Informatik

Kryptografie

Irene Rothe

Zi. B 241
irene.rothe@h-brs.de
Instagram: irenerothedesign

Informatik: 2 Semester für Ingenieure

Informatik = Lösen von Problemen mit dem Rechner

✓ Zum Lösen von Problemen mit dem Rechner braucht man **Programmierfähigkeiten** (nur mit Übung möglich): Was ist Programmieren?

✓ Was ist ein Flussdiagramm?

→**Programmiersprache C:**

- ✓ Elementare Datentypen
- ✓ Deklaration/Initialisierung
- ✓ Kontrollstrukturen: if/else, while, for
- ✓ Funktionen
- ✓ Felder (Strings)
- ✓ Zeiger
- ✓ struct
- → Speicheranforderung: malloc
- → Listen
- → Bitmanipulation

✓ Wie löst der Rechner unsere Probleme? → mit **Dualdarstellung** von Zeichen und Zahlen und mit Hilfe von **Algorithmen**

→ Ein Beispiel für ein Problem: **Kryptografie**

→ Sind Rechner auch Menschen? → **Künstliche Intelligenz**

→ Für alle Probleme gibt es viele Algorithmen. Welcher ist der Beste? → **Aufwand** von Algorithmen

Informatik: ein Semester für TJs und VTs

Informatik = Lösen von Problemen mit dem Rechner

✓ Zum Lösen von Problemen mit dem Rechner braucht man **Programmierfähigkeiten (nur mit Übung möglich)**: Was ist Programmieren? Kleine Beispiele mit Code und Flussdiagramm →Vorbereitung auf die Projektwoche

✓ Wie löst der Rechner unsere Probleme? → mit **Dualdarstellung** von Zeichen und Zahlen und mit Hilfe von **Algorithmen**

✓ Was ist ein Algorithmus? Beispiele von Algorithmen: **Sortieren** und **Suche**

→Ein Beispiel für ein Problem: **Kryptografie**

→Noch ein Beispiel für ein Problem: **Bildverarbeitung**

→Sind Rechner auch Menschen? → **Künstliche Intelligenz**

→Für alle Probleme gibt es viele Algorithmen. Welcher ist der Beste? → **Aufwand** von Algorithmen

→**Sicherheit** von Informationen

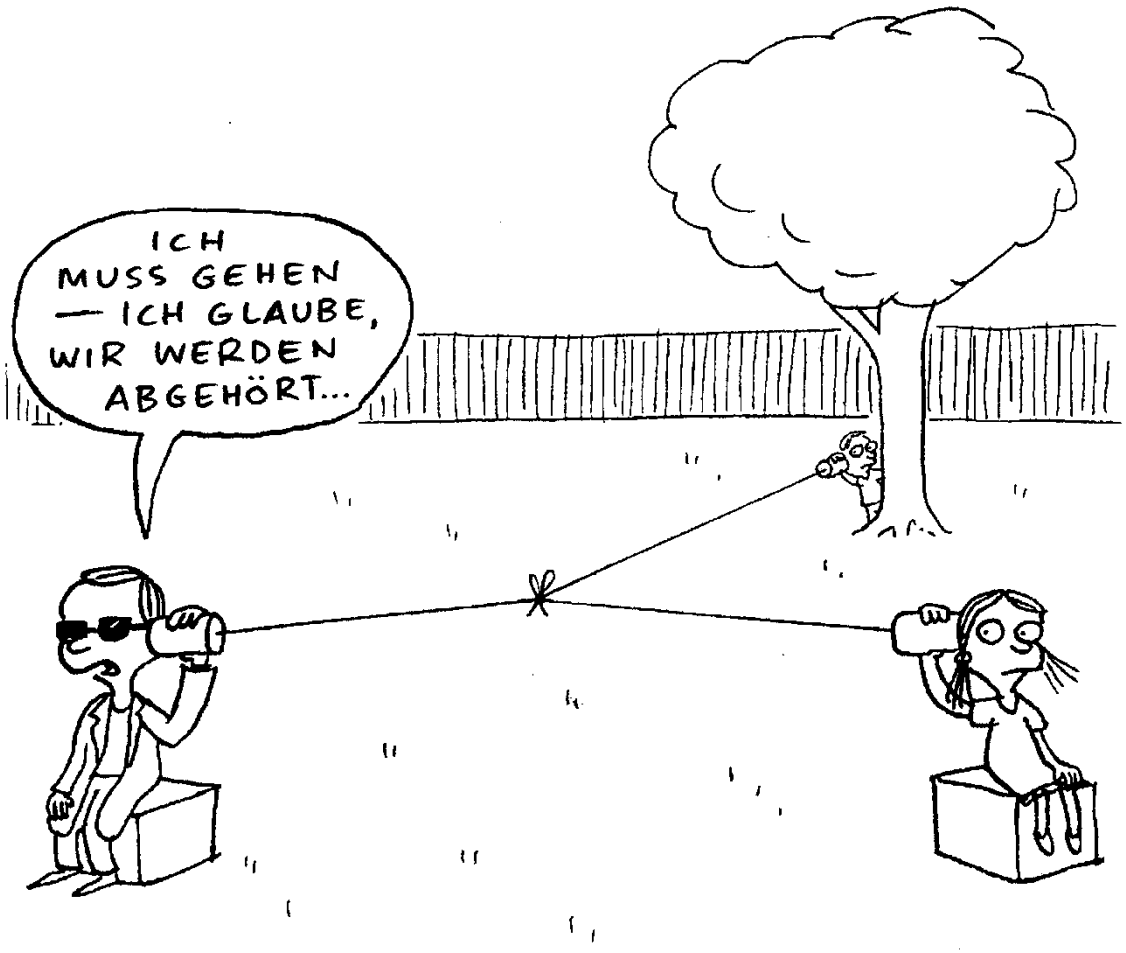
→Weitere Themen durch Mini-Vorträge

Kryptografie: Motivation

Ist mein online Banking überhaupt sicher?
Wie geht das überhaupt?

Kryptografie: Fragen

- Was ist Kryptografie?
- Was sind Techniken der Verschlüsselung?
- Wie läuft eine Verschlüsselung ab?
- Haben Chiffriermaschinen und die Enigma etwas miteinander zu tun?
- Was macht die Vorhängeschlossidee klar?
- Was ist und wie funktioniert RSA?
- Was ist PGP?


ICH MUSS GEHEN — ICH GLAUBE, WIR WERDEN ABGEHÖRT...

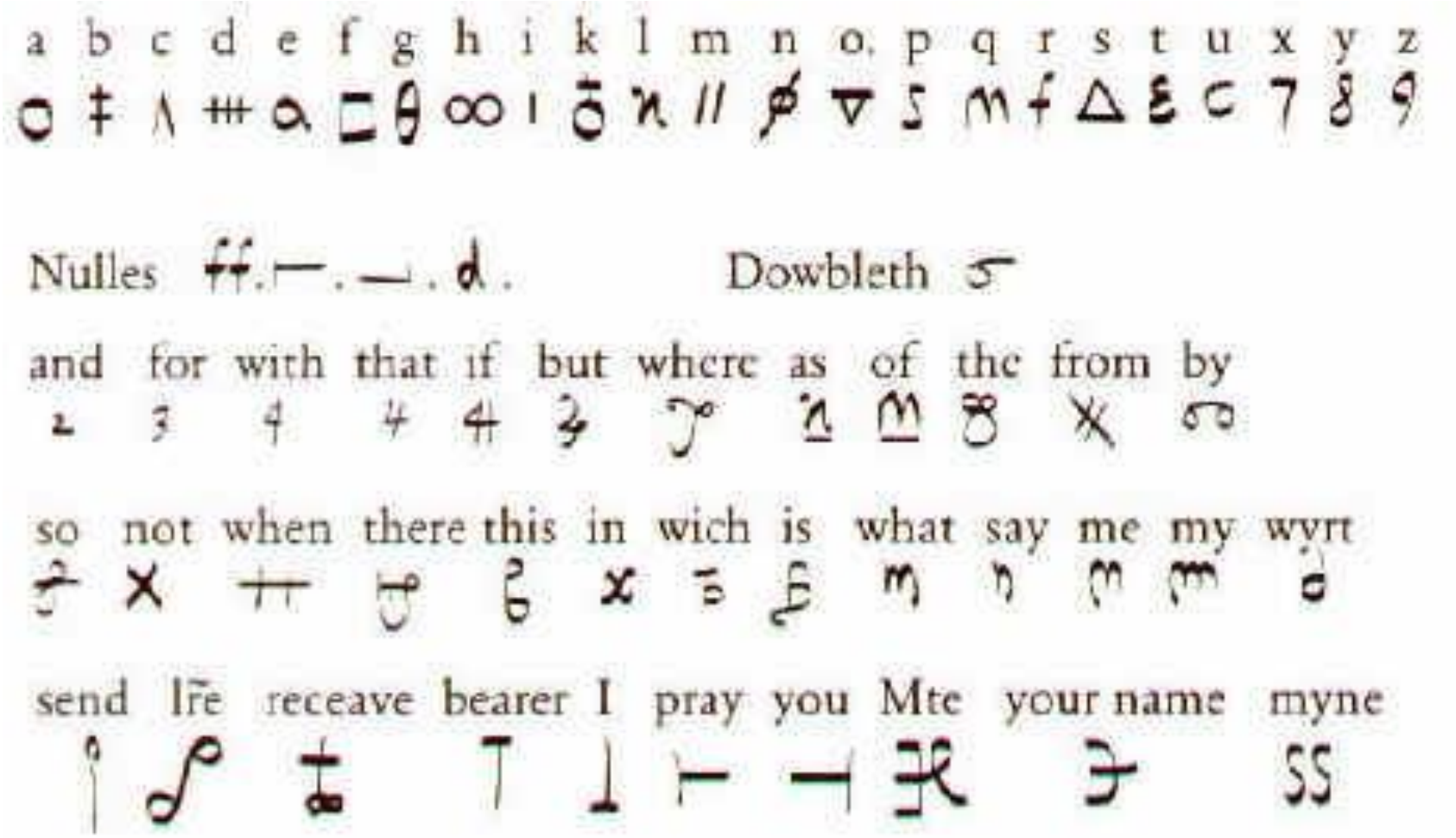
Kryptografie - Die Kunst der Verschlüsselung: Aufbau der Vorlesung

1. Geschichte der Kryptografie zur Einordnung der heute genutzten Methoden
   Geschichtliche Ereignisse, die heute eine Rolle spielen werden:
   → Maria Stuart (Anklage wegen Verrat)
   → Caeser im Galischen Krieg
   → 1. Weltkrieg (ADFGVX-System)
   → 2. Weltkrieg (Enigma)
   → Heute: RSA, PGP
2. **Ablauf** einer Verschlüsselung
3. Verwendung von **Mathematik**, um zu zeigen, dass die heutigen Methoden nachzuvollziehen sind
4. Vorführung der Verschlüsselung mit Browser (Firefox oder Explorer) beim Einkauf im Internet: die **Briefkastenidee**
5. Totsichere Verschlüsselung: **Quantenkryptografie**

Geschichte: Maria Stuart (15...)

geplanter Komplott gegen englische und irische Königin Elisabeth I.

Geschichte: Maria Stuart: Geheimschrift



Verschlüsselungsart: Steganografie

Benutzung unsichtbarer Tinte (mit Zitrone oder Milch auf Papier schreiben, lesbar machen durch Erhitzen des Blattes), um Botschaften geheim zu halten.

→ Gut geeignet für Kindergeburtstage!

Monologische Verschlüsselung: Verschlüsseln durch Transposition

Die Transposition als monologische Verschlüsselung ist eine Umstellung von Buchstaben nach einem handhabbarem System.

Beispiel 1: EHRENSENF

Beispiel 2: HALLO WIE GEHT ES IHNEN HEUTE?

Vorbearbeitung:
H L O I G H E I N N E T ?
A L W E E T S H E H U E

Verschlüsselung:

HLOIGHEINNET?ALWEETSHEHUE

Monologische Verschlüsselung: Verschlüsseln durch Substitution

Eine Substitution als monologische Verschlüsselung ist die Paarung von Buchstaben nach vorgegebenen Prinzip.

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

Klartext:
TREFFEN UM MITTERNACHT

Verschlüsselung:
ZLUWWUS EC CGZZULSVMBZ

(benutzte Caesar im Gallischen Krieg)

Folgendes neueres Buch hat viel mit solchen Verschlüsselungen zu tun:
NVJLGRUI

Kryptografie - Die Kunst der Verschlüsselung: Aufbau der Vorlesung

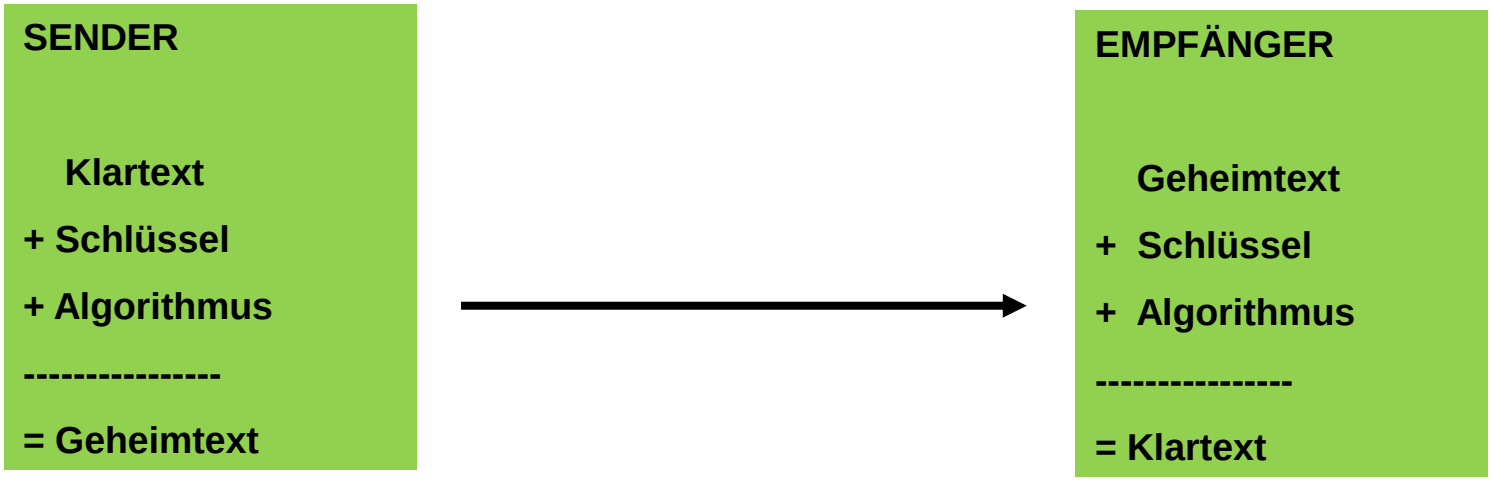
1. ✓ Geschichte der Kryptografie zur Einordnung der heute genutzten Methoden
   Geschichtliche Ereignisse, die heute eine Rolle spielen werden:
   → Maria Stuart (Anklage wegen Verrat)
   → Caeser im Galischen Krieg
   → 1. Weltkrieg (ADFGVX-System)
   → 2. Weltkrieg (Enigma)
   → Heute: RSA, PGP
2. **Ablauf** einer Verschlüsselung

3. Verwendung von **Mathematik**, um zu zeigen, dass die heutigen Methoden nachzuvollziehen sind

4. Vorführung der Verschlüsselung mit Browser (Firefox oder Explorer) beim Einkauf im Internet: die **Briefkastenidee**

5. Totsichere Verschlüsselung: **Quantenkryptografie**

Allgemeiner Verschlüsselungsablauf



Die Sicherheit eines Kryptografie-Systems darf nicht von der Geheimhaltung des Algorithmus abhängen, sondern von der Geheimhaltung des Schlüssels.

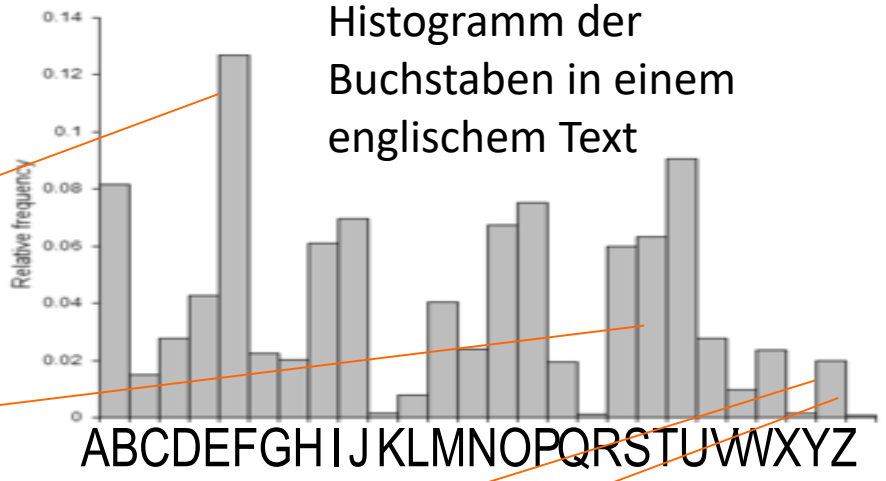
Entschlüsselung

- durch Häufigkeitsanalyse kann man die Buchstaben erraten
- z.B. kommt das 'e' im Deutschen am häufigsten vor (Reihenfolge im Deutschen: e,n,i,s,r,a,t...)
- danach kann man den Text durch Ausprobieren erraten
- Voraussetzungen: Text darf nicht zu kurz sein, Sprache muss bekannt sein
- genau dies wurde Maria Stuart zum Verhängnis

Entschlüsselung der Substitutionsmethode

Buchstabenanzahlen in einem englischen Text:

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



Histogramm der Buchstaben in einem englischem Text

Häufige 3-Buchstabenwörter:

THE AND FOR WAS HIS

Polyalphabetische Verschlüsselung

- Monologische Verschlüsselung klappte gut bis zum 17.Jhd.
- danach benutzte man 2 Geheimalphabete (1 und 2) *abwechselnd*

Beispiel:

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

Polyalphabetische Verschlüsselung

• Babagge fand 1854 Verfahren, um auch diese Geheimschriften zu knacken

• dies kam aber erst im 20. Jhd. ans Licht bei der Sichtung seines Nachlasses

• man vermutet, dass die Briten Babagges Entschlüsselung ausnutzten und ihn zur Geheimhaltung verpflichteten

• es gibt auch berühmte Schätze, die bis heute niemand fand, obwohl ein verschlüsselter Brief mit Ortsangaben vorhanden ist, z.B. die Beale-Chiffren von 1820 (Eine Möglichkeit Millionär zu werden: einfach diese Chiffre knacken!)

Verschlüsselung im 1.Weltkrieg

- Painvin half 1918 den Allierten den deutschen Code zu knacken: ADFGVX-System
- damit wusste man vorher, wo die Deutschen ihren Überraschungsangriff planten
- Codeknacker hatten Oberhand gegen Codierer!
- **ADFGVX-System**: Mischung aus *Substitution* und *Transposition*

Verschlüsselung im 1.Weltkrieg: ADFGVX-System: 1. Stufe

	A	D	F	G	V	X
A	8	P	3	D	1	N
D	L	T	4	O	A	H
F	7	K	B	C	5	Z
G	J	U	6	W	G	M
V	X	S	V	I	R	2
X	9	E	Y	0	F	Q

2. Stufe: Vorführung an der Tafel oder Internet

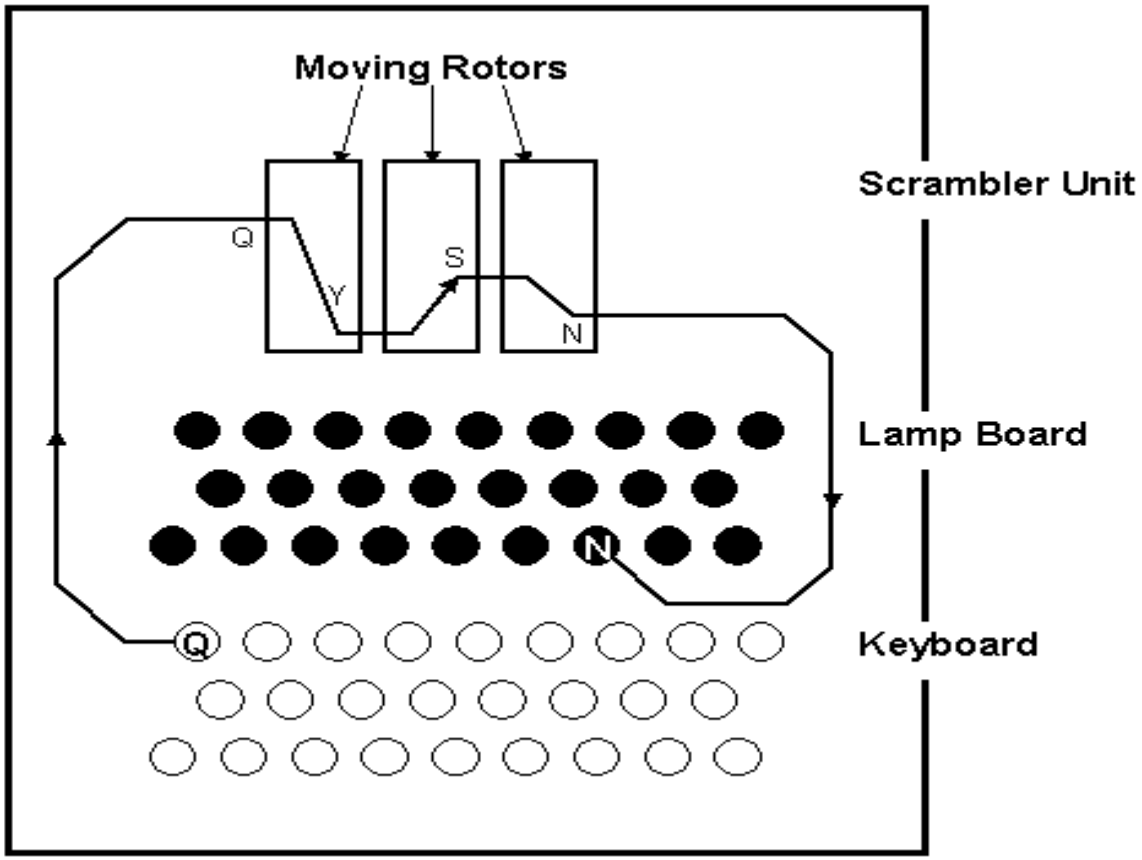
Verschlüsselung durch Chiffriermaschinen

- Chiffrierscheibe (15.Jhd.), Kryptorolle – abhängig vom Holzstab (5.Jhd.)
- Enigma von Scherbius 1918 erfunden
  - besteht aus Walzen, deren Lage verändert werden kann
  - Besteht zusätzlich aus Steckverbindungen, die auch neu gesteckt werden können

Aus Exitspiel mit Känguru

Chiffriermaschinen: Enigma 1

Chiffriermaschinen: Enigma - Inneres



Verschlüsselung im 2.Weltkrieg mit der Enigma

1. Lage der Walzen wurde jeden Tag verändert und wurde **Tagesschlüssel** genannt

2. Tagesschlüssel wurde in sogenannten **Schlüsselbüchern** verteilt

3. pro Nachricht wurde eine neue Steckverbindung verwendet, die am Anfang der Nachricht mit Tagesschlüssel verschlüsselt mitgeteilt wurde

4. Nachricht wurde mit Enigma getippt

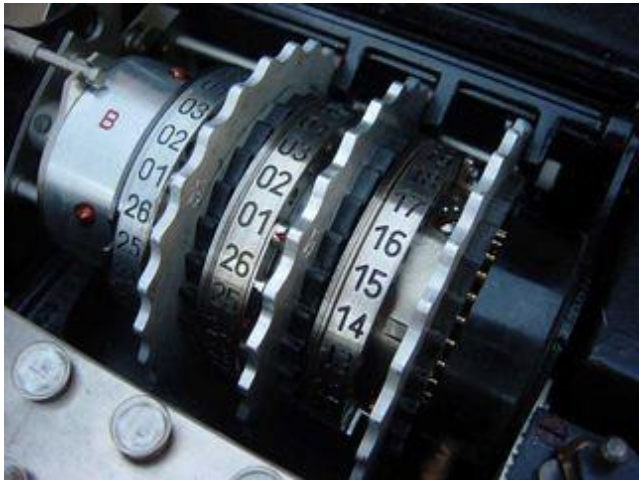
5. Enigma gab verschlüsselten Text aus

6. Verschlüsselter Text wurde von Funker dann gefunkt

Alan Turing und das Enigma Projekt

Alan M. Turing
1912-1954

The Mansion at Bletchley Park
(England's wartime codebreaking center)



Source: http://www.ellsbury.com/enigmabombe.htm

Enigma: Wie konnte dies von den Allierten geknackt werden?

- alle Nachrichten wurden selbstverständlich abgefangen und aufgehoben
- eine Enigma wurde im Kampf ergaunert
- ab und an wurden Schlüsselbücher ergattert
- im Bletchley Park arbeitet u.a. Alan Turing an der Entschlüsselung:
    - Entschlüsselung durch sogenannte Bomben (riesige Maschinen)
    - man wusste z.B., dass am Anfang immer der Wetterbericht gesendet wurde, dort konnte man nach Wörtern wie 'WETTER' suchen
    - solche Wörter waren immer der Start
    - danach gab es immer noch 159.000.000.000.000.000.000 mögliche Einstellungen für die Walzen
    - Turing fand Tricks, um diese Möglichkeiten einzuschränken
- gleichzeitig wurden große Beiträge in der Mathematik geleistet
- alles war TOP SECRET, auch Angehörige durften nichts wissen, Deutsche durften nicht ahnen, dass ihre Enigmas nicht mehr sicher waren
- erst 1974 wurde Geheimhaltung aufgehoben (bis dahin glaubte man immer noch, dass Enigma sicher sei), da war Turing leider schon tot
- man behauptet, dass durch Bletchley Park der 2. Weltkrieg viel viel schneller beendet werden konnte

Andere Verschlüsselungen

Amerikaner nutzten in verschiedenen Kriegen *Navajo*-Indianer

- dies ist nie aufgedeckt worden, da nie ein Indianer ergriffen wurde

- Sprache ist so ungewöhnlich und noch niemand hatte sie bis dahin erforscht, sodass es Sprachwissenschaftler nicht gelang, sie zu entschlüsseln

- Navajo-Verschlüsselung wurde erst 1982 bekannt gegeben

Verschlüsselung im Computerzeitalter: Vorbereitung - Codierung

- Verschlüsselung von Nullen und Einsen

- Deutsch in ASCII ist auch eine Codierung, über die aber jeder Bescheid weiß

H: 1001000
A: 1000001
L: 1001100
O: 1001111
Hiermit kann man das Wort HALLO codieren.

Oder
D: 1000100
A: 1000001
V: 1010110
I: 1001001
Hiermit kann man das Wort DAVID codieren.

Verschlüsselung: Beispiel mit 0en und 1en

Botschaft:	H	A	L	L	O
Botschaft in ASCII	1001000	1000001	1001100	1001100	1001111
Schlüssel = DAVID	1000100	1000001	1010110	1001001	1000100
Geheimtext	0001100	0000000	0011010	0000101	0001011

Algorithmus: Botschaftszeichen!=Schlüsselzeichen -> 1
Botschaftszeichen==Schlüsselzeichen -> 0

Bemerkung: Das ist ein symmetrischer Verschlüsselungsalgorithmus

Einigung auf einen gemeinsamen Schlüssel: Wie einigt man sich über den Schlüssel ohne sich zu treffen?

→ Die Diffie-Hellman-Idee

Typische klassische Paradoxie: Schlüssel selbst ist auch ein Geheimnis!

Wikipedia

• 1974 hatten Diffie und Hellman eine *geniale* Idee, wie man den Schlüsseltausch zwischen BOB und ALICE so ablaufen lassen kann, dass man alles übers öffentliche Internet oder die Post klären kann, sodass eine Schnüffelperson EVE nichts mit den abgefangenen Informationen anfangen kann

• diese ist das **erste bekannte Schlüsselaustauschverfahren**, bei dem es möglich ist, geheime Schlüssel über öffentliche Kanäle zu vereinbaren.

• Erklärung mit dem Prinzip von *Vorhängeschlössern* (von Shamir)
→Die Idee der asymmetrischen Verschlüsselung war geboren.

Bemerkung: wird bei whatsapp benutzt

Einigung auf einen gemeinsamen Schlüssel: die Vorhängeschlossidee

ALICE will geheime Nachricht an BOB schicken:

1. ALICE legt eine Nachricht in eine Eisenkiste, verschließt diese mit einem Vorhängeschloss und einem Schlüssel und behält den Schlüssel
2. ALICE schickt die Eisenkiste mit der Post an Bob
3. BOB hängt ein eigenes Vorhängeschloss an die Kiste und behält den Schlüssel zu seinem Schloss
4. BOB schickt die Kiste zurück an ALICE mit der Post
5. ALICE nimmt ihr Schloss von der Kiste mithilfe ihres Schlüssels und schickt die Kiste mit der Post an BOB zurück
6. BOB muss nun nur noch sein eigenes Vorhängeschloss öffnen und kann die Nachricht von ALICE lesen.

Kein Schlüssel wurde ausgetauscht und trotzdem konnte niemand anderes außer BOB die Nachricht von ALICE lesen!

Vorhängeschlossidee mit Zahlen

ALICE will eine geheime Nachricht an BOB schicken mit der Verschlüsselungsfunktion `7^x mod 11`:

1. ALICE wählt eine zufällige Zahl (z.B. **3**) und nennt sie **A** und hält sie geheim
2. BOB wählt eine zufällige Zahl (z.B. **6**) und nennt sie **B** und hält sie geheim
3. ALICE berechnet:
   `7^A mod 11 = 7^3 mod 11 = 343 mod 11 = 2 =` α
4. BOB berechnet:
   `7^B mod 11 = 7^6 mod 11 = 117649 mod 11 = 4 =` β
5. ALICE schickt α an BOB
6. BOB schickt β an ALICE
7. ALICE nimmt BOBs Ergebnis und berechnet:
   β`^A mod 11 = 4^3 mod 11 = 64 mod 11 = 9`
8. BOB nimmt ALICEs Ergebnis und berechnet:
   α`^B mod 11 = 2^6 mod 11 = 64 mod 11 = 9`

9 ist der gemeinsame Schlüssel, den beide benutzen!

Achtung:a^b bedeutet „a hoch b“, also a wird b-mal mit sich selbst multipliziert!

Was hat es auf sich mit der Funktion $Y^X \bmod P$

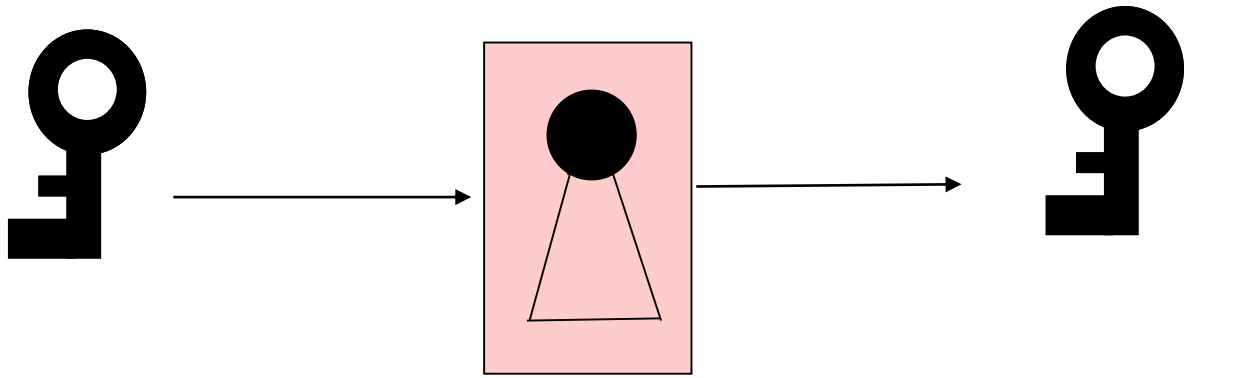
- diese Funktion ist eine sogenannte **Einwegfunktion**, d.h. sie ist fast nicht umkehrbar (z.B. Telefonbuch: Suche nach bestimmter Telefonnummer)
  Ist dies wirklich nicht möglich? -> *Offenes Problem*!
- **Beispiel aus dem Alltag**: Vermischung gelber und blauer Farbe zu grün ist einfach, aber die Trennung ist nahezu unmöglich ODER das Aufschlagen eines Hühnereis in einer Pfanne
- **Problem des diskreten Logarithmus modulo einer großen Primzahl**: Es ist sehr EINFACH aus **Y** und **X** den Wert **G=**Y^X **mod P** zu berechnen, aber PRAKTISCH UNMÖGLICH, aus **Y** und **G X** zu berechnen.
- Dies geht eigentlich nur durch *systematischem Ausprobieren*!
- umso größer **Y** und **P** gewählt werden, umso aufwendiger wird das Probieren
- Also: auch wenn EVE **Y** und **P** kennt, nutzt ihm das sehr wenig, um die Zahlen **A** und **B** zu erraten, die sich ALICE und BOB ausgedacht haben.

Das RSA (Ronald Rivest, Adi Shamir, Leonard Adleman) - Verfahren

Wikipedia

- **Vereinfachung** des Schlüsselverfahrens (in dem vorhin behandelten Modell, müssen beide vorher kommunizieren, um sich geheime Botschaften schicken zu können)
- *Idee*: jeder kann ein Vorhängeschloss zuschnappen lassen, aber nur der mit dem Schlüssel kann es öffnen, also könnte ALICE (Bank) ein Vorhängeschloss öffentlich irgendwo hinterlegen, sodass es jeder (Bankkunde) benutzen kann, um ihr etwas Geheimes zu schicken
- Ausnutzung des *noch nicht gelösten F*aktorisierungsproblems

Symmetrische Verschlüsselung



Bis 1976 glaubte man, dass Sender und Empfänger immer *gemeinsam* einen geheimen Schlüssel benötigen.
Aber: Symmetrische Verschlüsselung ist viel schneller als asymmetrische Verschlüsselung.
Beispiel: Folie 29, RC4

Kryptografie - Die Kunst der Verschlüsselung: Aufbau der Vorlesung

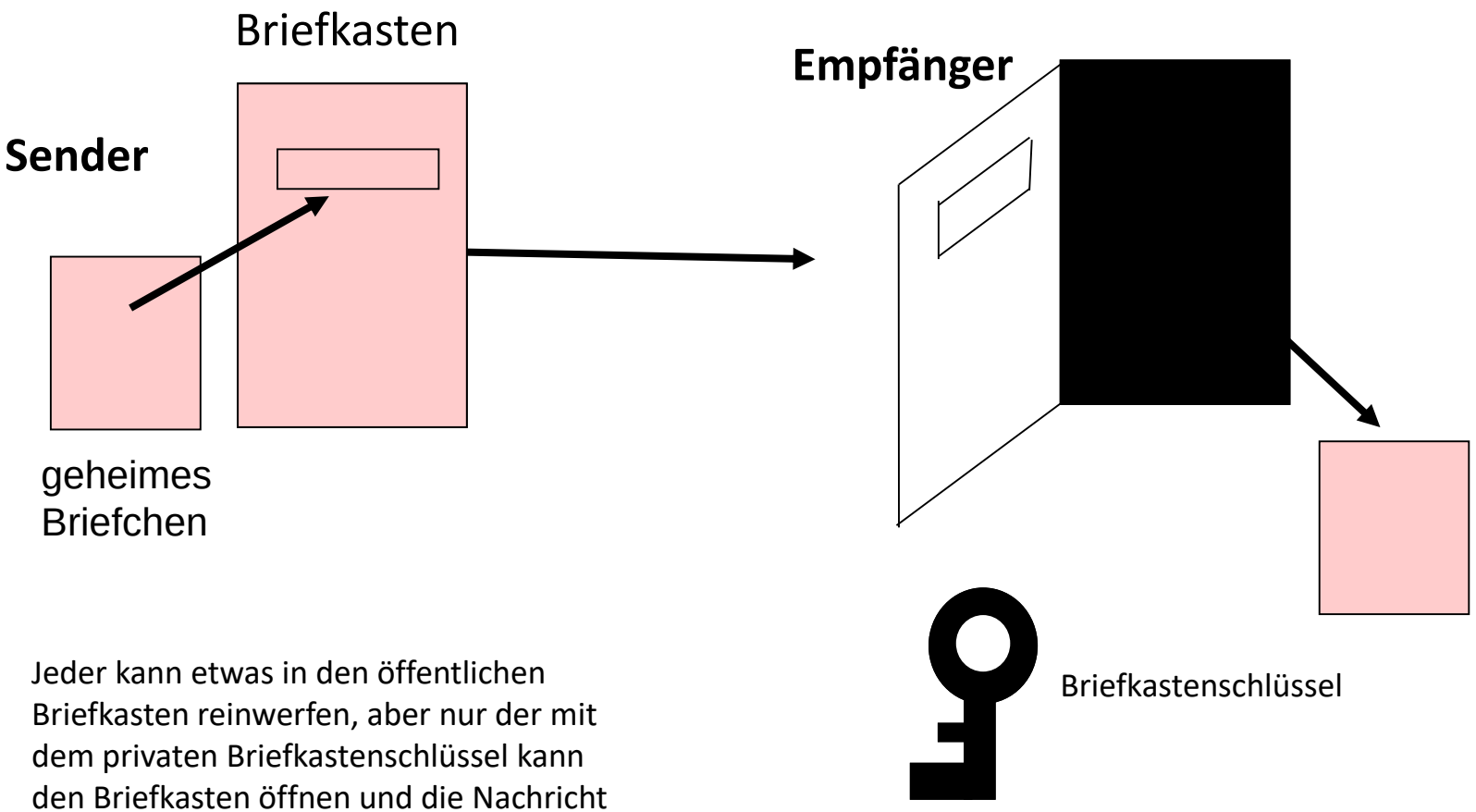
1. ✓ Geschichte der Kryptografie zur Einordnung der heute genutzten Methoden
   Geschichtliche Ereignisse, die heute eine Rolle spielen werden:
   → Maria Stuart (Anklage wegen Verrat)
   → Caeser im Galischen Krieg
   → 1. Weltkrieg (ADFGVX-System)
   → 2. Weltkrieg (Enigma)
   → Heute: RSA, PGP
2. ✓ **Ablauf** einer Verschlüsselung

3. ✓ Verwendung von **Mathematik**, um zu zeigen, dass die heutigen Methoden nachzuvollziehen sind

4. Vorführung der Verschlüsselung mit Browser (Firefox oder Explorer) beim Einkauf im Internet: die **Briefkastenidee**

5. Totsichere Verschlüsselung: **Quantenkryptografie**

Asymmetrische Verschlüsselung: Public-Key



Jeder kann etwas in den öffentlichen Briefkasten reinwerfen, aber nur der mit dem privaten Briefkastenschlüssel kann den Briefkasten öffnen und die Nachricht rausholen.

RSA-Verfahren

- BOB muss Schlüssel erzeugen, den er *öffentlich* irgendwo hinstellt.
- Der öffentliche Schlüssel muss durch eine *Einwegfunktion* erzeugt sein.
- BOB muss die ihm geschickten Nachrichten entschlüsseln können. Dazu braucht er einen *privaten* Schlüssel.

Mathematisch wird hier ausgenutzt das folgende Problem:

$$p * q = N$$

ist LEICHT zu berechnen. p und q sind dabei Primzahlen.
Hat man dagegen N und will p und q berechnen, ist das PRAKTISCH UNMÖGLICH (bis heute nur durch *systematisches* Ausprobieren möglich).

- N wäre dann BOBs *öffentlicher* Schlüssel.
- p und q sind BOBs *private* Schlüssel.

RSA-Verfahren: einige Infos

- da Rechner immer schneller werden, nimmt man heutzutage N aus einem Bereich 10 hoch 300
- Angst bei RSA: was ist, wenn doch mal jemand ein effektives Verfahren findet?
- 1977 erster öffentlicher Auftritt von RSA mit folgendem

  N = 114381625757888867669235779916146612010218296721242362562561842935706935245733897830597123563958705058989075147599290026879543541

RSA-Verfahren

1994 hatte eine Gruppe von Freiwilligen die Lösung gefunden:

q = 34905295108476509491478496199038981334177646384933
7843990820577

p = 32769132993266709549961988190834461413177642967992942539798288533

Eigentlich wurde RSA eher gefunden, aber von den Briten geheim gehalten. Die Ersterfinder sind eigentlich James Ellis, Chifford Cocks und Malcom Williamson 1975.

RSA-Verfahren: Vorführung mit Zahlen: Vorbereitung - Nachricht: Wort als Zahl

ALICE will die Nachricht **X** (Schmatzer) schicken:

1. X in ASCII: 1011000,
2. was als Dezimalzahl die 88 ist.

Also könnte 88 die zu verschlüsselnde Nachricht sein.

Im folgenden Beispiel ist die Nachricht allerdings 2 („JA“, ich heirate dich), damit die Rechnung nicht so riesig wird.

RSA-Verfahren: Vorführung mit Zahlen

ALICE will geheime Nachricht an BOB schicken:

1. BOB wählt zwei *riesige* Primzahlen p, q, z.B. p=3 und q=11. Diese Zahlen bleiben geheim. BOB berechnet: p*q=N, also 3*11=33.
2. BOB berechnet d=(p-1)(q-1)=2*10=20 und wählt zwei weitere Zahlen e und f, z.B. e=7 und f=3, mit e*f/d hat Rest 1 (technisches Detail, ggT!!).
3. BOB veröffentlicht **e** und N als sein *öffentliches* Schlüsselpaar, f ist sein *geheimer (privater)* Schlüssel.
4. ALICE will die Nachricht 2 (JA, ich heirate Dich) schicken. ALICE verschlüsselt ihre Nachricht mit BOBs öffentlichen Schlüsseln wie folgt:

$$C = 2^{e} (\mathrm{mod}\, N) = 2^{7} (\mathrm{mod}\, 33) = 29.$$

   Bemerkung: Es gibt clevere Methoden in der Mathematik, die diese Rechnung schnell ausführen!

5. ALICE schickt die Nachricht C=29 an BOB.
6. BOB entschlüsselt die Nachricht mit seinen privaten Schlüssel f wie folgt:

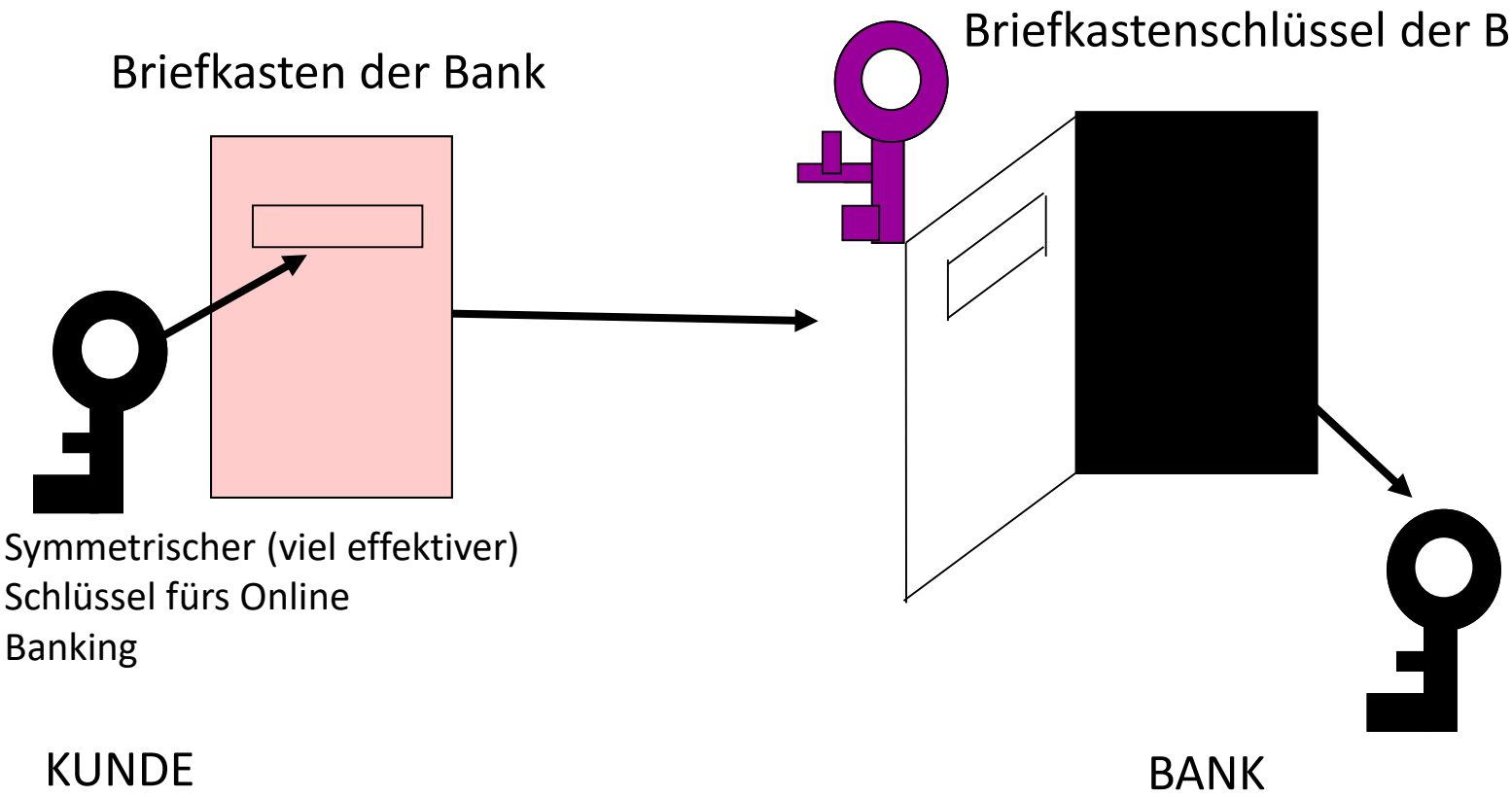
$$C^{f} (\mathrm{mod}\, N) = 29^{3} (\mathrm{mod}\, 33) = 2,$$

was JA, ich heirate Dich, bedeutet.

RSA-Verfahren: Sicherheit

Die Sicherheit von RSA hängt ab von der Schwierigkeit, große Zahlen zu faktorisieren. Deshalb müssen *p* und *q* sehr groß gewählt werden: >100 Bits

Verschlüsselung mit Bank



Also: Der Schlüssel für die symmetrische Verschlüsselung wird asymmetrisch verschickt.

Verschlüsselung mit der Bank

1. **Erzeugung eines Schlüssels** X auf meinem Rechner, den ich der Bank schicken will, um mit ihr einen sicheren Kanal (via symmetrischer Verschlüsselung) aufbauen zu können, über den ich meine Transaktionen durchführen kann.
2. Holen des **öffentlichen Schlüssels** der Bank
3. **Verschlüsselung meines Schlüssels** X mit dem öffentlichen Schlüssel der Bank via RSA und Verschickung des verschlüsselten Schlüssels an die Bank über öffentlichen Kanal (dafür brauche ich eine PIN -*personal identification number*- um mich zu authentifizieren und zu zeigen, dass ich berechtigt bin, mit der Bank zu kommunizieren).
4. **Bank entschlüsselt** meinen verschlüsselten Schlüssel mit Hilfe ihres privaten Schlüssels.
5. Aufbau einer sicheren Verbindung mit mir über den Schlüssel X für sichere Transaktionen.
6. Transaktion wird unterschrieben mit einem Einmalpasswort (TAN: *Transaktionsnummer*), womit das Geschäft rechtskräftig wird.

Alles geschieht in einem Zeitfenster.

RSA Security Inc.

- Gegründet von Rivest, Shamir und Adleman
- https://de.wikipedia.org/wiki/RSA_Security (in späteren Vorlesung: aus Snowden-Dokumenten (2013) wurde bekannt, dass man für die NSA eine Krypto-Backdoor eingebaut hatte, in dem man einen umstrittenen (seit 2007) Zufallszahlengenerator zum Standard machte (Dual-EC-DRBG), der knackbar ist)
- https://de.wikipedia.org/wiki/RSA-Kryptosystem: Abschnitt „Schwierigkeit des Faktorisierungsproblems“ bezieht sich auf Jens Franke von der Uni Jena (https://de.wikipedia.org/wiki/Jer

https://www.math.uni-bonn.de/members?mode=portrait&uid=frankea

RSA in PGP (Pretty Good Privacy) Programm

Wikipedia

- Ziel: RSA ohne Hintertür!!!
- dieses Programm schrieb in den USA Phil Zimmermann
- private Schlüsselerzeugung läuft über zufällige Mausbewegungen auf dem Bildschirm (Erzeugung von Zufallszahlen, die dann zur Primzahlerzeugung dienen)
- Programm wurde nicht verkauft (sonst wäre es garantiert vom amerikanischen Senat verboten worden), sondern 1991 frei ins Internet gestellt
- Zimmermann bekam aber trotzdem riesigen Ärger, der erst 1996 endete
- PGP bekannt für Festplattenverschlüsselung und um sicher Dateien zu löschen, jetzt auch für emails

Das PGP (Pretty Good Privacy) Programm

- Wichtig ist Ende-zu-Ende Verschlüsselung (Verschlüsselung am Gerät des Senders)
- Installation von PGP in Outlook (sehr praktisch und einfach): http://einklich.net/anleitung/pgp2.htm
- Key Programm: http://www.chip.de/downloads/Gpg4win_29258649.html

PGP: sichere emails

Frage: Sollen emails *Postkarten* oder *Briefe* sein?

Zwei Aspekte sind dabei wichtig:

1. Sorgfältiger Schutz des privaten Schlüssels vor Verlust oder unbefugten Zugriff
2. Globale Schlüsselverzeichnisse: Echtheit der öffentlichen Schlüssel?

→ Idee der Schlüsselhinterlegung bei Vertrauenswürdigem Dritten (TTP)? Dem Staat?

→ Teufelskreis: Web of Trust (WoT)

PGP: man hat alles selbst in der Hand

S/MIME (SSL): öffentliche Schlüssel kommen von Schlüsselhinterlegern abgelegt bei undurchsichtigen Zertifizierungsstellen, dadurch läuft alles aber schön automatisch ab

Andere Begriffe

- *Digitale Signatur:* Unterschrift von EINER Person erzeugt, aber von VIELEN verifizierbar.
- *TAN*: Einmal-Passwort (one time Pad): muss nicht verschlüsselt werden, da es nur einmal benutzt wird
- SSL: bisher erfolgreichstes Sicherheitsprotokoll, nutzt RSA
- Heutige bekannte symmetrische Verschlüsselungen: DES, AES, RC4
- Bundesgesetzblatt – öffentliche Schlüssel von Zertifizierern:
  http://www.bundesnetzagentur.de/enid/7314a7a33471388f742a8734f9408910,d0d2d85f7472636964092d0936333139/Veroeffentlichungen/Oeffentliche_Schluessel_st.html
  → geht nicht mehr, wird aber irgendwo immer noch zu finden sein

Kryptografie - Die Kunst der Verschlüsselung: Aufbau der Vorlesung

1. ✓ Geschichte der Kryptografie zur Einordnung der heute genutzten Methoden **Geschichtliche Ereignisse**, die heute eine Rolle spielen werden:
   → Maria Stuart (Anklage wegen Verrat)
   → Caeser im Galischen Krieg
   → 1. Weltkrieg (ADFGVX-System)
   → 2. Weltkrieg (Enigma)
   → Heute: RSA, PGP
2. ✓ **Ablauf** einer Verschlüsselung

3. ✓ Verwendung von **Mathematik**, um zu zeigen, dass die heutigen Methoden nachzuvollziehen sind

4. ✓ Vorführung der Verschlüsselung mit Browser (Firefox oder Explorer) beim Einkauf im Internet: die **Briefkastenidee**

5. Totsichere Verschlüsselung: **Quantenkryptografie**

Quantencomputer

…
sind der Alptraum eines Kryptographen und der Traum jedes Kryptoanalytikers. Mit seiner Hilfe kann man Zahlen in sehr kurzer Zeit in ihre Primfaktoren zerlegen und so das RSA-Verfahren knacken.

Haken: Bisher konnte niemand einen sinnvoll einsetzbaren Quantencomputer bauen.

Quantencomputer

Jeder, der über Quantenmechanik nachdenken kann, ohne dass ihm schwindelig wird, hat sie nicht verstanden (Niels Bohr)

- **Quantencomputer** könnte alle bisher genannten Verschlüsselungen entschlüsseln in vernünftiger Zeit
- statt Strom (Spannung da/Spannung nicht da) aus der Makroebene werden z.B. Photonen (Lichtpäckchen) aus der Mikroebene benutzt, die in mehr als nur 2 Zuständen sein können
- heutige Computer können mit 7 Bits EINE Zahl bis 128 darstellen
- eine Quantencomputer kann mit 7 Qubits ALLE 128 Zahlen auf einmal darstellen
- somit kann ein Quantencomputer *gleichzeitig* mehrere Schlüssel ausprobieren, wohingegen ein herkömmlicher Computer nur *nacheinander* Schlüssel ausprobieren kann

Quantencomputer

- **Google** wollte bis Ende 2017 einen Quantencomputer bauen mit 49 Qubits. Das dauert aber offensichtlich länger als gedacht.
- Quantencomputer können Operationen ausführen, die normale Computer nicht ausführen können. Sie brauchen dafür aber neue Algorithmen. Sie können aber nicht Schritte *schneller* ausführen.
- RSA beruht auf einem Problem, das Quantencomputer sofort lösen können durch ein single read-out measurement, all the „unrealized“ branches do not contribute, sie führen aber keine Rechenvorgänge parallel aus.
- Wenn man RSA decrypten möchte, würde man die Schlüssel suchen, nicht die Nachricht entschlüssen.
- Aber irgendwann können sie ganz sicher RSA unsicher machen, es ist nur eine Frage der Zeit.
- Rundreise und andere NP-complete Probleme können Quantencomputer nicht lösen.

Quantenkryptografie - perfekte Geheimhaltung

- B84-Protokoll: Verfahren in der Quantenkryptografie (1984 von Bennett und Brassard)
- Vorgehensweise: Photonen können wie folgt polarisiert sein:
  - / (kann z.B. als binäre 1 interpretiert werden)
  - \ (Interpretierung als 0)
  - -- (Interpretierung als 1)
  - | (Interpretierung als 0)

- dies kann mit Filtern (ähnlich wie Sonnenbrille) gemessen werden: X und +
- Dabei gilt: ein horizontal polarisiertes Photon wird durch ein Filter + *immer* richtig durchgelassen, aber auch mit 50% igen Wahrscheinlichkeit durch ein Filter X und dann immer *zufällig* abgeändert nach Passieren des Filters

Mit Hilfe von Quanten: Schlüsseleinigung von Alice und Bob mit Hilfe von Photonen

1. Alice schickt Bob zufällig polarisierte Photonen mithilfe eines Gerätes.
2. Bob hält zufällig ein Filter hoch/hin (+ oder x) und fängt die Photonen mit einer bestimmten Polarisation auf. Die erhaltene Polarisation schreibt er sich auf.
3. Bob und Alice rufen sich über das öffentliche Telefon an: Bob erzählt Alice (und auch allen Mithörern), welches Filter er jeweils benutzt hat. Alice sagt Bob, wann er immer das falsche Filter benutzt hatte und somit die Polarisation der Photonen verfälscht wurde. Über das Telefon werden also keine Informationen gegeben über echte Werte, wie 0 oder 1.
4. Als Schlüssel für die Kommunikation zwischen Alice und Bob werden nur die Photonen gewählt, die durch das *richtige* Filter gekommen sind, also bei dem Bob zufällig das richtige Filter zum Auffangen benutzt hat.
5. Zur Sicherheit werden die ersten 10 bis 20 Zahlen des Schlüssels zwischen Alice und Bob verglichen und dann verworfen (also ein Lauscher hätte auch davon nichts, weil genau die genannten Zahlen dann NICHT zum Schlüssel gehören werden). Sind die Zahlen gleich, kann man sich sicher sein, dass kein Lauscher den Quantenauffangprozess gestört hat.

Schlüsseleinigung von Alice und Bob: Beispiel – das B84-Protokoll

Von Alice gesendete Polarisation	/	/	\	\	__	__	|	|
Von Bob verwendetes Filter	X	+	X	+	X	+	X	+
Von Bob gemessene Polarisation	/	|	\	__	/	__	\	|
Filter richtig?	ja	nein	ja	nein	nein	ja	nein	ja
Verwendeter Schlüssel	1	.	0	.	.	1	.	0

Quantenkryptografie - Anwendungen

- **Lauschangriff**: Eve ändert unter Umständen bei seiner Messung (zufälliges Reinhalten seines Filters) den von Alice gesendeten Basiszustand (No-Cloning-Theorem), das würde Bob und Alice mindestens beim Vergleich der ersten 10 bis 20 Zahlen ihres Schlüssels auffallen
- **technische Realisierung**: Fehler durch die Messwerte, Rauschen (Doppelbrechung im Glasfaserkanal, Wechselwirkung mit anderen Teilchen)
- **April 2004**: 1. Geldüberweisung mittels Quantenkryptografie (Glasfaserkabel zur Übertragung der verschränkten Photonen war etwa 1.500 m lang und führte von der Bank Austria Creditanstalt durch das Wiener Kanalnetz zum Wiener Rathaus)
- **Oktober 2007**: Übertragung der Wahlergebnisse in der Schweiz mit Hilfe von Quantenkryptografie
- Quantenkryptografiesystem kann man käuflich erwerben, sie sind allerdings teuer und nur für geringe Reichweiten geeignet

Quantenkryptografie: 2017

- Quantum Science Satellite (Projekt mit China und Österreich):
  Schlüsselaustausch über Satelliten und Quantenverschränkung:
  → Photonenpaare haben einen gemeinsamen Quantenzustand egal wie weit sie von einander entfernt sind
  → ändert man den Spin eines Photons, verändert sich der Spin des verschränkten Photons entsprechend
- NIST competition is something that keeps the community busy right now, and on the attack and implementation side, this is very much an ongoing project

Quantencomputer - Bemerkungen

- *Man denkt*, dass nach Quantencomputern nichts mehr kommt.

- Alle denkbaren Computer würden mit den Gesetzen der Physik kollidieren, wie z. B. Zeitreisen oder „Zeit unendlich klein“ (bei 10^{-43} ist Schluss)

- *Man denkt*, Quantencomputer werden nicht alle Problem aus NP lösen können. Alle bis heute bekannten Algorithmen für Quantencomputer nutzen die spezielle Struktur des Problems aus. Für Probleme, wie Rundreise oder Finden von 2 gleichen Elementen in einer Liste, hat man noch nicht einmal den Hauch einer Idee.
- Man kann Quantencomputer kaufen von z.B. QuintessenceLabs und IDQuantique. Sie sind aber sehr groß und sehr langsam und sehr teuer.

Kryptografie: Zusammenfassung

- Kryptografie: *Kunst* der Verschlüsselung
- Techniken: *monologische* und *polyalphabetische* Verschlüsselungen mit *Transposition* und *Substitution*, *asymmetrische* Verschlüsselungen durch Primzahlzerlegung (Einwegfunktionen)
- Verschlüsselungsablauf: Schlüssel, *Algorithmus*, Klartext, Geheimtext
- Enigma ist *Chiffriermaschine*
- Vorhängeschlossidee: jeder kann ein Schloss zuschnappen lassen, aber nur einer kann es öffnen
- *RSA*: asymmetrisches Verschlüsselungsverfahren, das das Faktorisierungsproblem ausnutzt
- *PGP*: kostenloses Programm zur RSA-Verschlüsselung
- Quantenkryptografie ist sicher, nutzt die 50%ige Durchdringung durch nicht passende Filter aus

Literatur:

- Dagmar Pruß: „Quanteninformation“
- Roger Penrose: „Computerdenken“
- Simon Singh: „Geheime Botschaften“
- Jens Gallenbacher: „Abenteuer Informatik“, Spektrum, 2006
- Jörg Schwenk: „Sicherheit und Kryptographie im Internet“ Springer, 2002