

## Allgemeines

Die Kryptologie lässt sich in drei Teilbereiche aufgliedern:

- Kryptographie,
- Kryptoanalyse und
- Steganographie.

Die Begriffe Kryptologie und Kryptographie sind aus den griechischen Wörtern *kryptos* (geheim), *logos* (das Wort, der Sinn) und *graphein* (schreiben) gebildet.

Die **Kryptographie** ist die Wissenschaft von der Datenverschlüsselung. Eine Nachricht wird unverständlich gemacht. Obwohl der verschlüsselte Text noch buchstabenweise lesbar ist, ist aber inhaltlich nur noch „Kauderwelsch“ erkennbar. Man spricht von „offenen Geheimschriften“.

Die Hauptaufgabe besteht darin, dass aus einem Geheimtext  $G$  der Klartext  $K$  für Dritte nicht oder nur schwer rekonstruierbar wird. Mathematisch ist die Verschlüsselung  $V$  eine Funktion, die einem Klartext  $K$  einen Geheimtext  $G$  zuordnet:

$$G = V(K).$$

Entsprechend ist die Entschlüsselung  $E$  eine Funktion, die den Geheimtext in den Klartext überführt:

$$K = E(G).$$

Entsprechend muss gelten

$$E(V(K)) = K.$$

Wird zum Chiffrieren (Verschlüsseln) und Dechiffrieren (Entschlüsseln) der gleiche Schlüssel benutzt, so spricht man von einem *symmetrischen* Verfahren. Bei *asymmetrischen Verfahren* unterscheiden sich Chiffrier- und Dechiffrierschlüssel.

Die **Kryptoanalyse** beschäftigt sich mit dem Aufbrechen der Verschlüsselung ohne Kenntnis des Schlüssels. Eine versuchte Kryptoanalyse eines Dritten heißt *Angriff*. Der bekannteste Angriff war wohl die Entschlüsselung der *Enigma* durch ein Team des Informatikers ALAN TURING, was wohl mitentscheidend für den Verlauf des zweiten Weltkrieges war.

Die Aufgabe der **Steganographie** ist, es, die Existenz einer Nachricht zu verbergen. Deshalb spricht man in diesem Zusammenhang von „verdeckten Geheimschriften“. Zu den klassischen Verfahren zählen unter anderem:

- unsichtbare Tinte,
- Zitronensaft,
- Mikrofilme,
- doppelte Böden oder hohe Schuhabsätze,
- Semagramme (das Verstecken von Informationen in Bildern).

### Beispiel 1:

Die folgende Zeitungsanzeige ist auch nicht auf den ersten Blick als Träger einer geheimen Botschaft erkennbar<sup>1</sup>

**8-ung!!!**  
**Umzüge, Haushaltsauf-**  
**lösungen,**  
**Räumungsverkäufe -**  
 Bieten eine intelligente Lö-  
 sung all Ihrer Lagerproble-  
 me an.  
 Tel.: 0123-456 789

### Beispiel 2:

Das Rezept für deutsche Geheimtinte

LOS ANGELES, 12. Juli.

Fast 95 Jahre nach der Erfindung von Geheimtinte durch deutsche Wissenschaftler werden die Rezepturen jetzt in den Vereinigten Staaten zum ersten Mal öffentlich gezeigt. Im Washingtoner Nationalarchiv ist unter anderem ein Dokument vom 14. Juni 1918 in französischer Sprache zu sehen, das eine Mixtur aus „einer Tablette Pyramidon, einer Tablette Aspirin und 400 Milliliter reinem Wasser“ beschreibt. Wie das historische Dokument belegt, hatten die Franzosen die Kommunikation ihrer deutschen Feinde längst durchschaut, als während des Ersten Weltkriegs Briefe mit der vermeintlichen Geheimtinte an die Front geschickt wurden. Die in den vergangenen Wochen durch den amerikanischen Geheimdienst CIA freigegebenen Rezepte zählen zu den Dokumenten der National Archives, die am längsten geheim gehalten wurden.

*(aus: Frankfurter Allgemeine Zeitung, Nr. 160, Seite 7, 13. Juli 2011)*

### Beispiel 3:

Im alten Griechenland soll es eine ganz besondere Art der Steganographie gegeben haben. Um eine Nachricht zu versenden, wurde zunächst einem Sklaven der Kopf kahlgeschoren. Dann wurde die geheime Nachricht auf seiner Kopfhaut eintätowiert. Nach kurzer Zeit war von der Nachricht nichts mehr zu sehen. Der Sklave wurde nun zum Empfänger gesandt. Dieser scherte die Haare des Überbringers ab und erhielt die Nachricht.

Manchen Überlieferungen zufolge wurden den Sklaven nach Empfang der Nachricht nicht nur die Haare, sondern gleich der ganze Kopf abgetrennt, um die Geheimhaltung der Nachricht zu gewährleisten.

---

<sup>1</sup>Lösung: Man lese nur die Anfangsbuchstaben.

# Einige Beispiele

## U-Sprache

Jedes Wort beginnt mit einem „u“. Wenn das Wort mit einem Vokal beginnt, wird dieser durch „u“ ersetzt. *Udies ust win ugeheimer Ubrief..*

## I-Sprache

Jeder Vokal wird durch ein „i“ ersetzt: *Drii Chinisin mit dim Kintribiss.*

## Bi-Sprache

Nach jedem Vokal wird ein „bi“ eingefügt: *Dabis ibist nibicht schwebir.* Der Schriftsteller JOACHIM RINGELNATZ (1883-1934) hat in dieser Sprache ein Gedicht gemacht:

Ibich habibebi dibich,  
Lobittebi, sobi liebib.  
  
Habist aubich dubi mibich  
Liebib? Neibin, vebirgibib.  
  
Nabih obidebir febirn  
Gobitt seibi dibir gubit.  
Meibin Hebirz habit gebirn  
Abin dibir gebirubiht.

## Das Große Lalulã

CHRISTIAN MORGENSTERN (1871-1914) schreibt in seinen *Galgenliedern* das folgende Gedicht.

Das Große Lalulã  
Kroklokwaftzi? Semememi!  
Seiokrontro - prafriplo:  
Bifzi, bafzi; hulalemi:  
quasti basti bo...  
Lalu, lalu lalu lalu la!  
  
Hontraruru miromente  
zasku zes rü rü?  
Entepente, leiolente  
klekwapufzi lü?  
Lalu lalu lalu lalu la!  
  
Simarar kos malzipempu  
silzuzankunkrei (;)!

Marjomar dos: Quempu Lempu  
Siri Suri Sei !!!  
Lalu lalu lalu lalu la!

Ob das Gedicht etwas bedeutet, womöglich eine verschlüsselte Schachpartie darstellt o.a. ist durchaus umstritten.

## Die Ror-Sprache

Nach jedem Konsonanten wird ein o eingefügt und dann der Konsonant wiederholt: *Dodasos isostot einone schoschwowerore Gogehoheimomsospoprachoche.*

Die Ror-Sprache ist allen Kalle Blomquist<sup>2</sup>-Lesern aufs beste bekannt.

## Einige Beispiele aus der Geschichte

### Atbasch

Jüdische religiöse Schreiber der Antike verbargen manchmal die Bedeutung des Geschriebenen, indem sie das Alphabet umkehrten, d.h. den letzten Buchstaben des Alphabets (Taw) anstelle des ersten (Aleph), den vorletzten (Sch) anstelle des zweiten (Beth) usw. benutzten. Dieses System, genannt **Atbasch**, ist auch in der Bibel durch ein Beispiel belegt, und zwar in Jeremia 25, 26. Dort ist „Sheshech“ für „Babel“ (Babylon) geschrieben worden. Es wurden also der zweite und der zwölfte Buchstabe des hebräischen Alphabets von hinten anstelle des zweiten und zwölften von vorn benutzt.

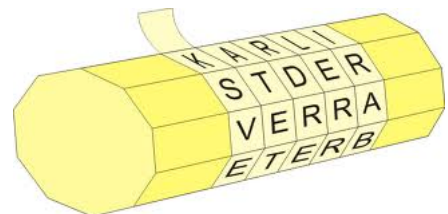
Eine Besonderheit ist, dass bei Atbasch Verschlüsselungs- und Entschlüsselungsmethode identisch sind. Daher genügt es, die Atbasch-Substitution ein zweites Mal auf den Geheimtext anzuwenden, um wieder den Ursprungstext zu erhalten.

Übertragen auf das lateinische Alphabet sieht die Zuordnung dann so aus:

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

### Skytale von Sparta

Spartanische Ephoren<sup>3</sup> kommunizierten vor mehr als 2500 Jahren mit ihren Feldgenerälen, indem sie Mitteilungen quer über die nebeneinanderliegenden Ränder eines Streifens Pergament schrieben, der spiralförmig um einen Stab, genannt Skytale, gewickelt wurde. War der Streifen erst einmal abgewickelt, konnte die Mitteilung nur gelesen werden, wenn der Streifen um genau so einen Stab gewickelt wurde.



<sup>2</sup>von ASTRID LINDGREN

<sup>3</sup>Aufseher bzw. hohe Beamte

## Der Polybios-Code

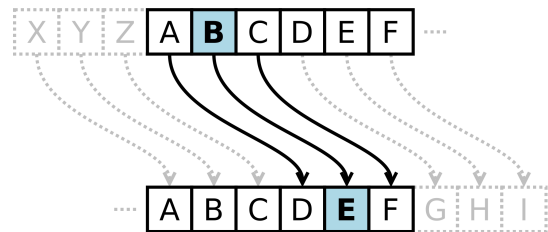
POLYBIOS war ein Schriftsteller, der vor über 2000 Jahren (200 - 120 v. Chr.) in Griechenland lebte. Er erfand den durch die folgende Tabelle dargestellten Code. Die Buchstaben werden in eine 5 × 5-Tabelle geschrieben. Da es 26 Buchstaben gibt, müssen „I“ und „J“ in dasselbe Kästchen.

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Zur Verschlüsselung hat man die links neben dem Buchstaben stehende Ziffer als Zehnerziffer und die über dem Buchstaben stehende als Einerziffer genommen. Der Buchstabe R erhielt demnach die Nr. 42. Diese Zuordnung ist wohl der Urahn unserer heutigen ASCII-Tabelle.

## Die Caesar-Verschlüsselung

Der Name der Cäsar-Verschlüsselung leitet sich vom römischen Feldherrn GAIUS JULIUS CAESAR ab, der nach der Überlieferung des römischen Schriftstellers SUTTON diese Art der geheimen Kommunikation für seine militärische Korrespondenz verwendet hat. Dabei benutzte Caesar eine Verschiebung des Alphabets um drei Buchstaben. Mehr dazu später.



## Bacon-Code

Im Buch Nummer 6, Kapitel 1 seines Buches „The Advancement of Learning“, beschreibt FRANCIS BACON (1561–1626) detailliert ein Substituierungssystem: Die Buchstaben des Alphabetes wurden durchnummeriert und die zugeordnete Nummer durch eine Folge von „a“ und/oder „b“ bestehend aus 5 Zeichen derart substituiert, dass es sich effektiv um eine 5-Bit-Binärkodierung handelt. Es fällt auf, dass es noch keine klare Unterscheidung von U und V gibt, die sich erst ab dem 17. Jahrhundert durchsetzte.

*A*    *B*    *C*    *D*    *E*    *F*  
*aaaaa*   *aaaab*   *aaaba*   *aaabb*   *aabaa*   *aabab* .  
*G*    *H*    *I*    *K*    *L*    *M*  
*aabba*   *aabbb*   *abaaa*   *abaab*   *ababa*   *ababb* .  
*N*    *O*    *P*    *Q*    *R*    *S*  
*abbaa*   *abbab*   *abbba*   *abbbb*   *baaaa*   *baaab* .  
*T*    *V*    *W*    *X*    *Y*    *Z*  
*baaba*   *baabb*   *babaa*   *babab*   *babba*   *babbb* .

## Aufgaben:

1. Die folgende Buchstabenfolge ist die Aufschrift bzw. der Papierstreifen einer Skytale:

SIHLTITADOCIUELHSPROETTKGRDZRIHAIYEESEP

Man weiß nur, dass die Skytale einen Umfang von 4 oder 5 Buchstaben hat. Welcher Klartext ergibt sich?

2. Verschlüsse den Text „V I E L G L U E C K“ mit dem Polybios-Code.
3. Im Film „2001 - Odyssee im Weltraum“ von Stanley Kubrick spielt der Computer HAL eine Hauptrolle. Der Name des Computers könnte eine Anspielung auf den Namen einer sehr großen Computerfirma sein<sup>4</sup>. Welche Caesar-Verschlüsselung wurde hier benutzt?
4. Entschlüsse den folgenden Text mit dem Original-Caesar-Verfahren:  
„Ghu Noxjhuh jlew vrodqjh qdfk, elv hu ghu Gxpph lvw!“
5. Der folgende Text ist nach dem Atbasch-Verfahren codiert worden.  
„orvyvi vmv uorvtv rn kliavoozmozvwm zoh vrm vovuzmg rm wvi hfkkv“
6. Welche Nummer hat der Buchstabe „R“ heute und welche Nummer hätte er, wenn sich die Codierung von Bacon durchgesetzt hätte?

## Das System von Caesar

Der folgende Text ist nach dem Caesar-Verfahren verschlüsselt worden. Der Schlüssel ist aber nicht bekannt.

WRQRE XNAA QVR IREFPUYHRFFRYHAT IBA PNRFNE RVASNPV XANPXRA.

Buchstabe:	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
Anzahl:																										

1. Bestimme mit Hilfe der Tabelle den Buchstaben, der am häufigsten im Text vorkommt.
2. Entschlüssele dann den angegebenen Geheimtext.

Die Entschlüsselung nach diesem Verfahren der Häufigkeitsanalyse hat seine Grenzen. Der französische Schriftsteller GEORGES PEREC hat es geschafft, sogar ein ganzes Buch mit etwa 85.000 Wörtern zu schreiben, ohne ein einziges Mal den Buchstaben „e“ zu benutzen. Noch erstaunlicher ist es, dass sogar Übersetzungen in das Spanische (der häufigste Buchstabe ist das „a“) ohne ein „a“ und auch ins Englische, Schwedische und Deutsche ohne ein „e“ auskamen. Der deutsche Übersetzer EUGEN HEMLE veröffentlichte das Buch unter dem Titel „Anton Voyls Fortgang“. Das Buch fängt so an:

*Kardinal, Pastor und Admiral, als Führungstrio null und nichtig und darum völlig abhängig vom Ami-Trust, tat durch Radionachricht und Anschlag kund, daß Nahrungsnot und damit Tod aufs Volk zukommt. Zunächst tat man das als Falschinformation ab. Das ist Propagandagift, sagt man. Doch bald schon*

<sup>4</sup>Der Buchautor ARTHUR C. CLARKE widerspricht dieser Darstellung.

*ward spürbar, was man ursprünglich nicht glaubt. Das Volk griff zum Stock, zum Dolch. „Gib uns das täglich Brot“, hallts durch Land und „pfui auf das Patronat, auf Ordnung, Macht und Staat.“ ...*

Bemerkenswert dabei ist insbesondere, dass Autor und Übersetzer ins Deutsche mit „e“s in ihren Namen geradezu gesegnet sind.

## Verschlüsselung mit einem Tabellenkalkulationsprogramm

### Einige wichtige Funktionen

1. **=REST(Zähler; Nenner)** liefert den Rest bei einer ganzzahligen Division.  
Beispiel: =REST(13; 11) liefert 2.
2. **=WENN(Bedingung; Dann-Ergebnis; Sonst-Ergebnis)** liefert das Dann-Ergebnis, wenn die Bedingung erfüllt ist, sonst das Sonst-Ergebnis.  
Beispiel: =WENN(REST(A3;2)=0;"Zahl ist gerade"; "Zahl ist ungerade.")
3. **=ZEICHEN(Zahl)** liefert das Zeichen mit der angegebenen Nummer im ASCII-Code.  
Beispiel: =ZEICHEN(65) liefert ein A.
4. **=CODE(Zeichen)** liefert die Nummer des Zeichens im ASCII-Code.  
Beispiel: =CODE("A") liefert 65.
5. **=GROSS(Text)** wandelt den Text komplett in Großbuchstaben um.  
Beispiel: =GROSS("Ene mene mu") liefert „ENE MENE MU“.
6. **=VERKETTEN(Text1;Text2;...)** liefert die Verkettung der Texte.  
Beispiel: =VERKETTEN("Ene"; "Mene"; "MU") liefert „Ene Mene Mu“.
7. **=TEIL(Text; Startposition; Anzahl)** liefert ab der Startposition Anzahl Buchstaben des Textes.  
Beispiel: =TEIL("Quatschkopf"; 8; 1) liefert „k“.
8. **=ZÄHLENWENN(Bereich; Kriterium)** liefert die Anzahl der Zellen, die im Bereich dem Kriterium entsprechen.  
Beispiel: =ZÄHLENWENN(A1:A10;67) liefert die Anzahl der Zellen von A1 bis A10, die den Wert 67 enthalten.

### **Aufgabe 1:**

Fertige eine Tabelle zur Verschlüsselung eines eingegebenen Textes an. Es sollen nur die Buchstaben verschlüsselt werden. Ziffern und Satzzeichen sollen erhalten bleiben. Es genügt, wenn der eingegebene Text vor der Verschlüsselung in Großbuchstaben umgewandelt und dann verschlüsselt wird. Die Verschlüsselung soll in Abhängigkeit von einem einzugebenen Schlüsselbuchstaben (D für Original-Caesar-Verschlüsselung) verwirklicht werden.

Eine Vorlage für ein solches Tabellenblatt findest du hier:

<http://www.gierhardt.de/informatik/krypto>

In dieser Datei sind auch die unten angegebenen Beispiele enthalten.

### **Aufgabe 2:**

Schreibe das Tabellenblatt so weit um, dass damit auch die Entschlüsselung erledigt werden kann. Dazu ist es hilfreich, die Häufigkeit der Buchstaben im Text zu untersuchen.

### **Aufgabe 3:**

Entschlüssele die folgenden Texte:

1. EPPIVERJERKMWXWGLAIV
2. XZCRPYDEFYOSLEMWPTTXSTYEP CY
3. XEBDYDOPSCMROCMRGSWWOXWSDNOWCDBYW
4. FGNRQGVFPURFTLZANFVHZONQYNNFCUR
5. HMENQLZSHJLZBGSROZRR
6. BDASDMYYUQDQZUEFEOTIQD
7. FKGGTFGKUVGKPGUEJGKDG
8. STGBDCSXHIPJHZPTHT
9. MGLOEQMGLWELMGLWMIKXI
10. WBKUSAMKDISXTKRYIJABQIIU

### **Aufgabe 4 (freiwillige Zusatzaufgabe):**

Es soll auch noch nach Groß- und Kleinbuchstaben unterschieden werden.