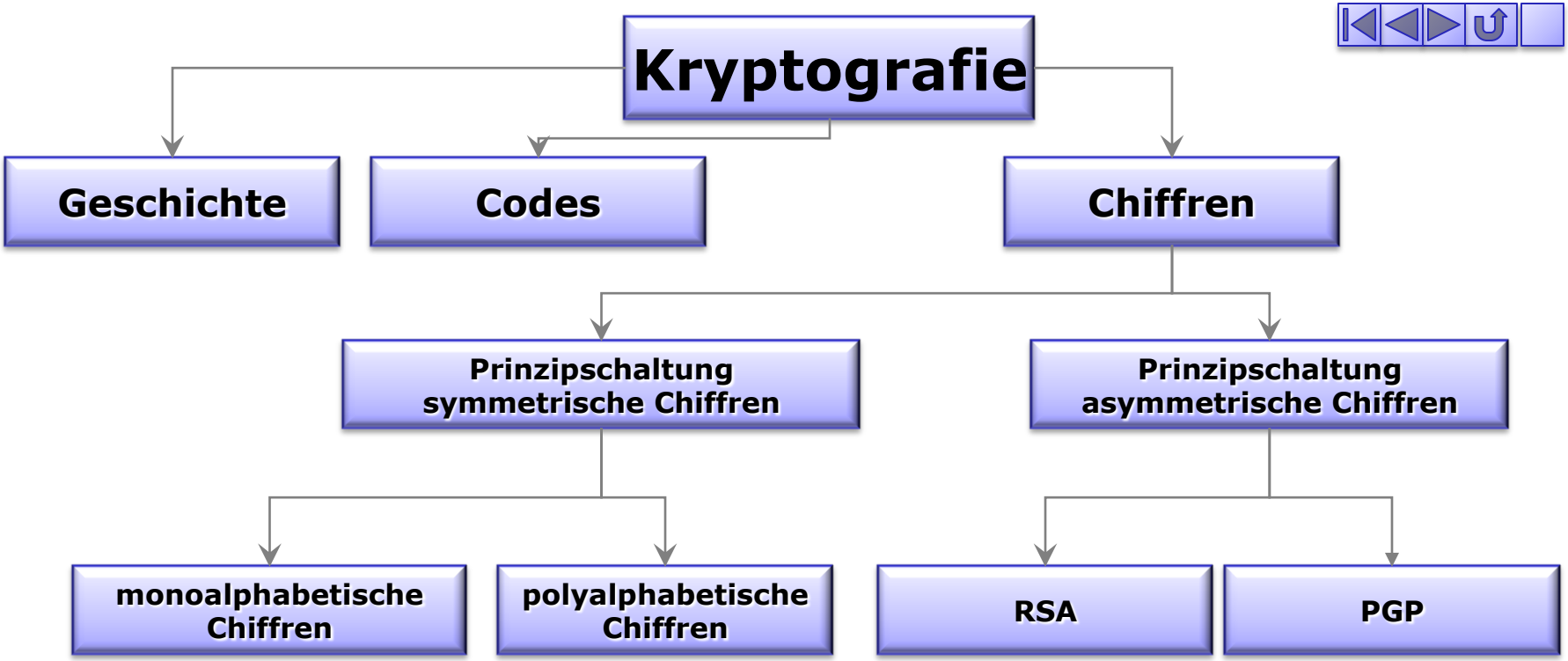


Aufgaben

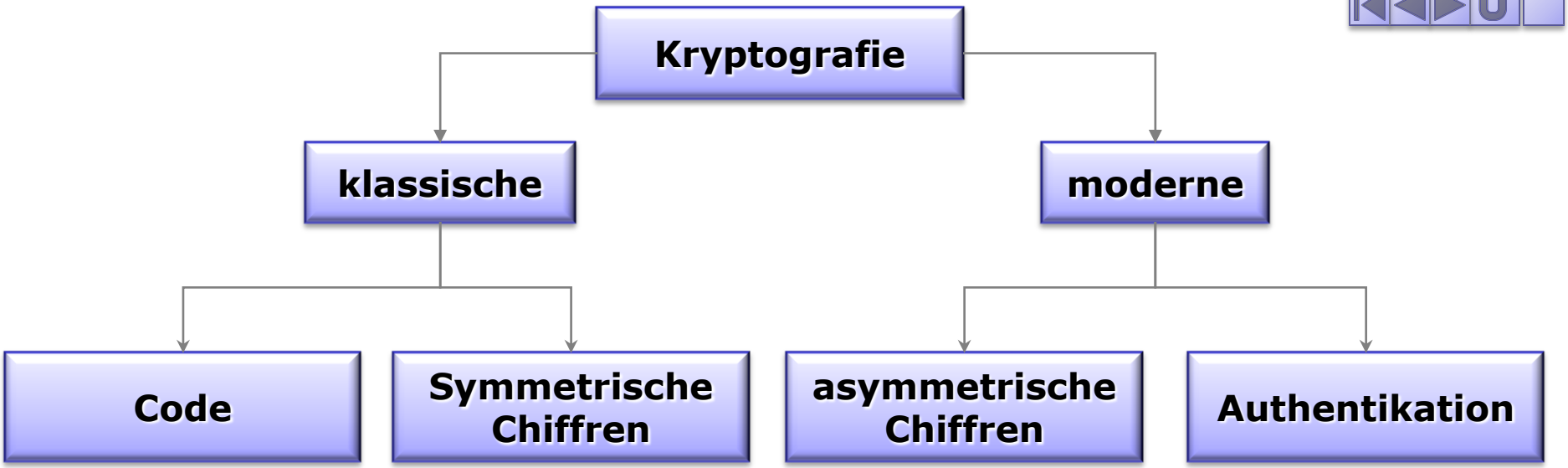
Ein Text zur „Einstimmung“

Passwort-verschlüsselung

Authentifikation

GLHVHU WHAW ZXUGH PLW HLQHP DOJRULWKPXV YHUVFKOXHVVHOW, GHQ
VLFK MXOLXV FDHVDU DXVJHGDFKW KDW.
ZLU ZHUGHQ XQV LP XQWHUULFKW PLW GLHVHP XQG DQGHUHQ
DOJRULWKPHQ EHVFKDHIWLJHQ.
CXQDHFKVW LQIRUPLHUW LKU HXFK DOOHUGLQJV XHEHU GLH
JHVFKLFKWH GHU NUBSWRORJLH.
LKU VROOW DXFK NODHUHQ, ZDV NUBSWRORJLH HLJHQWOLFK LVW,
ZHOFKH WHLOGLVCLSOLQHQ HV JLEW XQG ZRPLW VLFK GLHVH
EHVFKDHIWLJHQ.
SDUDOOHO CXU EHKDQGOXQJ GHU DOJRULWKPHQ ZHUGHW LKU HLQ
SURJUDPP VFKUHLEHQ, LQ GDV HLQLJH GHU EHVSURFKHQHQ
DOJRULWKPHQ LPSOHPHQWLHUW ZHUGHQ.
DEVFKOLHVVHQ ZHUGHQ ZLU PLW GHU EHKDQGOXQJ GHV UVD-DOJRULWKPXV.

DIESER TEXT WURDE MIT EINEM ALGORITHMUS VERSCHLUESSELT, DEN
SICH JULIUS CAESAR AUSGEDACHT HAT.
WIR WERDEN UNS IM UNTERRICHT MIT DIESEM UND ANDEREN
ALGORITHMEN BESCHAEFTIGEN.
ZUNAECHST INFORMIERT IHR EUCH ALLERDINGS UEBER DIE
GESCHICHTE DER KRYPTOLOGIE.
IHR SOLLT AUCH KLAEREN, WAS KRYPTOLOGIE EIGENTLICH IST,
WELCHE TEILDISZIPLINEN ES GIBT UND WOMIT SICH DIESE
BESCHAEFTIGEN.
PARALLEL ZUR BEHANDLUNG DER ALGORITHMEN WERDET IHR EIN
PROGRAMM SCHREIBEN, IN DAS EINIGE DER BESPROCHENEN
ALGORITHMEN IMPLEMENTIERT WERDEN.
ABSCHLIESSEN WERDEN WIR MIT DER BEHANDLUNG DES RSA-ALGORITHMUS.



Gib mit Hilfe der beiden folgenden oder anderer Links einen Überblick über die Geschichte der Kryptografie und erläutere an einem Beispiel die Kodierung nach CAESAR.
Folgende Begriffe sollten zeitlich eingeordnet werden:

Steganografie, Codes, Chiffren, One-Time-Pad, Enigma, Public-Key-Verfahren

http://www.oszhdl.be.schule.de/gymnasium/faecher/informatik/krypto/
http://www.ferres-online.de/

Geschichte

Bezeichnungen und Fachbegriffe

Die zu übermittelnde Nachricht wird **Klartext** genannt. Die Zeichen des Klartextes stammen aus dem **Klartextalphabet** (KTA), das in der Regel das deutsche Alphabet ist. Das Verschlüsseln nennt man auch **Chiffrieren**. Dabei wird der Klartext in einen **Geheimtext** umgewandelt. Die Zeichen des Geheimtextes stammen aus dem **Geheimtextalphabet** (GTA). Das Entschlüsseln heißt auch **Dechiffrieren**.

Von den vielen kryptographischen Methoden seien nur folgende erwähnt: Früher wurden oft sogenannte **Codes** oder Codesysteme benutzt. Darunter versteht man ein Wörterbuch, in dem hinter jedem Wort eine Zahlen- oder Zeichenfolge steht, mit der das entsprechende Wort verschlüsselt wird.

Solche Systeme sind sehr unflexibel, denn wenn der Code geknackt ist, braucht man ein neues Codebuch. Außerdem können nicht beliebige Wörter verschlüsselt werden, sondern nur solche, die in dem Wörterbuch verzeichnet sind.

Beispiele für Codes

Wir befassen uns daher im Weiteren mit den vorteilhafteren **Chiffren**. Dabei werden beim Verschlüsseln jeweils ein (oder mehrere) Zeichen durch eins (oder mehrere) ersetzt. Wir beschränken uns hier auf solche Chiffren, bei denen jeweils ein Zeichen durch ein anderes ersetzt wird.

Eine Chiffre besteht aus einer **Chiffriermethode** und einem **Schlüssel**. Der Schlüssel gibt an, wie die Chiffriermethode angewandt werden soll. Da Schlüssel gewechselt werden können, sind die Chiffren flexibel. Die Chiffriermethode braucht und kann im übrigen nicht geheim gehalten werden (da im allgemeinen zu viele Leute davon wissen). Das Geheimnis besteht daher in der Kenntnis des Schlüssels, der deswegen auf einem sicheren Weg übermittelt werden muss.

Ein berechtigter Einwand lautet nun: Dann kann man ja gleich die ganze Nachricht auf diesem sicheren Weg senden! Das ist sicher richtig, jedoch ist es schwieriger, eine mitunter lange Botschaft sicher zu übertragen als einen kurzen Schlüssel. Außerdem müssen dringende Meldungen oft sehr eilend gesendet werden, während ein Schlüssel vorher in Ruhe ausgetauscht werden kann.

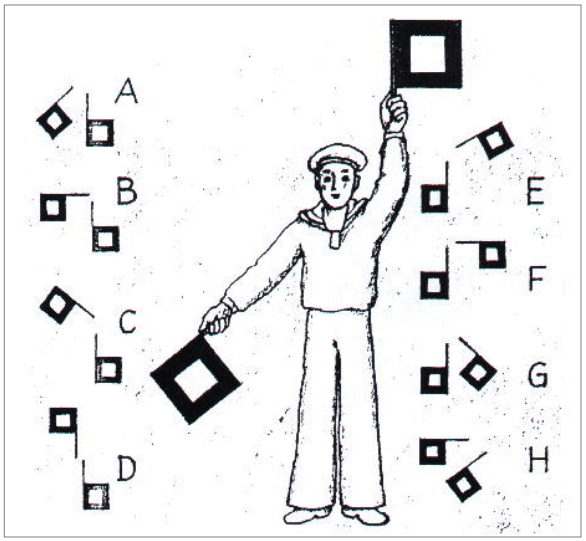
Chiffren

Codes

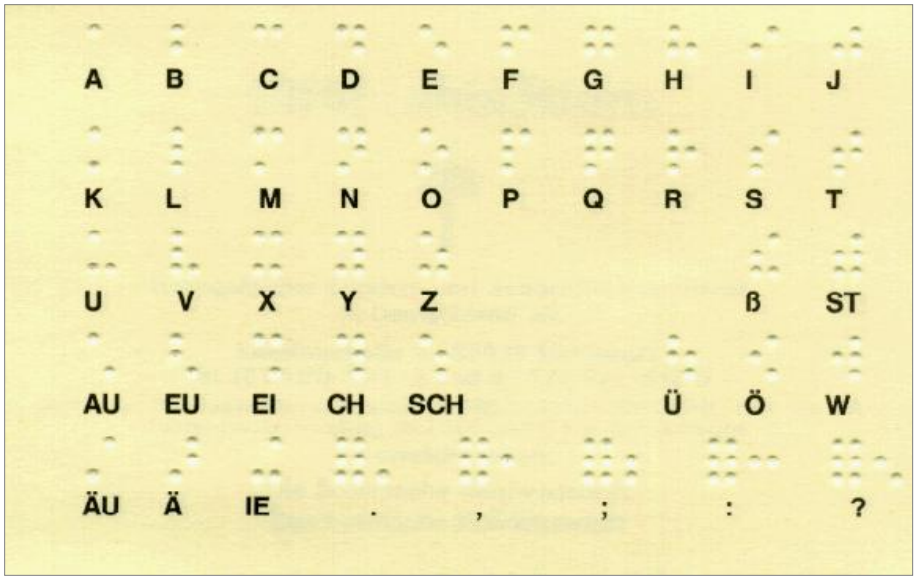
Ein Zeichen wird immer durch das selbe Zeichen des Codes codiert, es gibt keinen Schlüssel.

Morsealphabet

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 --..				



Das **Braille**-System besteht aus sechs Punkten. Die 63 verschiedenen Zeichen lassen sich mit Schreibtafel und Stift oder mittels einer Spezial-Schreibmaschine herstellen.



Die Codierung kann auch mittels eines beliebigen Buches, das Sender und Empfänger besitzen müssen, erfolgen: Dabei können Buchstaben oder ganze Wörter durch ihren Platz in dem Buch (Seite, Zeile, Nr. in der Zeile) codiert werden.

Eine weitere Möglichkeit wäre bei der Codierung mittels Computer die Nutzung des ASCII- bzw. ANSI-Codes oder auch einfach die Nutzung anderer „Schriftarten" (z.B. Wingdings) Hallo = Hallo

Geschichte der Kryptografie

ca. 500 vor Christus	Die Spartaner haben ein System namens Sky-Tale erfunden. (Spaltentransposition auf einem Holzstock mit Rollenstreifen)
ca. 100-44 vor Christus	G. J. Caesar Er entwickelte zur Zeit seiner Regentschaft im römischen Reich ein Kodierungsverfahren das auf der Gegenüberstellung eines Klartextalphabetes und eines Geheimtextalphabetes basiert. (heute **Caesar-Code** genannt).
ca. 500-1400 nach Christus	In Europa herrschte das "Dunkle Zeitalter der Kryptographie". In dieser Zeit ging viel Wissen über Kryptographie verloren. Kryptographie wurde lange Zeit als schwarze Magie angesehen. ABER in derselben Zeit blühte in arabischen Ländern neben anderen Wissenschaften auch die Kryptographie auf.
im Jahre 855 nach Christus	**Das erste Buch über Kryptoanalyse** (die Kunst des Entschlüsselns) wurde von *Abu Abd al-Rahman al-Khalil ibn Ahmad ibn Amr ibn Tammam al Farahidi al-Zadi al Yahmadi* geschrieben.
1379	Die erste **Nomenklatur** entstand. Das ist ein System, bei dem zuerst die Wörter und Begriffe in kurze Buchstabenfolgen codiert werden, und dann einer monoalphabetischen Substitution unterzogen werden. Dieses System wurde in seinen verschiedenen Anwendungen ca. 450 Jahre beibehalten und verwendet.

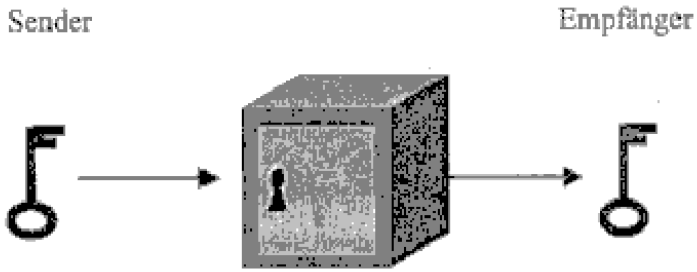
1590	Blaise de Vigenère, einer der bekanntesten Kryptologen, entwickelte mehrere Kryptographiesysteme. Eines davon, das unter dem Namen **"Vignere Chiffre"** bekannt ist, wird bis heute oft verwendet, obwohl es mit dem Coinzidenz-Index Verfahren sehr leicht geknackt wird. Dabei wird ein Passwort immer wieder über den Text "gelegt". Selbst 1917 behauptete eine Zeitschrift namens "Scientific American", daß dieser Algorithmus unmöglich zu knacken sei. Auch Philip Zimmermann, Autor von PGP, "entwickelte" diesen Algorithmus in seiner Jugend aufs neue.
1628	Die königliche Armee unter Henry II von Bourbon griff die Hugenotten in Realmont an. Diese meinten, dass ihnen die Belagerung nicht viel ausmachen würde. Eine verschlüsselte Nachricht von einem Boten der Hugenotten aus der Stadt an eine äußere Stellung wurde abgefangen. Doch die Nachricht konnte zuerst nicht entziffert werden. Nach einer Woche wurde die Nachricht an eine Familie in Albi weitergegeben, die für ihr Interesse an Kryptologie bekannt waren. Diese entschlüsselten die Nachricht: Wenn Realmont nicht bald Verstärkung durch Munition bekommt, würden sie aufgeben. Realmont gab auf. Antoine Rissignol wurde **der erste vollzeitlich angestellte Kryptoanalytiker**.

1700	Ein russischer Zar hatte eine **große Codiertabelle** von 2000-3000 Silben und Worten für die Nomenklatur.
1795	Thomas Jefferson entwickelte das "wheel cypher", **eine der ersten Kryptographie-Maschinen**.
1911	In Amerika wurde eine militärische Vorlesung über Kryptologie gehalten, die einige gute Ideen der Studenten hervorriefen. Zum Beispiel die **Umbeschriftung von Schreibmaschinentastaturen**.
1917	Entwicklung des **OTP** (One Time Pad von AT&T), das damals als absolut sicheres System galt!
1918	Das Buch "**The Index of Coincidence and its Application in Cryptography**" von William F. Friedman erschien.
1923	Auf dem internationalen Postkongress wurde die vom deutschen Ingenieur Arthur Scherbius aus Berlin entwickelte Chiffriermaschine **ENIGMA (Typ A u. B)** vorgestellt.
1926	Die deutsche Reichsmarine führte den *Funkschlüssel C* **(ENIGMA Typ C)** ein. Eine andere Variante **(ENIGMA Typ D)** wurde in verschiedenen Ländern als Patent angemeldet und dorthin verkauft. Zum Beispiel nach Großbritannien, USA, Polen, in die Schweiz und nach Schweden.

1941	Decodierung der japanischen Angriffsmeldung für den 2. Weltkrieg. Viele Historiker meinen, dass die Kryptographie im 2. Weltkrieg ein Jahr Krieg erspart hat.
1967	Das Buch "**The Codebreakers**" von David Kahn erscheint.
1975	Public-Key Kryptographie, **DES** (Data Encryption Standard) wird entwickelt.
1977	Entwicklung der **RSA**-Chiffrierung
1990	Kryptographiesoftware: **PGP (Pretty Good Privacy)** erste Version von Philip Zimmermann "Public Key for the masses"
1994	**PGP 2.63** von Philip Zimmermann bleibt für die nächsten 3 Jahre aktuell und wichtig.
1997	**PGP 5.0** von Philip Zimmermann, erstmals volle Integration in das Betriebssystem Windows 95.
1998	**PGP 5.5i** von Philip Zimmermann, Integration in das Betriebssystem Windows 98.

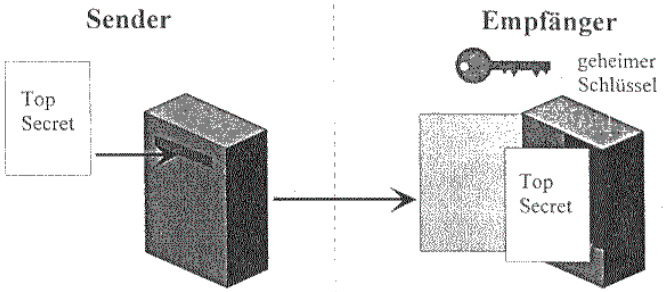
Chiffren

- **symmetrische**
  - **monoalphabetische**
  - **polyalphabetische**
- **asymmetrische**
  - **Public-key-Verfahren**



- Sender und Empfänger haben beide denselben geheimen Schlüssel
- Sowohl Ver- als auch Entschlüsseln findet im Geheimen statt
- Wer verschlüsseln kann, kann auch entschlüsseln (und umgekehrt)
- Immer besteht das Problem des Schlüsselaustauschs. Beide Seiten müssen über einen sicheren Kanal einen Schlüssel vereinbaren.

Prinzipschaltung



- Das Verschlüsseln geschieht öffentlich, das Entschlüsseln geheim
- Der Sender kann die eigene Nachricht **nicht** entschlüsseln. Dies kann nur der Empfänger
- Der Sender muss kein Geheimnis des Empfängers kennen, um zu kommunizieren

Prinzipschaltung

Monoalphabetische Chiffren

Verschiebechiffre
Methode: Verschieben des Alphabets
Schlüssel: Verschiebungsstrecke
Zahl der Schlüssel: 25 (bzw. 26, wenn man die Verschiebung um 0 Buchstaben dazuzählt)

Beispiel mit Schlüssel 3 (Das ist die bei Caesar erwähnte Methode):

KTA	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
GTA	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

Schlüsselwort
Methode: (Teilweise) Vertauschen der Buchstaben des Alphabets
Schlüssel: Schlüsselwort
Zahl der Schlüssel: Ziemlich viele (so viele, wie es Schlüsselwörter gibt)

Beispiel: Schlüsselwort LENGYMASIU (doppelte Buchstaben werden weggelassen) :

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

Das Schlüsselwort wird unter das Klartextalphabet geschrieben, die übrigen Buchstaben in alphabetischer Reihenfolge angehängt. Jetzt wird z.B. ABEND durch LEYFG verschlüsselt. Man braucht das Schlüsselwort nicht bei A anfangen zu lassen, es geht auch ein beliebiger anderer Buchstabe, zum Beispiel so:

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

Tauschchiffren
Methode: Vertauschen der Buchstaben des Alphabets
Schlüssel: Durcheinander gewürfeltes Alphabet
Zahl der Schlüssel: Alle 26! Vertauschungen des Alphabets

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

Monoalphabetischen Chiffren kann man leicht mit einer Analyse der Buchstabenhäufigkeiten „knacken", und das trotz der astronomisch hohen Schlüsselzahl von 26! bei den Tauschchiffren).

Programm | Aufgaben

Polyalphabetische Chiffren

polyalphabetische

Vigenère-Chiffre
- Schlüsselwort und Vigenère-Quadrat
- 26 Verschiebechiffren
- Schlüsselwort gibt an, welches der 26 Alphabete aus dem Vigenère-Quadrat zum Verschlüsseln benutzt wird

One-Time-Pad
- Verschiebungen zufällig
- Schlüssel ist eine Zufallsfolge
- Wenn der Text **n** Zeichen besitzt, gibt es also 26^n mögliche Schlüssel. Ansonsten läuft die Verschlüsselung wie bei Vigenère.

Bei langen Texten gibt es Regelmäßigkeiten, durch die die Schlüsselwortlänge und damit das Schlüsselwort ermittelbar werden.

KTA	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
GTAe	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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

Klartext	B	A	C	K	E	B	A	C	K	E	K	U	C	H	E	N
Schlüsselwort	H	E	F	E	Z	O	P	F	H	E	F	E	Z	O	P	F
Geheimtext	I	E	H	O	D	P	P	H	R	I	P	Y	B	V	T	S

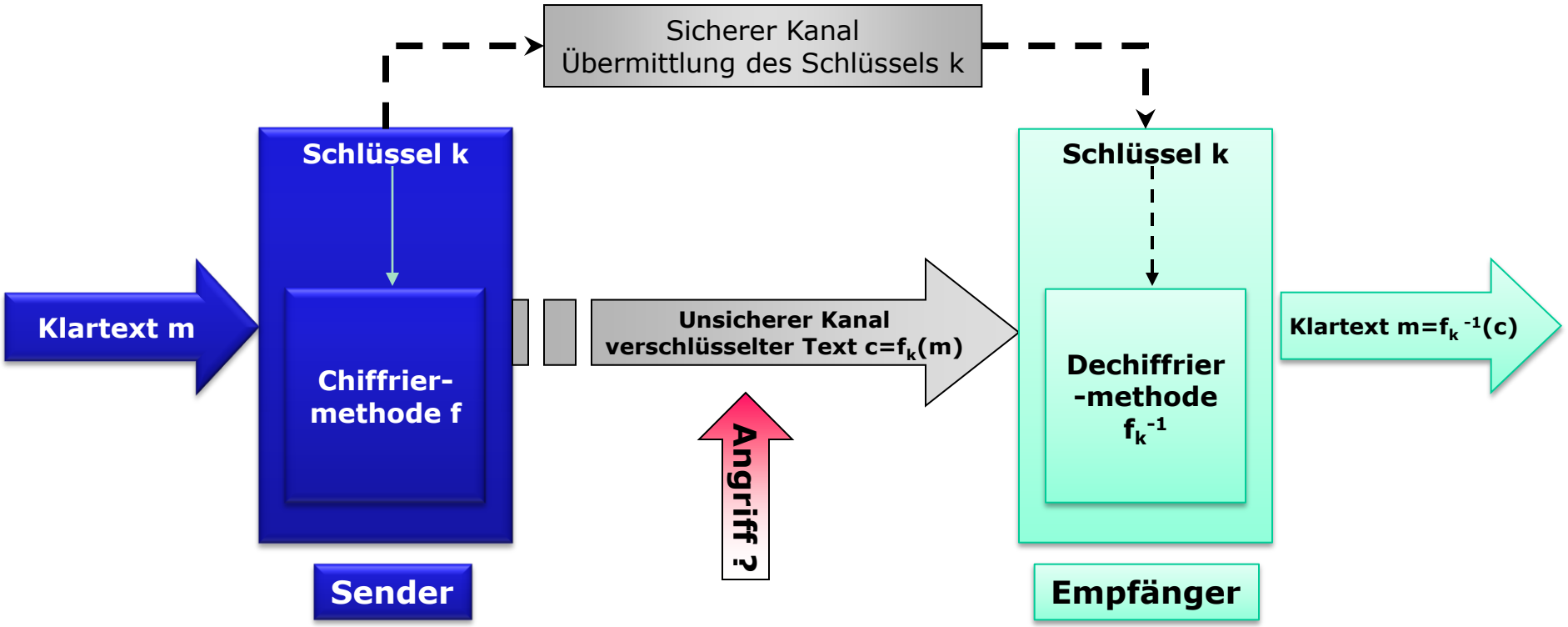
Das Schlüsselwort ist eine zufällige Buchstabenfolge, die genau so lang ist, wie der zu verschlüsselnde Text. Die Verschlüsselung selbst erfolgt dann nach dem Vigenère-Quadrat.
Diese Chiffrierung ist absolut sicher. Ihr Nachteil ist der sehr lange Schlüssel.

KTA	B	A	C	K	E	B	A	C	K	E	K	U	C	H	E	N
Schlüssel	P	V	F	O	B	B	A	W	D	S	L	S	K	N	T	G
Geheimtext	Q	V	H	Y	F	C	A	Y	N	W	V	M	Z	U	X	T

Aufgabe zur Vigenère-Verschlüsselung

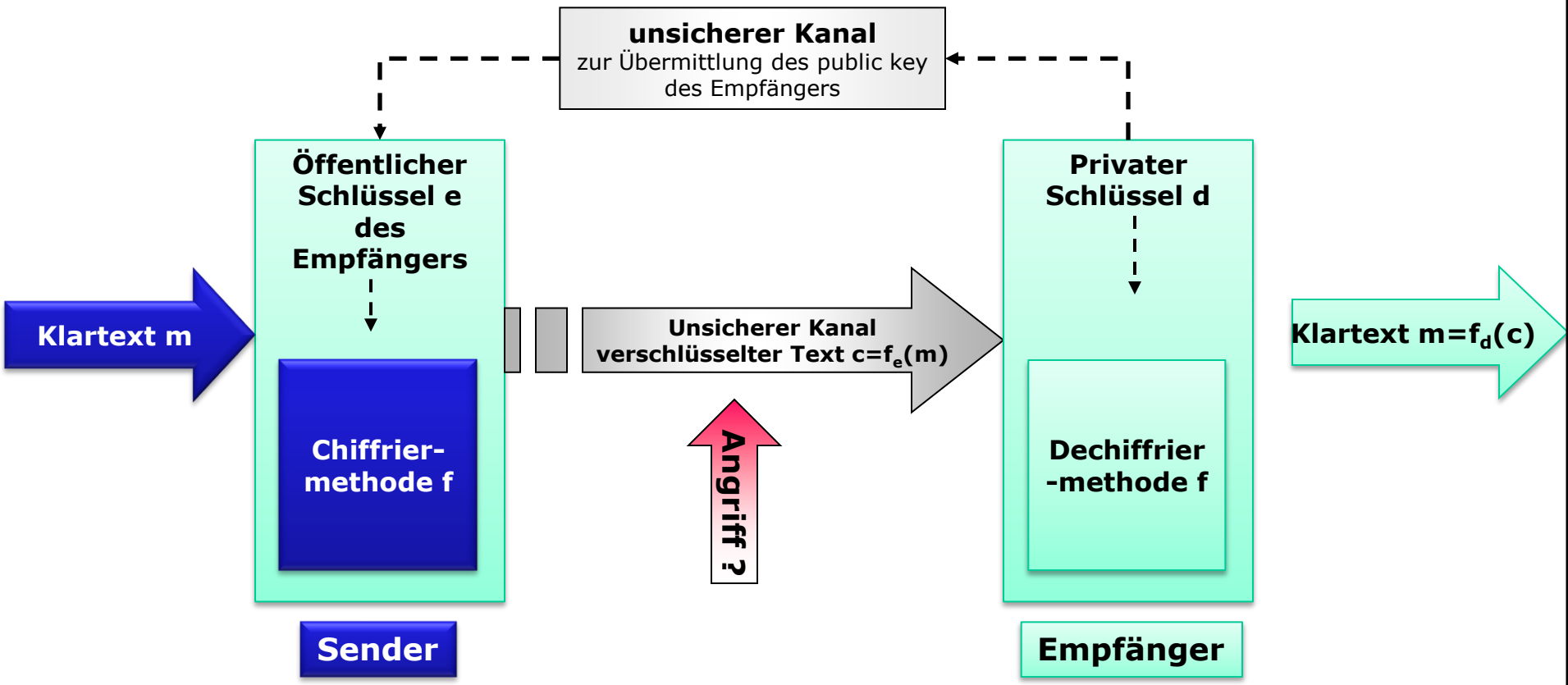
Verschlüsselung mit Passwort ?

Prinzipschaltung einer symmetrischen Chiffrierung



Man kann sich das ganze auch so vorstellen, dass der Sender eine Kiste mit geheimen Inhalt mit seinem Schlüssel verschließt, an den Empfänger schickt und dieser, der als einziger einen Zweitschlüssel besitzt, die Kiste wieder öffnen kann.
Beide Partner sind **gleichberechtigt** und haben beide Kenntnis des geheimen Schlüssels.
Daher spricht man von einem **symmetrischen** Verfahren.

PRINZIPSCHALTUNG EINER ASYMMETRISCHEN CHIFFRIERUNG



- $f_d=(f_e)^{-1}$ → f_d ist die Umkehrfunktion von f_e.
- $f_e(m)$ kann leicht berechnet werden, aber $f_d(c)$ ist für Nichteingeweihte nicht bzw. nur mit astronomisch hohem Zeitbedarf berechenbar (f_e ist eine Einwegfunktion)
- (Bsp.: Telefonbuch: f_e → Name → Nummer f_d → Nummer → Name)

RSA

Verschlüsselung mit einem Passwort

Das Prinzip:
Der Sender legt ein Passwort fest. Das Passwort wird entsprechend der Länge des zu verschlüsselnden Textes über diesen gelegt. Die ASCII- bzw. ANSI-Codes der einzelnen Zeichen des Textes werden mit den zugehörigen Zeichen des Passwortes XOR-verknüpft.
Der Empfänger entschlüsselt den Text mit dem Schlüssel (Passwort) des Senders.

Bsp.:

KTA	B	a	c	k	e	B	a	c	k	e	K	u	c	h	e	n
Schlüssel (Passwort)	G	Y	M	N	A	S	I	U	M	G	Y	M	N	A	S	I
Geheimtext	□	8	.	%	$	□	(	6	_	"	□	8	~	)	6	'

Verschlüsselung mit einem Passwort

```
ord(B)=66 → Dual → 01000010
                          ↓XOR
ord(G)=71 → Dual → 01000111
 □=chr(5) ← Dezi ← 00000101
```

```
ord(k)=107 → Dual → 01101011
                          ↓XOR
ord(N)= 78 → Dual → 01001110
 %=chr(37) ← Dezi ← 00100101
```

Für die Programmierung müssen die ASCII-Codes nicht in Dualzahlen umgewandelt werden. Folgende Konstruktion ist möglich:

g:=chr(ord(k) **XOR** ord(p))

mit

- g → Zeichen des Geheimtextes
- k → Zeichen des KTA
- p → Zeichen des Schlüssels (Passwortes)

ASCII → **A**merican **S**tandard **C**ode for **I**nformation **I**nterchange
ANSI → **A**merican **N**ational **S**tandards **I**nstitute
Die Codes sind im Tafelwerk nachlesbar und stellen eine eineindeutige Zuordnung zwischen Zeichen und Codezahlen dar. Beide Codes sind bis auf Sonderzeichen (z.B. ä, ö ü, ...) identisch. Bis zu der Codezahl 31 liegen die nicht druckbaren Steuerzeichen (8 → TAB ; 13 → Return ; 27 → ESC ; 32 → Space), die meist durch ein □ dargestellt werden.

Aufgabe

Public-Key-Verfahren

Als Beispiel für ein public-key-Verfahren soll die 1977 erfundene **RSA**-Verschlüsselung, die sich im Internet durchgesetzt hat, dienen.

(Ron **R**ivert, Adi **S**hamir, Leonard **A**dleman)

Wir werden uns „nur" mit der Funktionsweise des Verfahrens beschäftigen. Dass der mathematische Hintergrund des Verfahren exakt beweisbar ist, kann unter **http://www.ferres-online.de/** nachgelesen werden.

Zum Algorithmus:

Wähle zwei sehr große Primzahlen p, q	p = 17	q = 31
Bilde **n** = pq	n = 527	
Bilde f(n) = (p-1)(q-1)	f(527) = 16*30 = 480	
Bilde f(n)+1	f(527)+1 = 481	
Faktorisiere f(n)+1 = de	481 = 13*37	
Wähle **d** und **e**	d = 13	e = 37

f(n) ist die EULERsche Funktion, die die Anzahl der zu n teilerfremden Zahlen angibt.

Jetzt bilden **e** (encription) und **n** den public key und **d** (decription) ist der private key.

Es wird mit $\mathbf{g = k^e \bmod n}$ chiffriert und mit $\mathbf{k = g^d \bmod n}$ dechiffriert.

(g - Geheimtext ; k - Klartext)

Warum ist dieses Verfahren sicher, obwohl doch e und n öffentlich sind ?

- Zum Dechiffrieren muss d bekannt sein. Um d zu berechnen zu können, muss f(n)+1 und damit f(n) bekannt sein.
- Um f(n) berechnen zu können, muss die Primfaktorenzerlegung von n bekannt sein.
- Wenn n durch Multiplikation zweier großer Primzahlen entstanden ist, dann ist die Primfaktorenzerlegung von nur mit einem see…eeeehr großen Rechenaufwand zu finden:
  - → p und q seien von der Größenordnung 10^{10}
  - → also ist $n \approx 10^{20}$
  - → um einen primen Teiler von n zu finden, müssen alle Zahlen bis $\sqrt{n} \approx 10^{10}$ getestet werden
  - → wenn man einen Rechner hätte, der diesen Test für 10^4 Zahlen pro Sekunde schaffte, dann würde das Ganze immerhin $(10^{10} : 10^4)s = 10^6 s \approx 11{,}6$ Tage dauern.

AUFGABEN

1. Und Cäsar sprach: SBKF SFAF SFZF.

2. Man knacke den folgenden Geheimtext. Er wurde mit einer Schlüsselwortchiffrierung und einem deutschen Schlüsselwort verfasst.

YZBY YZBKJYNGJBO ZB XZY
MZHHYBHWNUKI LCA LYGHWNTJYHHYTB
LYGVYGOYB JBX LYGNYZATZWNYB

3. Entwickle einen Algorithmus, mit dem beliebige, mit monoalphabetischen Chiffren verschlüsselte Texte bei Zugrundelegung der Tabelle dechiffriert werden können. Erläutere die Arbeitsweise des Algorithmus.

Relative Häufigkeit der Buchstaben in einem deutschen Text:

A	4,3309 %	O	1,7717 %
Ä	0,4907 %	Ö	0,2547 %
B	1,5972 %	P	0,4992 %
C	2,6733 %	Q	0,0142 %
D	4,3854 %	R	6,8577 %
E	14,7004 %	S	5,3881 %
F	1,3598 %	T	4,7310 %
G	2,6672 %	U	3,1877 %
H	4,3554 %	Ü	0,5799 %
I	6,3770 %	V	0,7350 %
J	0,1645 %	W	1,4201 %
K	0,9558 %	X	0,0129 %
L	2,9312 %	Y	0,0173 %
M	2,1336 %	Z	1,4225 %
N	8,8351 %	Σ	82,7159 %

4. Man verschlüssele den folgenden Klartext mit dem Vigenère-Verfahren und dem Schlüsselwort INFORMATIK

DIESER SATZ IST FALSCH

5. Welcher Art von Chiffren ist die Verschlüsselung mit einem Passwort zuzuordnen ? Begründe !

6. Erläutere, weshalb für die Verschlüsselung die logische Verknüpfung **XOR** verwendet werden **muss**.

7. Schreibe in Delphi ein Programm, mit dem Texte mittels Passwort ver- und entschlüsselt werden können.

8. Man stelle sich folgenden Austausch einer geheimen Kiste vor: Der Sender A befestigt ein Vorhängeschloss an der Kiste, das nur er öffnen kann, und schickt die Kiste zu Empfängerin B. Diese macht zusätzlich ihr eigenes Vorhängeschloss daran, für das sie als einzige den Schlüssel hat und schickt alles wieder zu A. Nun entfernt A sein eigenes Schloss und die Fracht wandert wieder zu B. Nun kann B die Kiste öffnen.

   Dies ist ein Verfahren, bei dem eine Nachricht ohne Kenntnis des Schlüssels des jeweiligen Partners übertragen wird. Übertrage dieses Beispiel auf eine public-key-Übermittlung. Der Sender A habe dabei den privaten (öffentlichen) Schlüssel $\mathbf{D_A\ (E_A)}$, für B analog $\mathbf{D_B\ (E_B)}$. Welche Funktionen werden jeweils von A und B angewendet?

9. Es seien n=2128691 und e=385 als public key einer RSA-Verschlüsselung bekannt. Berechne d. Ist es günstig oder ungünstig, n als Produkt von Primzahlzwillingen zu berechnen.

10. Chiffriere HALLO mit dem RSA-Verfahren. Wähle dazu selbst zwei (nicht zu große) Primzahlen p und q. Dechiffriere dein Ergebnis.