal Algorithm for Homophonic Coding

Auch in der Moderne wurden homophone Chiffren weiterhin betrachtet. Es gab die Idee, homophone Substitutionen zu verwenden, um bestehende Verschlüsselungsverfahren sicherer zu machen. So brachte man die Idee hervor, homophone Substitutionen vor einer Verschlüsselung mit dem damaligen Standard DES durchzuführen, um die statistische Analyse von DES zu erschweren.

Homophone Verschlüsselung: Aufgaben

1. Aufgabe (einfach)

Verschlüsseln Sie einen eigenen Text mit dem Geheimalphabet des Beispiels. Benutzen Sie dafür ein Tabellenkalkulationsprogramm. Versuchen Sie, die Aufgabe möglichst effizient zu lösen. Welche Funktionen stehen Ihnen dafür zur Verfügung?

2. Aufgabe (anspruchsvoll)

Sie möchten ein Programm entwickeln, das Klartexte mit der Geheimschrift chiffriert. Beschreiben Sie zuerst Ihre Lösungsidee mit eigenen Wörtern.
Schreiben Sie anschliessend das Lösungsverfahren, den Algorithmus auf. Damit haben Sie die Vorarbeiten für das Programmieren bereits geleistet.

3. Aufgabe (anspruchsvoll)

Im folgenden Text wurde jeder Buchstabe durch 2 Ziffern codiert. 03 steht zum Beispiel für einen Buchstaben.

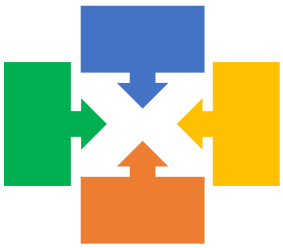
Versuchen Sie, die geheime Botschaft zu entschlüsseln.
So viel kann verraten werden:
35 steht für den Buchstaben Q.

03-24-19 84-95-46-00-26-50 58-30-85 03-83-64 35-34-98-27-18-45 62-74-96 78-95-74-96-06-91 34-71-03 13-44-77 56-19-60-71-03 33-18-22 61-05-30-14-40-82-11 35-61-67-18-57-38. 93-02 50-36-34-07-01-64 04-76-85 14-42 98-58-00-23-33-48-68 20-49-94-74-11-06-90-41 34-05-13 60-00-92-57-35-60-24-59. 55-80 20-94-27-22 59-04-97 35-60-31-81-84-43-58-18-92-57-77 89-44-77-56-58-23-97-45-75 28-82-40-62-14-38 63-07-13 35-61-09-18-89-94-22-27 43-08-82-80-92-57-05. 66-63 01-88-14-17-14-59 66-28-24-81-84 73-33-78-87-72 28-83-80 45-37-54-82-72 02-95-10-19-13-57-40 79-38-85-17-46-38-01-55-97, 62-87-80 20-97-31-75-17 43-48-68-99-06-18-18 33-56-37-55-11-08 61-72-03 35-34-09-18-83-75-33-49-37-89 50-63-69-64 53-40-92-10-58-97 22-98-88-17-69-31-49. 13-64-71 29-11-15-99-66-79-99 61-72-62 41-58-10 35-63-16-16-90 76-95-22-22 10-80 89-24-40-43-81-65-95-72-46-00

4. Frage

Mit welcher Strategie suchen Sie nach dem Vorhandensein des Buchstaben Q? Besprechen Sie diese Frage im Team.

Zusammenfassung /wichtige Begriffe



Was haben wir gelernt?

Homophone Verschlüsselungen sind eine besondere Form der monoalphabetischen Substitutionschiffren. Der Unterschied ist, dass bei homophonen Verschlüsselungen das Geheimtextalphabet grösser sein kann als das Klartextalphabet. So kann es für jeden Klartextbuchstaben mehrere Geheimtextbuchstaben geben, auf die dieser abgebildet werden kann. Die Geheimtextbuchstaben heissen Homophone. Die Anfälligkeit für statistische Angriffsmethoden wird dadurch reduziert, dass für die stochastische Kryptoanalyse mehrere Parameter betrachtet werden müssen. Die Häufigkeit des Vorkommens der einzelnen Buchstaben ist nicht mehr relevant beziehungsweise hilfreich für die Kryptoanalyse. Vielmehr muss man Bigrammen oder sogar Trigrammen Beachtung schenken.

Weil einem Klartextbuchstaben mehrere Geheimtextsymbole zugeordnet werden können, muss man sich darüber hinaus eine Strategie überlegen, welche der vorhandenen Möglichkeiten man zu welchem Zeitpunkt aussucht. Die eine Strategie ist, immer zufällig einen passenden Geheimtextbuch-staben zu wählen. Die andere Methode ist, die Geheimtextbuchstaben abwechselnd zu nutzen. Bei dem ersten Vorkommen eines Buchstabens im Klartext wird der erste zu diesem Buchstaben passende Geheimtextbuchstabe gewählt. Kommt der Buchstabe danach erneut vor, wird der zweite Geheimtextbuchstabe gewählt. Eine Möglichkeit, homophone Chiffren mit Stift und Papier anzugreifen, ist, zu versuchen, Wörter in dem Geheimtext zu finden. Ist ein Wort gefunden, so kann man die weiteren Vorkommen der somit festgelegten Homophone betrachten und versuchen, weitere Wörter zu finden. Diese Abschätzung
und auch das Erkennen der Wörter im Text erfordern menschliche Fähigkeiten, wodurch dieser Angriff nicht einfach auf Computersysteme übertragbar ist.

Lösungen

Eingangsrätsel:

Die Chiffrierung von «n» ist der häufigste Buchstabe im Geheimtext, weil «e» durch drei unterschiedliche Zeichen chiffriert wird. Somit ordnet man dem häufigsten Buchstaben «F» des Geheimtextes den Buchstaben «n» zu.

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
													F												

Das liefert das Zwischenergebnis:

TOnJX CQUKX XHYQEI OIYT DVCCJY 2V OIY YGCAQKHHEIJn OEI UTWT
ROY TOn AGYW DOC KOnJD AVEITn VnR KOnJY ZSQXEIK NJOn
WYOnUT ROTXKX AGJYWEITn WOCCK 2VY UYGXXDVCCJY IOnQVX
XOT OXC AYQnA VnR XEINQEI VnR NOYR XOEI RQYVKWJY ZYKVJn PQ
RQX DGKEICJ OEI UTYnK CVn XQUCJ YGCAQKHHEITn 2V OIYJY
DVCCKY
ROJ UYGXXDVCCKY NGInCT RYQVXXJn OD NQSR KOnJ IQSWK XCVnRT
BGD RGYZ JnCZTYnC QSX YGCAQKHHEIJn RTn NQSR WKCYQC
WJUTUnKCJ OIY RTY NGSZ YGCAQJHHEIKn NVXXCT nOEIC RQXX JY
WGKXT NQY VnR ZVJYEICKCJ XOEI nOEIC BGY OID UVCTn CQU
YGCAQKHHEIJn XHYQEI TY XEIGKnJn RQnA NGSZ NG NOSSXC RV
RTnn IOn XG ZYVKI YGCAQJHHEITn 2VY UYGXXDVCCKY NQX CYQJUXC
RV RQ On RTOnKD AGJYWEIKn AVEITn VnR NJOn RQDOC XOEI ROK
UYGXXDVCCTY RQYQn XCQJYAKn AQnn NG NGInC RTnn RJOnK
UYGXXDVCCJY nGEI TOnK UVCJ BOTYCKSXCVnRJ NTOCKY OD NQSR
VnCJY RTn RYKO UYGXXJn TOEIKn XCJIC OIY IQVX XQUCT
YGCAQKHHEIJn RTY NGSZ RQEICK RQX AOnR NOYR DOY nGEI WJXXTY
XEIDKEAJn QSX ROT QSCK RV DVXXC ROY JOnTn HSQn QVXRKnAJn
RQXX RV WTORK JYNOXEITn AQnnXC

Als Nächstes fallen die Wörter mit drei Buchstaben und einem «n» in der Mitte auf: VnR. Es gibt nur wenige solcher Wörter in der deutschen Sprache. Das allerhäufigste davon ist «und» (neben «uns», «eng» und «uni»). Vermutlich steht also V für «u» und R für «d».

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
			R										F							V					

Damit erhält man:

TOnJX CQUKX XHYQEI OIYT DuCCJY 2u OIY YGCAQKHHEIJn OEI UTWT
dOY TOn AGYW DOC KOnJD AuEITn und KOnJY ZSQXEIK NJOn
WYOnUT dOTXKX AGJYWEITn WOCCK 2uY UYGXXDuCCJY IOnQuX
XOT OXC AYQnA und XEINQEI und NOYd XOEI dQYuKWJY ZYKuJn PQ
dQX DGKEICJ OEI UTYnK Cun XQUCJ YGCAQKHHEITn 2u OIYJY DuCCKY
dOJ UYGXXDuCCKY NGInCT dYQuXXJn OD NQSd KOnJ IQSWK XCundT
BGD dGYZ JnCZTYnC QSX YGCAQKHHEIJn dTn NQSd WKCYQC

WJUTUnKCJ OIY dTY NGSZ YGCAQJHHEIKn NuXXCT nOEIC dQXX JY
WGKXT NQY und ZuJYEICKCJ XOEI nOEIC BGY OID UuCTn CQU
YGCAQKHHEIJn XHYQEI TY XEIGKnJn dQnA NGSZ NG NOSSXC du dTnn
IOn XG ZYuKI YGCAQJHHEITn 2uY UYGXXDuCCKY NQX CYQJUXC du
dQ On dTOnKD AGJYWEIKn AuEITn und NJOn dQDOC XOEI dOK
UYGXXDuCCTY dQYQn XCQJYAKn AQnn NG NGInC dTnn dJOnK
UYGXXDuCCJY nGEI TOnK UuCJ BOTYCKSXCundJ NTOCKY OD NQSd
unCJY dTn dYKO UYGXXJn TOEIKn XCJIC OIY IQuX XQUCT
YGCAQKHHEIJn dTY NGSZ dQEICK dQX AOnd NOYd DOY nGEI WJXXTY
XEIDKEAJn QSX dOT QSCK du DuXXC dOY JOnTn HSQn QuXdKnAJn
dQXX du WTOdK JYNOXEITn AQnnXC

Nun kann man weitere kurze Wörter mit teilweise enttarnten Buchstaben untersuchen. So steht beispielsweise «2u» für «zu», «Cun» für «tun», «dTn» für «den». Auffallend ist auch das «dQXX», das wegen des Doppelbuchstabens am Schluss vermutlich für «dass» steht.

eOnJs taUKs sHYaEI OIYe DuttJY zu OIY YGtAaKHHEIJn OEI UeWe dOY
eOn AGYW DOt KOnJD AuEIen und KOnJY ZSasEIK NJOn WYOnUe
dOesKs AGJYWEIen WOttK zuY UYGssDuttJY IOnaus sOe Ost AYanA
und sEINaEI und NOYd sOEI daYuKWJY ZYKuJn Pa das DGKEItJ OEI
UeYnK tun saUtJ YGtAaKHHEIen zu OIYJY DuttKY
dOJ UYGssDuttKY NGInte dYaussJn OD NaSd KOnJ IaSWK stunde BGD
dGYZ JntZeYnt aSs YGtAaKHHEIJn den NaSd WKtYat WJUeUnKtJ OIY
deY NGSZ YGtAaJHHEIKn Nusste nOEIt dass JY WGKse NaY und
ZuJYEItKtJ sOEI nOEIt BGY OID Uuten taU YGtAaKHHEIJn sHYaEI eY
sEIGKnJn danA NGSZ NG NOSSst du denn IOn sG ZYuKI YGtAaJHHEIen
zuY UYGssDuttKY Nas tYaJUst du da On deOnKD AGJYWEIKn AuEIen
und NJOn daDOt sOEI dOK UYGssDutteY daYan staJYAKn Aann NG
NGInt denn dJOnK UYGssDuttJY nGEI eOnK UutJ BOeYtKSstundJ
NeOtKY OD NaSd untJY den dYKO UYGssJn eOEIKn stJIt OIY Iaus saUte
YGtAaKHHEIJn deY NGSZ daEItK das AOnd NOYd DOY nGEI WJsseY
sEIDKEAJn aSs dOe aStK du Dusst dOY JOnen HSan ausdKnAJn dass du
WeOdK JYNOsEIen Aannst

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
Q	W	E	R	T J K	Z	U	I	O	P	A	S	D	F	G	H	L	Y	X	C	V	B	N	M	1	2

Ab jetzt erkennt man immer mehr Wörter und der Text lässt sich leicht entschlüsseln. Aufmerksame Lernende werden auch schon bald die Gestalt des Schlüssels wiedererkennen...

eines tages sprach ihre mutter zu ihr rotkaeppchen ich gebe dir einen
korb mit einem kuchen und einer flasche wein bringe dieses
koerbchen bitte zur grossmutter hinaus sie ist krank und schwach

und wird sich darueber freuen ja das moechte ich gerne tun sagte rotkaeppchen zu ihrer mutter
die grosssmutter wohnte draussen im wald eine halbe stunde vom dorf entfernt als rotkaeppchen den Wald betrat begegnete ihr der wolf rotkaeppchen wusste nicht dass er boese war und fuerchtete sich nicht vor ihm guten tag rotkaeppchen sprach er schoenen dank wolf wo willst du denn hin so frueh rotkaeppchen zur grossmutter was traegst du da in deinem koerbchen kuchen und wein damit sich die grossmutter daran staerken kann wo wohnt denn deine grossmutter noch eine gute viertelstunde weiter im wald unter den drei grossen eichen steht ihr haus sagte rotkaeppchen der wolf dachte das kind wird mir noch besser schmecken als die alte du musst dir einen plan ausdenken dass du beide erwischen kannst

Aufgabe 3

Wenn man alle 35 durch Q ersetzt, alle Folgezahlen durch U und alle Wörter der Länge drei, die mit U beginnen, als «UND» vermutet, entdeckt man ein Wort der Form QU-16-16-N. Die 16 steht also für «E». Einige naheliegende Ersetzungen später sieht der Text so aus:

d-24-19 84-95-e-n-26-50 58-30-85 d-i-e q-u-98-27-18-45 d-74-96 78-95-74-96-06-91 u-n-d d-44-77 56-19-u-n-d 33-18-22 u-n-30-14-40-82-11 q-u-67-18-57-38. 93-02 50-36-u-n-01-e 04-76-85 14-42 98-58-n-23-33-48-68 20-49-94-74-11-06-n-41 u-n-d u-n-92-57-q-u-24-59. 55-80 20-94-27-22 59-04-97 q-u-31-81-84-43-58-18-92-57-77 89-44-77-56-58-23-97-45-75 28-82-40-d-14-38 u-n-d q-u-09-18-89-94-22-27 43-08-82-80-92-57-n. z-u 01-88-14-17-14-59 z-28-24-81-84 73-33-78-87-n 28-i-80 45-37-54-82-n 02-95-10-19-d-57-40 79-38-85-17-e-38-01-55-97, d-87-80 20-97-31-75-17 43-48-68-99-06-18-18 33-56-37-55-11-08 u-n-d q-u-09-18-i-75-33-49-37-89 50-u-69-e 53-40-92-10-58-97 22-98-88-17-69-31-49. d-e-n 29-11-15-99-z-79-99 u-n-d 41-58-10 q-u-e-e-n 76-95-22-22 10-80 89-24-40-43-81-65-95-n-e-n

Ab diesem Zeitpunkt wird die Entschlüsselung schwieriger. Das erste Wort «d-24-19» könnte ein Artikel sein. Ausserdem kommt die Kombination «...-q-u-24-...» vor, die darauf hindeutet, dass 24 für einen Vokal steht. «24 = a» und «24 =i» liefern unsinnige Ergebnisse, also steht 24 wohl für ein «e».

Mit ähnlichen Überlegungen und viel Geduld kann man den Klartext schliesslich finden:

d-e-r k-o-e-n-i-g i-s-t d-i-e q-u-e-l-l-e d-e-s b-o-e-s-e-n u-n-d d-e-r g-r-u-n-d a-l-l u-n-s-e-r-e-r q-u-a-l-e-n. i-m g-r-u-n-d-e i-s-t e-r e-i-n-f-a-c-h s-t-o-e-r-e-n-d u-n-d u-n-b-e-q-u-e-m. e-r s-o-l-l m-i-t q-u-e-c-k-s-i-l-b-e-r v-e-r-g-i-f-t-e-t w-e-r-d-e-n u-n-d q-u-a-l-v-o-l-l s-t-e-r-b-e-n. z-u d-i-e-s-e-m z-w-e-c-k h-a-b-e-n w-i-r e-i-n-e-n m-o-e-r-d-e-r e-n-t-s-e-n-d-e-t, d-e-r s-t-e-t-s s-c-h-n-e-l-l a-g-i-e-r-t u-n-d q-u-a-l-i-t-a-t-i-v g-u-t-e a-r-b-e-i-t l-e-i-s-t-e-t. d-e-n p-r-i-n-z-e-n u-n-d d-i-e q-u-e-e-n s-o-l-l e-r v-e-r-s-c-h-o-n-e-n