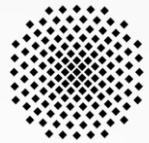


Universität Stuttgart

Tag der Mathematik

Kryptographie

Tara Wagner, Mira Gerstner und Dominik Schwenk

Nachrichten, die du in diesem Chat sendest, sowie Anrufe, sind jetzt mit Ende-zu-Ende-Verschlüsselung geschützt. Tippe für mehr Infos.

WAS IST KRYPTOGRAPHIE?

griechisch

verborgen +

schreiben


Sicher Kommunizieren einfach erklärt

STEGANOGRAPHIE

- Übermittlung geheimer Nachrichten, bei der verborgen bleibt, dass überhaupt eine Botschaft existiert

- Bsp. 1: Wachsbällchen
- Bsp. 2: Nachricht auf Kopfhaut einbrennen
- Bsp. 3: Thithymalus-Pflanze
- **Problem:** Möglichkeit zur Offenlegung der geheimen Nachricht
  → Kryptographie entsteht

SKYTALE-CHIFFRIERUNG (500 v.Chr.)

Sparta

SKYTALE-CHIFFRIERUNG (500 v.Chr.)

SKYTALE-CHIFFRIERUNG (500 v.Chr.)

Umordnung:

Angriff im Morgengrauen

SKYTALE-CHIFFRIERUNG (500 v.Chr.)

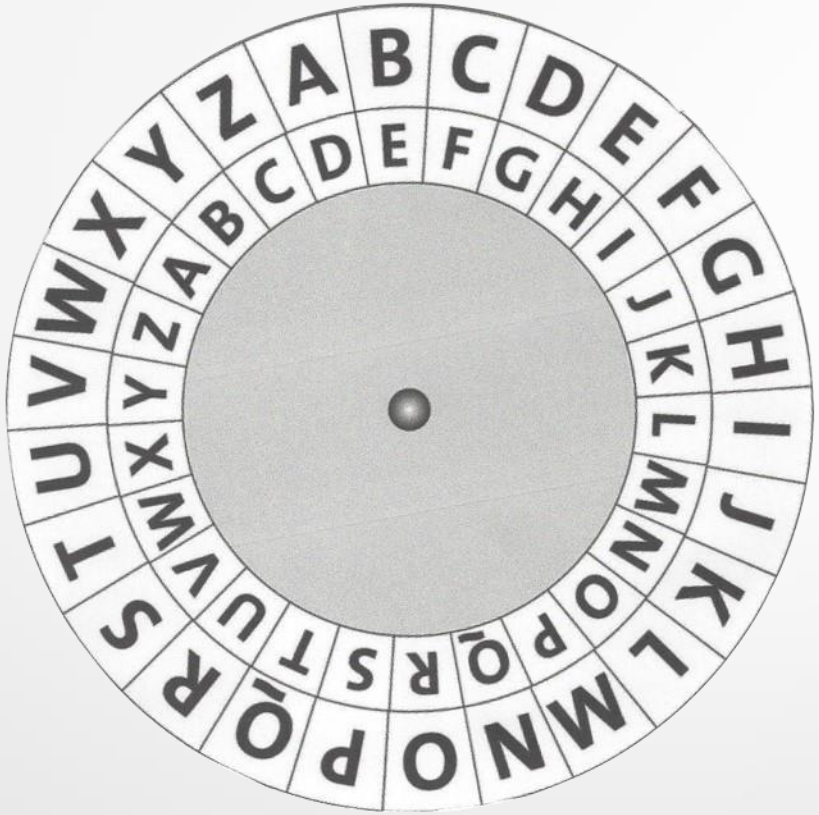
Umordnung:

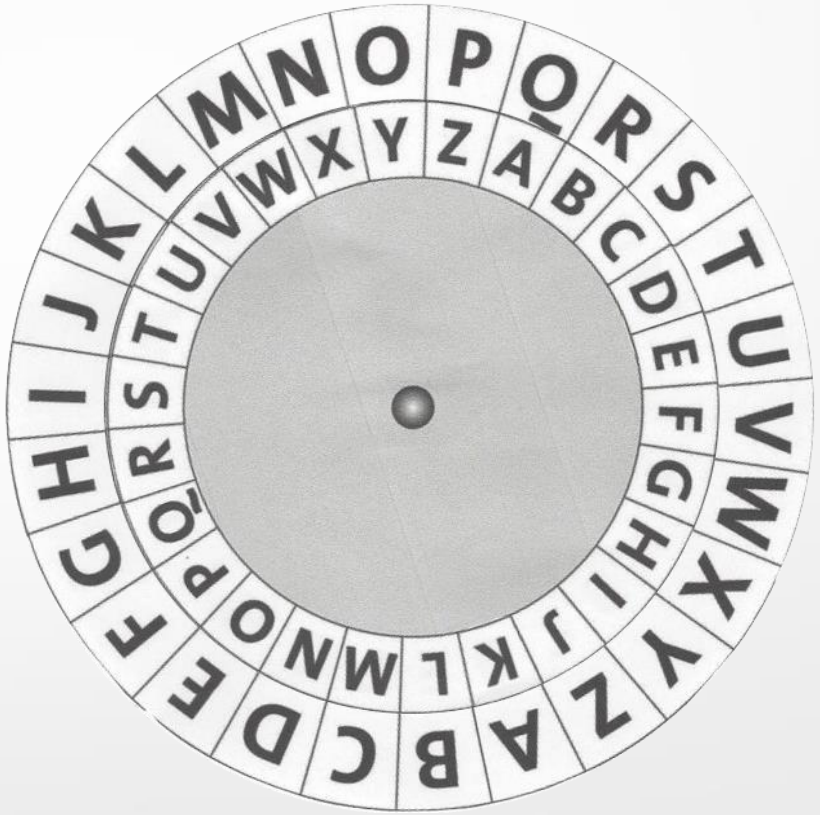
Aforn ragigurmeei nnfMg

CAESAR-VERSCHLÜSSELUNG (60 v. Chr.)

Rom

CAESAR-VERSCHLÜSSELUNG (60 v. Chr.)





- 25 Möglichkeiten

BELIEBIGES UMSORTIEREN

Ausgangs- Alphabet

ABCDEFGHIJKLMNOPQRSTUVWXYZ

Umgeordnetes Alphabet

COEZRHDJATKXMGFNPSUBVQWLYI

- 26! = 403.291.461.126.605.635.584.000.000 Möglichkeiten
  - Ausprobieren dauert zu lange!

DIE ENTSCHLÜSSELUNG EINES GEHEIMTEXTES

PR ISRSQ YSPUD SYOCREBS GPS NFRZB GSY NCYBVEYCWDPS SPRSZVOUDS HVOONVQQSRDSPB, GCZZ GPS NCYBS SPRSY SPRMPESR WYVHPRM GSR YCFQ SPRSY ECRMSR ZBCGB SPRRCDQ FRG GPS NCYBS GSZ YSPUDZ GSR SPRSY WYVHPRM. QPB GSY MSPB ASTYPSGPEBSR GPSZS FSASYQCSZZPE EYVZZSR NCYBSR RPUDB OCSRESY, FRG QCR SYZBSOOBS SPRS NCYBS GSZ YSPUDZ, GPS ESRCF GPS EYVSZZS GSZ YSPUDZ DCBBS.

Problem:  **???**

HÄUFIGKEITSVERTEILUNG DER BUCHSTABEN DES DEUTSCHEN ALPHABETS

DIE ENTSCHLÜSSELUNG EINES GEHEIMTEXTES

Buchstaben aus dem Klartext

Buchstabe	Häufigkeit in %
e	17,40
n	9,78
i	7,55
s	7,27
r	7,00

=

=

Buchstaben aus dem Geheimtext

Buchstabe	Häufigkeit in %
S	20,4
R	9,7
P	9,1
Y	8,8
Z	7,3

DIE ENTSCHLÜSSELUNG EINES GEHEIMTEXTES

- S = e
- Häufigkeitsanalyse verfeinern: Zweier- und Dreierkombinationen (ZK und DK)

ZK
SR
SP
SY
SZ
ZS

=

ZK
ei
er
en
es
se

DK
SPR

=

DK
ein

DIE ENTSCHLÜSSELUNG EINES GEHEIMTEXTES

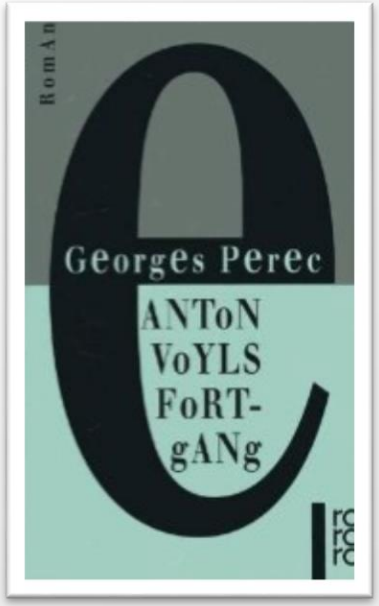
Klartext	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Geheimtext	C	A	U	G	S	T	E	D	P	I	N	O	Q	R	V	W	X	Y	Z	B	F	H	J	K	L	M

HÄUFIGKEITSANALYSE

- Antons Puls schlug zu stark. Ihm war warm. Anton macht das Wandloch mit Glas davor auf und schaut durch Nacht und Wind zum Mond hinauf. Warm wars, doch nicht zu warm. Vom Vorort drang kaum hörbar Lärm zu ihm rauf.

- „La Disparition“ (1969), George Perec

- „Anton Voyls Fortgang“ (1986), Eugen Helmlé



Bildquelle: amazon.de

DAS BABINGTON-KOMPLOTT

- Renaissance in Europa
- Kryptographie gewinnt an Bedeutung

DAS BABINGTON-KOMPLOTT

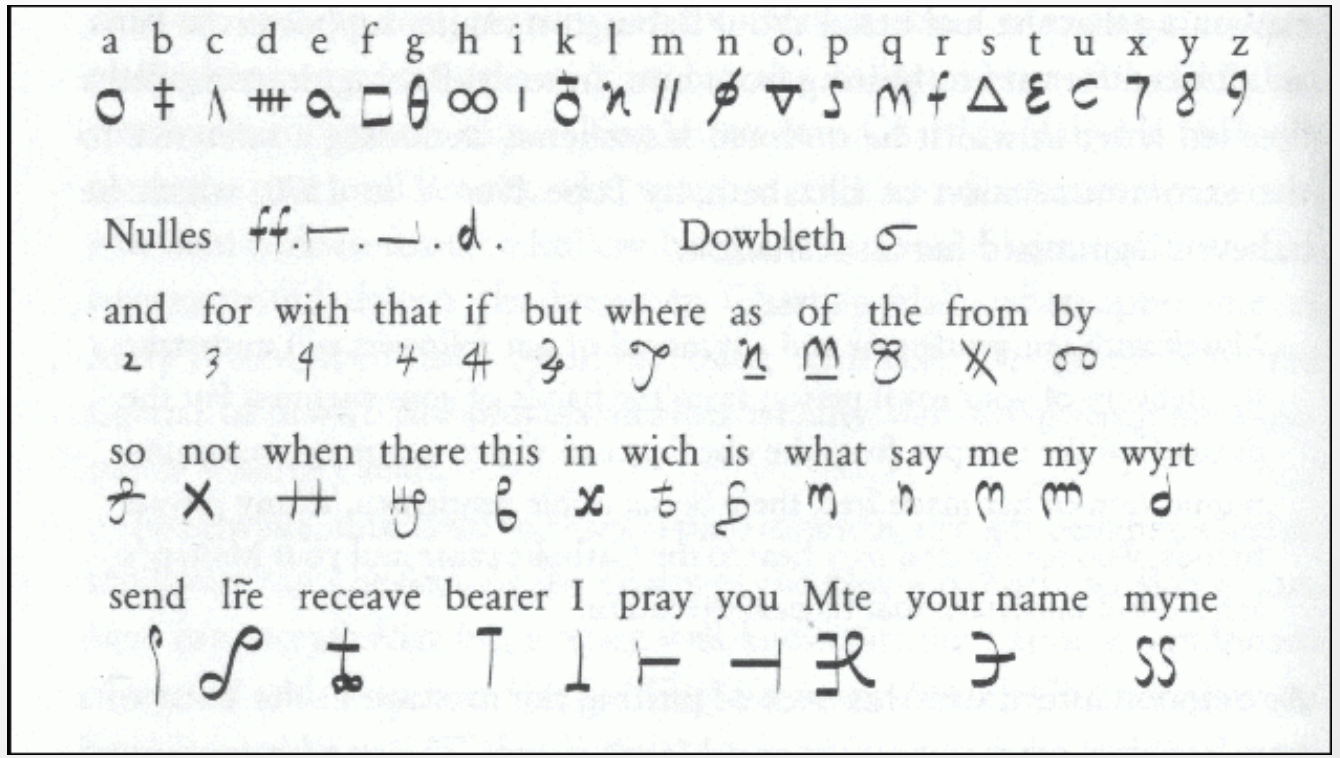
Chiffrierscheibe

- Renaissance in Europa
- Kryptographie gewinnt an Bedeutung
- Verschlüsselung über ein Geheimalphabet stößt an ihre Grenzen

DAS BABINGTON-KOMPLOTT

Maria Stuart (1542-1587), Königin von Schottland

DAS BABINGTON-KOMPLOTT



Maria Stuart (1542-1587), Königin von Schottland, und ihre Geheimschrift

DAS BABINGTON-KOMPLOTT

Maria Stuarts Hinrichtung

VIGENÈRE-VERSCHLÜSSELUNG (16. Jh.)

Blaise de Vigenère
(1523-1596)

VIGENÈRE-VERSCHLÜSSELUNG (16. Jh.)

Formatierter Klartext:

Am Anfang schuf Gott Himmel und Erde. Und die Erde war wüst und leer, und es war finster auf der Tiefe; und der Geist Gottes schwebte auf dem Wasser. Und Gott sprach: Es werde Licht! Und es ward Licht. Und Gott sah, dass das Licht gut war. Da schied Gott das Licht von der Finsternis und nannte …

VIGENÈRE-VERSCHLÜSSELUNG (16. Jh.)

Unformatierter Klartext:

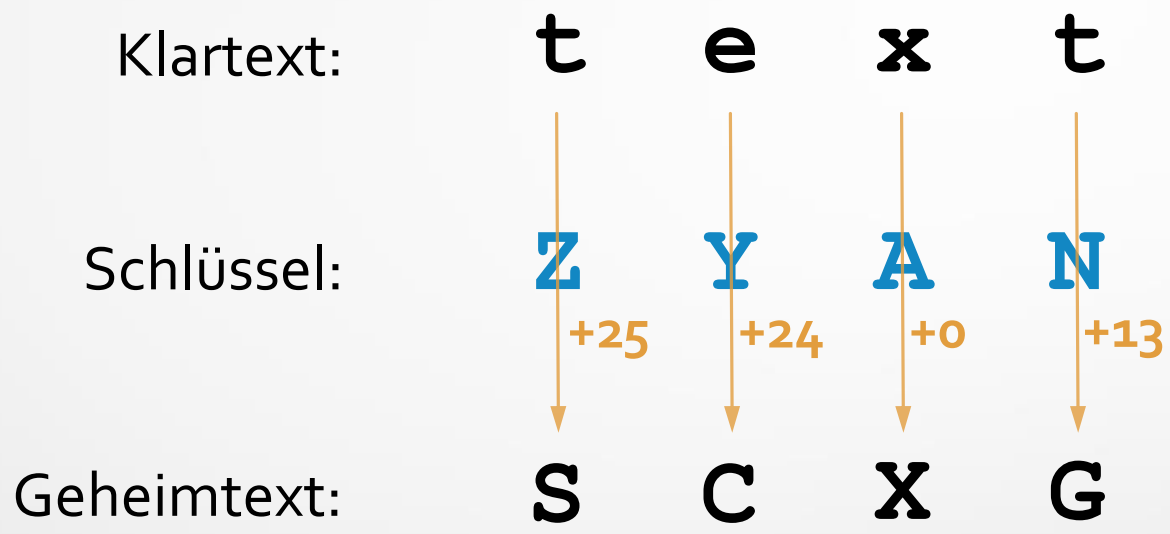
amanfangschufgotthimmelunderdeunddieerd
ewarwuestundleerundeswarfinsteraufderti
efeunddergeistgottesschwebteaufdemwasse
rundgottspracheswerdelichtundeswardlich
tundgottsahdassdaslichtgutwardaschiedgo
ttdaslichtvonderfinsternisundnanntedasl
ichttagunddiefinsternisnachtdawardausab
endundmorgenderersteteag

VIGENÈRE-VERSCHLÜSSELUNG (16. Jh.)

Klartext: amanfangschufgotthimmelunderde

Schlüssel: KRYPTKRYPTKRYPTKRYPTKRYPTKRYPT

VIGENÈRE-VERSCHLÜSSELUNG (16. Jh.)



VIGENÈRE-VERSCHLÜSSELUNG (16. Jh.)

Klartext: amanfangschufgotthimmelunderde

Schlüssel: KRYPTKRYPTKRYPTKRYPTKRYPTKRYPT

Geheimtext: KDYCYKEEHVRLDVHDKFXFWVJJGNVPSX

VIGENÈRE-VERSCHLÜSSELUNG (16. Jh.)

Geheimtext:

KDYCYKEEHVRLDVHDKFXFWVJJGNVPSXEEBSBOVPS
XGRPLNOJRJGNCCTKEEBTLGRPUBXJRTKKLDSXBKG
TYOLLSWOIETBCKEDMDVQHVRNCQMORSUWODUPLCV
PJGNXMIMCGPPVRVQLXBUCABMYRJGNVQLTBUJXVR
KSCWQFRILKYBPLCUYHESTFIZEKUPKNRQRASVBVH
DKBPLVZAWMFFLSXBWGCLDVPCBCLLSGKELIXNRQA
BMYRITQLLSWSVDXGCKCGGSJLPVRKBPPKIBPNCRZ
TGNLLSFYIETGNVPTKCKCITQ

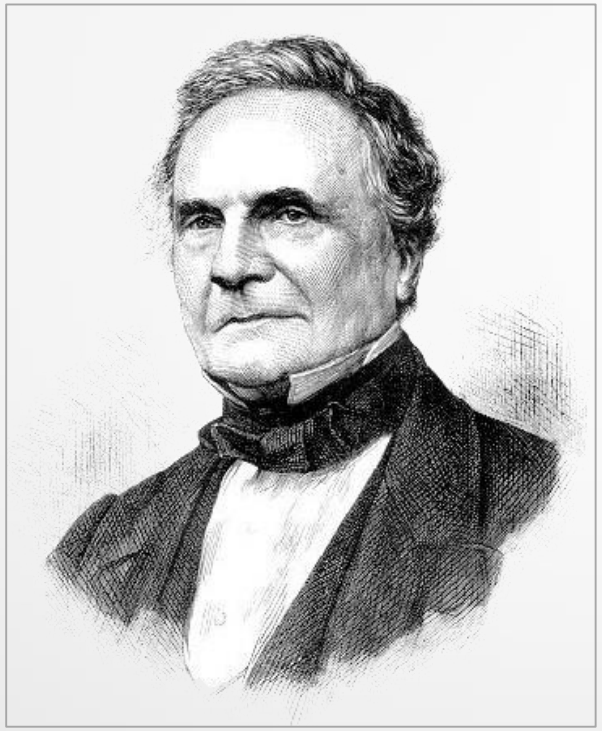
VIGENÈRE-VERSCHLÜSSELUNG (16. Jh.)

Häufigkeitsverteilung (Deutsch):

VIGENÈRE-VERSCHLÜSSELUNG (16. Jh.)

Häufigkeitsverteilung (Geheimtext):

VIGENÈRE-ENTSCHLÜSSELUNG



Charles Babbage
(1791-1871)

Friedrich Wilhelm Kasiski
(1805-1881)

VIGENÈRE-VERSCHLÜSSELUNG

und

ZYANZYANZYANZYANZYANZYANZYAN

TLD

VIGENÈRE-VERSCHLÜSSELUNG

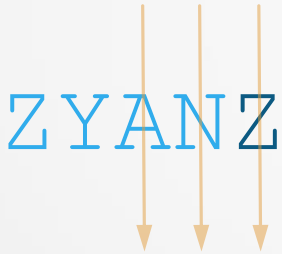
und

ZYANZYANZYANZYANZYANZYANZYAN

SNQ

VIGENÈRE-VERSCHLÜSSELUNG

und

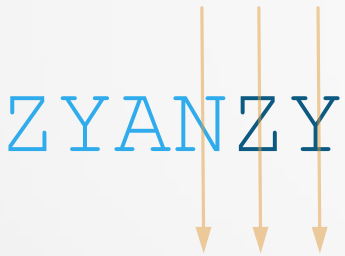


ZYANZYANZYANZYANZYANZYANZYAN

UAC

VIGENÈRE-VERSCHLÜSSELUNG

und



ZYANZYANZYANZYANZYANZYANZYAN

HMB

VIGENÈRE-VERSCHLÜSSELUNG

und

TLD

VIGENÈRE-VERSCHLÜSSELUNG

und

SNQ

VIGENÈRE-VERSCHLÜSSELUNG

und

UAC

VIGENÈRE-VERSCHLÜSSELUNG

und

HMB

VIGENÈRE-VERSCHLÜSSELUNG

und

TLD

VIGENÈRE-VERSCHLÜSSELUNG

und

SNQ

VIGENÈRE-VERSCHLÜSSELUNG

und

UAC

VIGENÈRE-VERSCHLÜSSELUNG

und

HMB

VIGENÈRE-VERSCHLÜSSELUNG

und

TLD

VIGENÈRE-VERSCHLÜSSELUNG

und

TLD

VIGENÈRE-VERSCHLÜSSELUNG

und

TLD

VIGENÈRE-VERSCHLÜSSELUNG

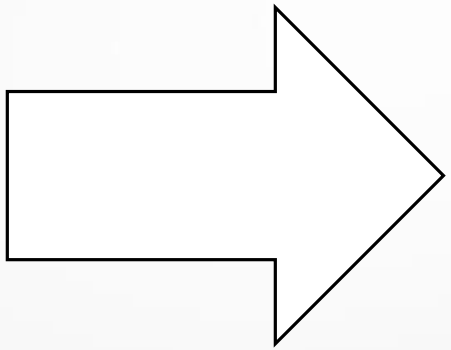
und

ZYANZYANZYANZYANZYANZYANZYAN

TLD

VIGENÈRE-ENTSCHLÜSSELUNG

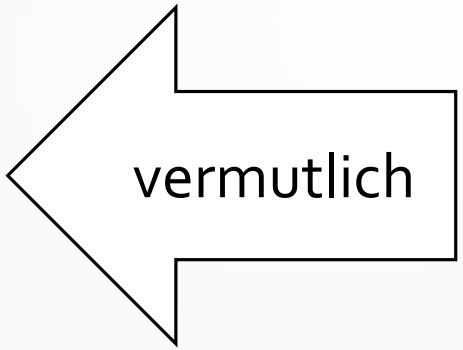
Textbaustein um **Vielfaches der Schlüssellänge** verschoben



Textbaustein **identisch** verschlüsselt

VIGENÈRE-ENTSCHLÜSSELUNG

Textbaustein um **Vielfaches der Schlüssellänge** verschoben



Textbaustein **identisch** verschlüsselt

VIGENÈRE-ENTSCHLÜSSELUNG

Geheimtext:

KDYCYKEEHVRLDVHDKFXFWVJJGNVPSXEEBSBOVPS
XGRPLNOJRJGNCCTKEEBTLGRPUBXJRTKKLDSXBKG
TYOLLSWOIETBCKEDMDVQHVRNCQMORSUWODUPLCV
PJGNXMIMCGPPVRVQLXBUCABMYRJGNVQLTBUJXVR
KSCWQFRILKYBPLCUYHESTFIZEKUPKNRQRASVBVH
DKBPLVZAWMFFLSXBWGCLDVPCBCLLSGKELIXNRQA
BMYRITQLLSWSVDXGCKCGGSJLPVRKBPPKIBPNCRZ
TGNLLSFYIETGNVPTKCKCITQ

VIGENÈRE-ENTSCHLÜSSELUNG

Geheimtext:

KDYCYKEEHVRLDVHDKFXFWVJJGNVPSXEEBSBOVPS
XGRPLNOJRJGNCCTKEEBTLGRPUBXJRTKKLDSXBKG
TYOLLSWOIETBCKEDMDVQHVRNCQMORSUWODUPLCV
PJGNXMIMCGPPVRVQLXBUCABMYRJGNVQLTBUJXVR
KSCWQFRILKYBPLCUYHESTFIZEKUPKNRQRASVBVH
DKBPLVZAWMFFLSXBWGCLDVPCBCLLSGKELIXNRQA
BMYRITQLLSWSVDXGCKCGGSJLPVRKBPPKIBPNCRZ
TGNLLSFYIETGNVPTKCKCITQ

VIGENÈRE-ENTSCHLÜSSELUNG

Zähle Abstände:

0 1 2 3 4 5 ..

KDYCYKEEHVRLDVHDKFXFWVJ**JGN**VPSX

. . . . . 23 24 25

EEBSBOVPSXGRPLNOJR**JGN**CCTKEEBT…

VIGENÈRE-ENTSCHLÜSSELUNG

Abstände häufig auftretender Buchstabenfolgen:

JGN: 25, 70, 25

GRP: 20

LLS: 140, 20, 35

ITQ: 60

durch **5** teilbar

Vermutung:
Schlüssel hat Länge **5**

VIGENÈRE-ENTSCHLÜSSELUNG

Geheimtext:

KDYCYKEEHVRLDVHDKFXFWVJJGNVPSXEEBSBOVPS
XGRPLNOJRJGNCCTKEEBTLGRPUBXJRTKKLDSXBKG
TYOLLSWOIETBCKEDMDVQHVRNCQMORSUWODUPLCV
PJGNXMIMCGPPVRVQLXBUCABMYRJG…

VIGENÈRE-ENTSCHLÜSSELUNG

Geheimtext:

KDYCY KEEHV RLDVH DKFXF WVJJG NVPSX
EEBSB OVPSX GRPLN OJRJG NCCTK EEBTL
GRPUB XJRTK KLDSX BKGTY OLLSW OIETB
CKEDM DVQHV RNCQM ORSUW ODUPL CVPJG
NXMIM CGPPV RVQLX BUCAB MYRJG …

VIGENÈRE-ENTSCHLÜSSELUNG

Geheimtext:

KDYCY KEEHV RLDVH DKFXF WVJJG NVPSX
EEBSB OVPSX GRPLN OJRJG NCCTK EEBTL
GRPUB XJRTK KLDSX BKGTY OLLSW OIETB
CKEDM DVQHV RNCQM ORSUW ODUPL CVPJG
NXMIM CGPPV RVQLX BUCAB MYRJG …

Caesar-Verschlüsselung → Häufigkeitsanalyse

→ Vermutung:
K erster Schlüsselbuchstabe

VIGENÈRE-ENTSCHLÜSSELUNG

Geheimtext:

KDYCY KEEHV RLDVH DKFXF WVJJG NVPSX
EEBSB OVPSX GRPLN OJRJG NCCTK EEBTL
GRPUB XJRTK KLDSX BKGTY OLLSW OIETB
CKEDM DVQHV RNCQM ORSUW ODUPL CVPJG
NXMIM CGPPV RVQLX BUCAB MYRJG …

Caesar-Verschlüsselung → Häufigkeitsanalyse

→ Vermutung:
R zweiter Schlüsselbuchstabe

VIGENÈRE-ENTSCHLÜSSELUNG

Geheimtext:

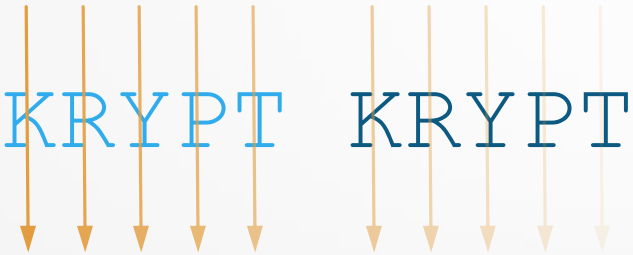
KDYCY KEEHV RLDVH DKFXF WVJJG NVPSX
EEBSB OVPSX GRPLN OJRJG NCCTK EEBTL
GRPUB XJRTK KLDSX BKGTY OLLSW OIETB
CKEDM DVQHV RNCQM ORSUW ODUPL CVPJG
NXMIM CGPPV RVQLX BUCAB MYRJG …

Caesar-Verschlüsselung → Häufigkeitsanalyse

→ Vermutung:
Y dritter Schlüsselbuchstabe

VIGENÈRE-VERSCHLÜSSELUNG

Geheimtext: KDYCY KEEHV RLDVH DKFXF WV



Schlüssel: KRYPT KRYPT KRYPT KRYPT KR

Klartext: amanf angsc hufgo tthim me

ONE-TIME-PAD

- Schlüssellänge $\geq$ Textlänge
- Unknackbar ohne Schlüsselkenntnis
- Anwendung: Heißer Draht
- Nachteil: Schlüssellänge

Eine Festplatte verschlüsseln?

MASCHINELLE KRYPTOGRAPHIE - ENIGMA

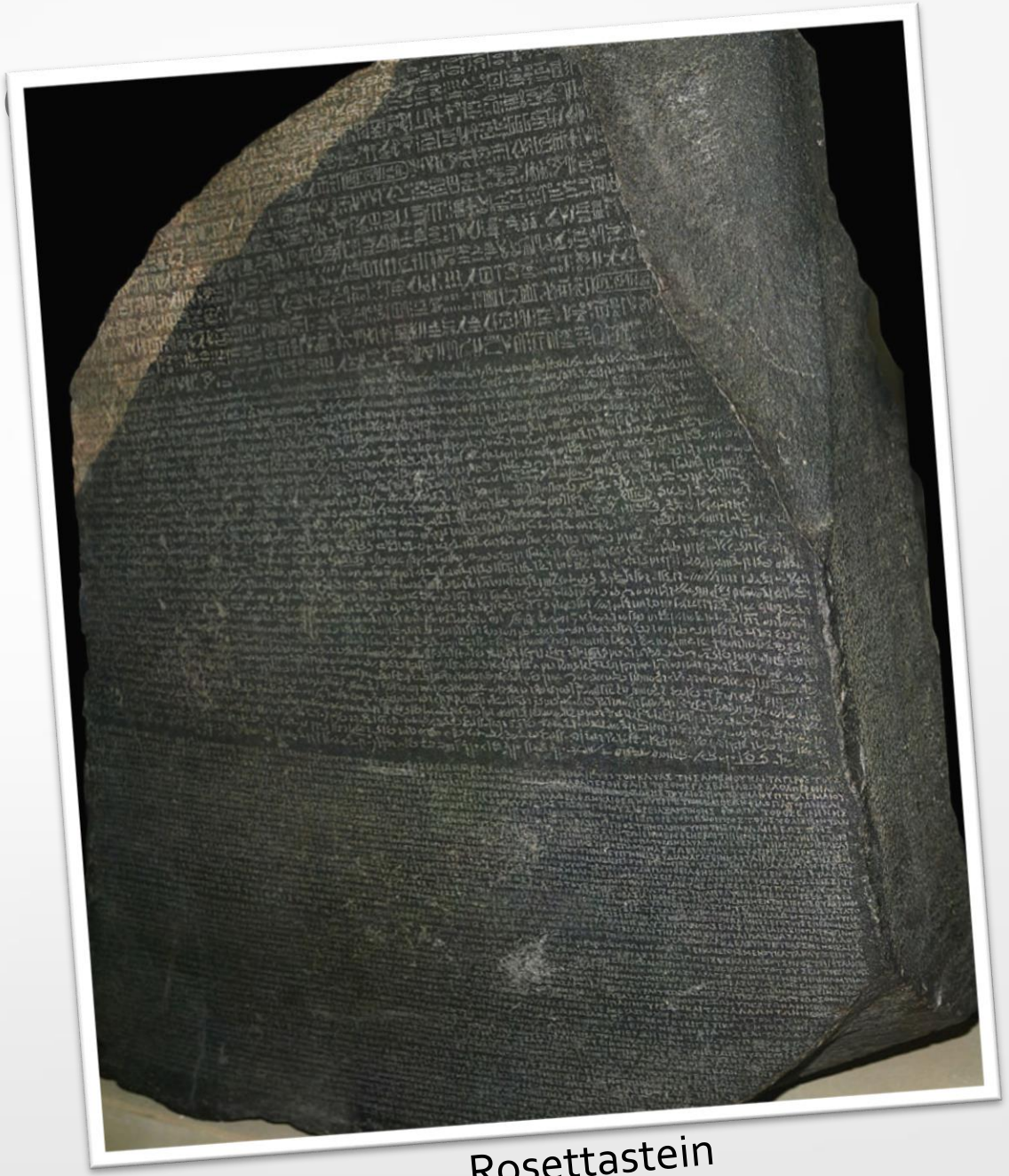
Vorteil: Schnelle Ver- und Entschlüsselung mit hoher Sicherheit

Knacken:

- „Security by Obscurity“ funktioniert nicht
- Berechenbare Funksprüche
- nur durch eine andere Maschine möglich (Turing- Bombe)

NAVAJO-CODESPRE

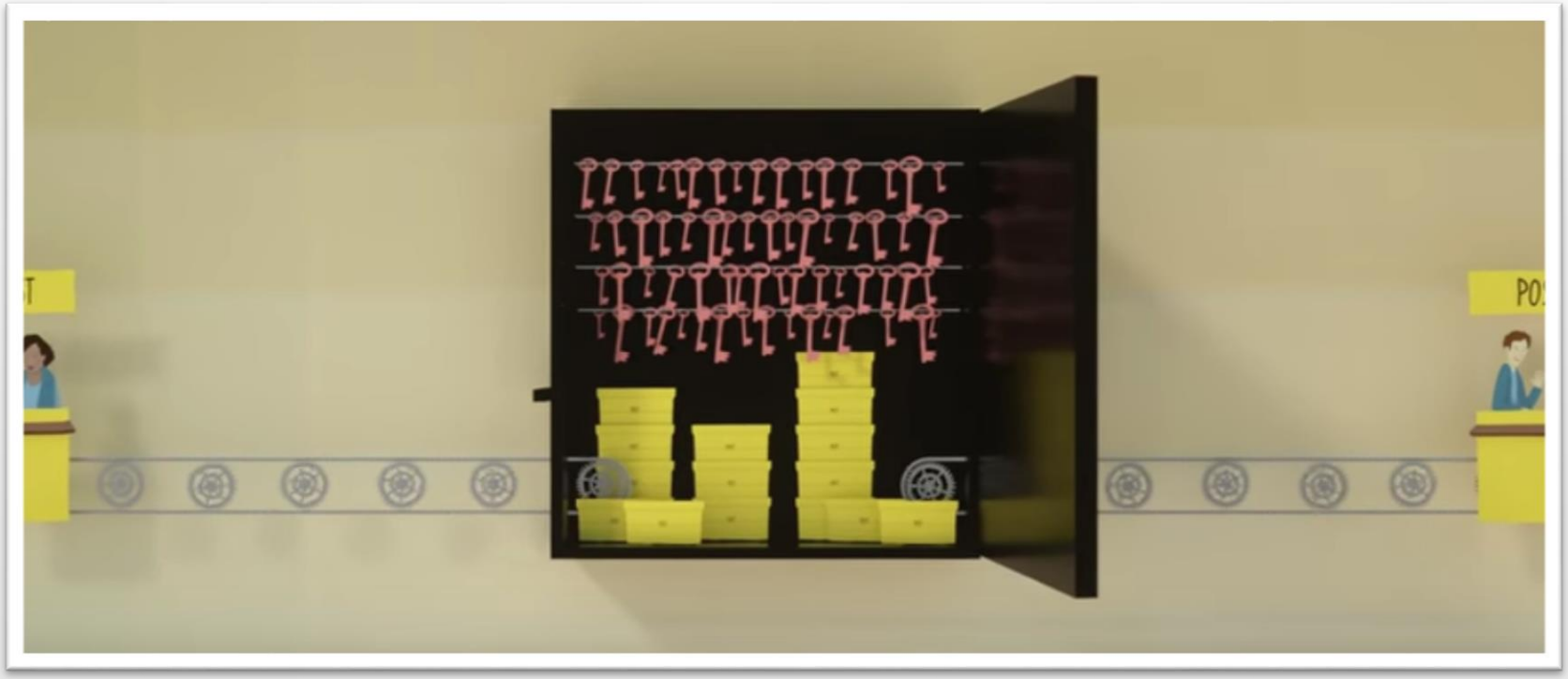
- Pazifikkrieg 1942: Amerika vs. Japan
- Navajos: Amerikanische Ureinwohner, Verschlüsselung wurde nie geknackt
- Parallele: Hieroglyphen



Rosettastein

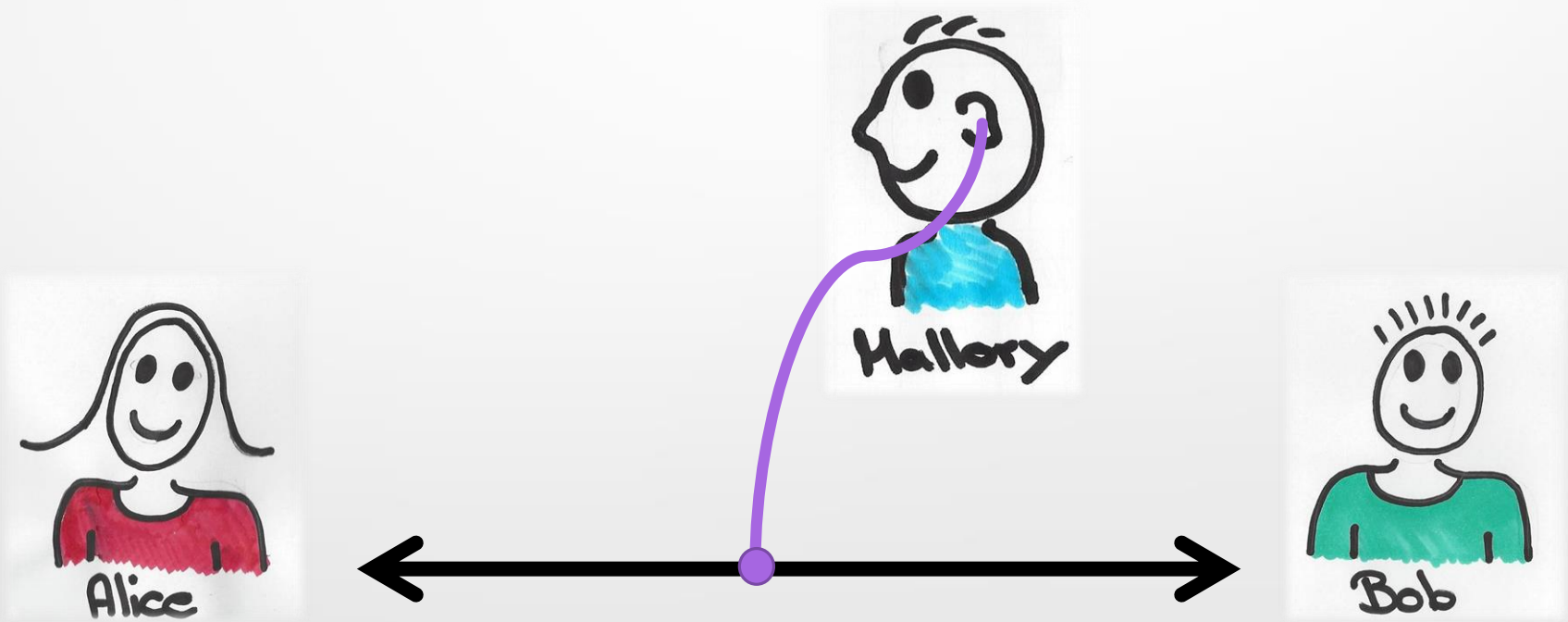
Bis jetzt: Vorangegangener Schlüsselaustausch nötig!

Wenn Schlüssel bekannt, dann Nachricht bekannt!

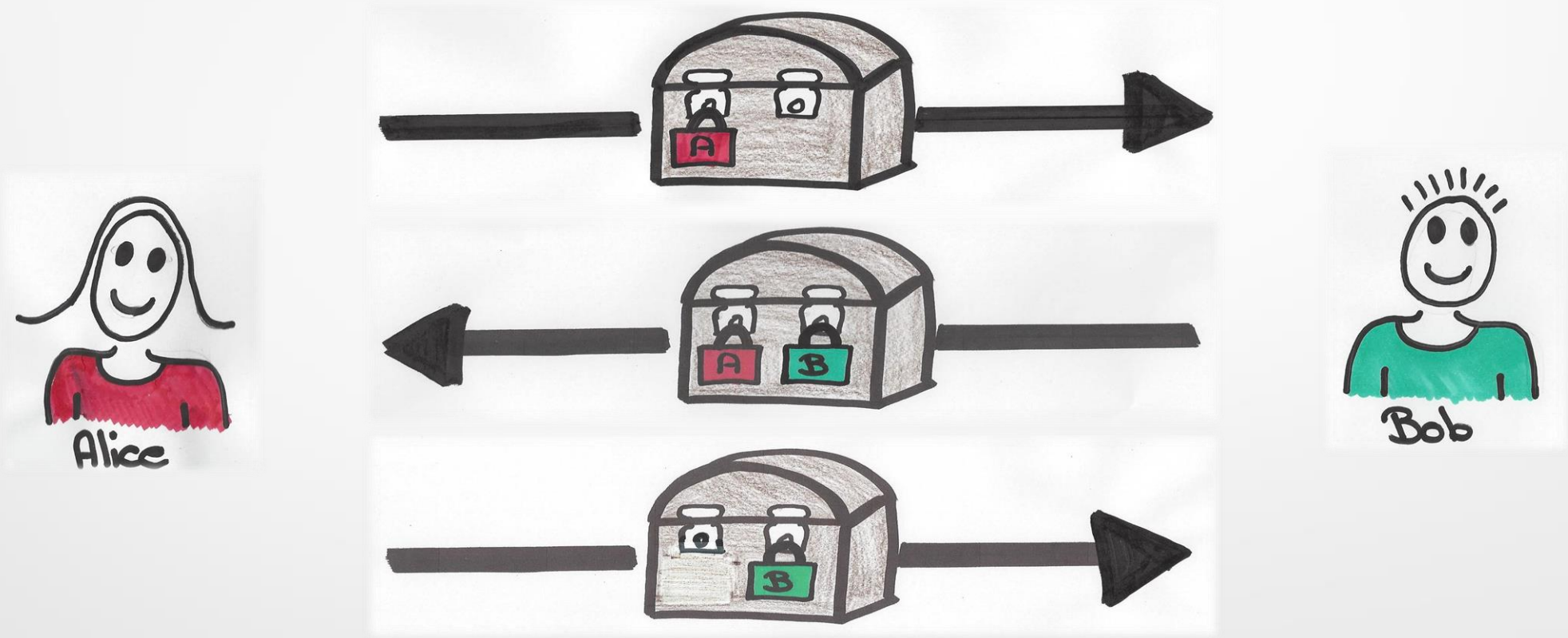


ALLGEMEINES MODELL

- Alice und Bob tauschen über einen Kanal Daten aus
- **Entscheidend:** Möglichkeit übertragene Daten abzufangen

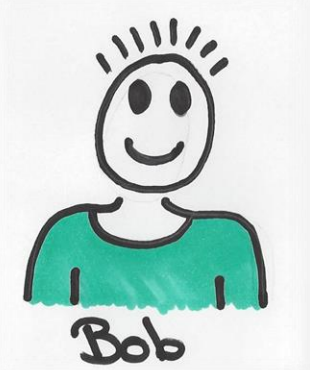


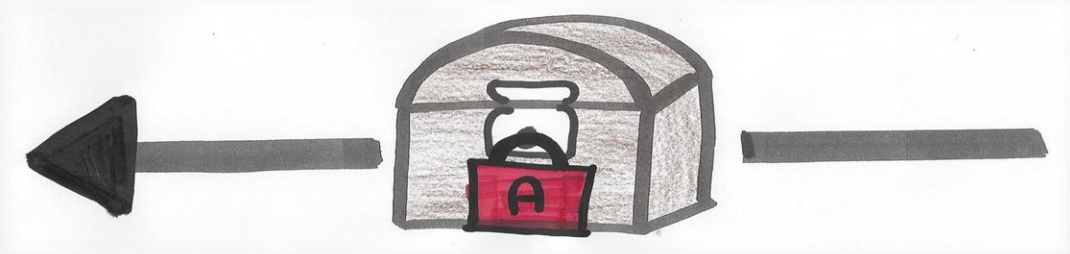
VERSCHLÜSSELTE KOMMUNIKATION OHNE SCHLÜSSELAUSTAUSCH?

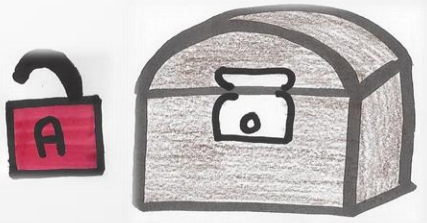


Diffie- Hellmann- Verfahren

ASYMMETRISCHE VERSCHLÜSSELUNG







Rivest-**S**hamir-**A**dleman-Verfahren

ZIELE DER KRYPTOGRAPHIE

- **Verschlüsselung von Informationen**
- **Vertraulichkeit:** soziale Medien, Patienteninformationen
- **Identität und Authentizität:** Dienstplan Fluggesellschaft
- **Schutz vor Manipulation:** Online-Banking
- **Zurechenbarkeit:** Vertrag im Internet

WIE GEHT ES WEITER?

In der Kryptographie…

- Mathematische Verfahren wurden immer bedeutsamer
- Suche nach einem grundsätzlichen Verfahren geht weiter

Bei uns…

- Workshop
  „RSA- Sicherheit durch Primzahlen“

QUELLEN, LITERATUR UND LINKS

- Bücher: - Simon Singh, Codes
  - Simon Singh, Geheime Botschaften
  - Klaus Schmeh, Nicht zu Knacken
  - Dominik Landwehr, Mythos Enigma
- Film: The Imitation Game
- Vigènere online ausprobieren: https://gc.de/gc/vigenere/
- Häufigkeitsanalyse: https://gc.de/gc/buchstabenhaeufigkeit/

Vielen Dank für Eure Aufmerksamkeit!