UNIKASSEL VERSITÄT

Angewandte Informations Sicherheit

SFN

SchülerKrypto 2017

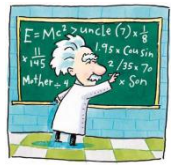
Kryptographie – Die Sprache der Geheimagenten

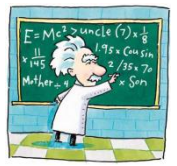
Prof. Arno Wacker
Angewandte Informationssicherheit
Universität Kassel

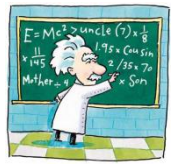
Mit freundlicher Unterstützung von Prof. B. Esslinger, Uni Siegen

Programm

- **Einführung in die Kryptologie – Teil 1 (8:30-10:15)**
  - Einleitung
  - Einfache und verbesserte Verschlüsselung
- **Agenteneinsatz – Teil 1 (10:30-11:30)**
  - Grundausbildung zum Geheimagent
  - Aufträge 1-2
- **Einführung in die Kryptologie – Teil 2 (11:45-13:00)**
  - Maschinelle Verschlüsselung
  - Moderne Verschlüsselung (Teil 1/2)
- **Mittagessen**
- **Einführung in die Kryptologie – Teil 3 (13:30-14:30)**
  - Moderne Verschlüsselung (Teil 2/2)
- **Agenteneinsatz – Teil 2 (14:45-16:15)**
  - Agentenfortbildung
  - Aufträge 3-4







Literatur (1/2)

- **Codeknacker gegen Codemacher**
  Klaus Schmeh
- **Geheime Botschaften**
  Simon Singh
- **Entzifferte Geheimnisse**
  Friedrich L. Bauer
- **Versteckte Botschaften**
  Klaus Schmeh

Literatur (2/2)

- **Kryptografie**
  Klaus Schmeh
- **Angewandte Kryptographie**
  Bruce Schneier
- **Applied Cryptanalysis**
  M. Stamp, R. Low
- **Modern Cryptanalysis**
  Christopher Swenson

Online Ressourcen

- **CrypTool 1.4.40** (Release)
  http://www.cryptool.org/cryptool1
- **CrypTool 2.1** (Stable / Nightly builds)
  http://www.cryptool.org/cryptool2
- **Schülerkrypto** Webseite
  http://www.cryptool.org/schuelerkrypto/
- **MysteryTwister C3**
  http://www.mysterytwisterc3.org

Übersicht

- Einleitung
- Einfache Verschlüsselung
- Verbesserte Verschlüsselung
- Maschinelle Verschlüsselung
- Moderne Verschlüsselung
- Zusammenfassung

Einleitung

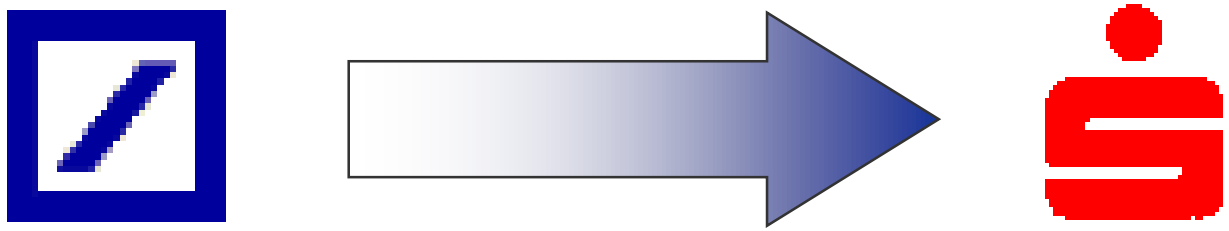
Schülerkrypto 2017

Kryptographie im Alltag

- Euroscheckkarten, Geldautomaten

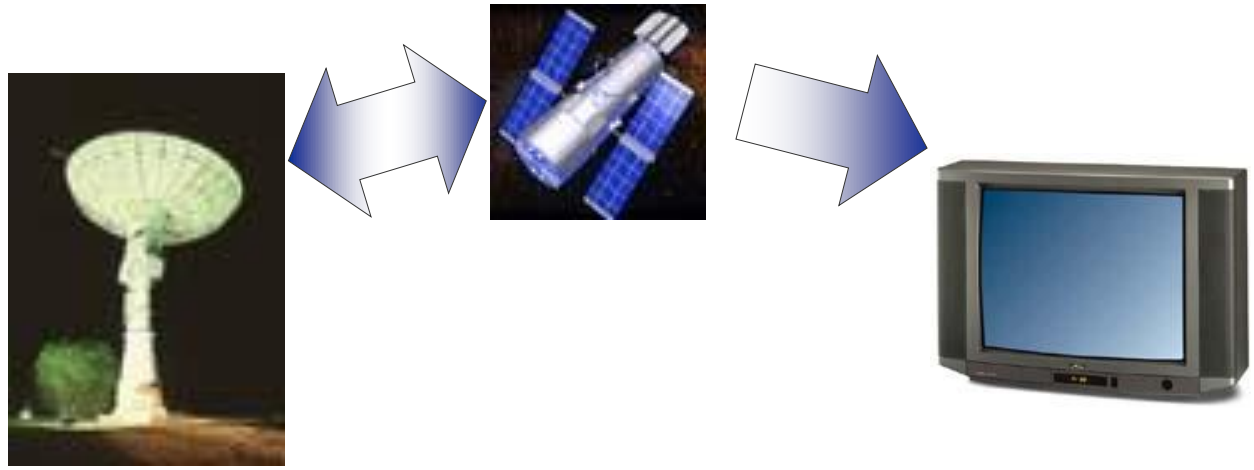
Kryptographie im Einsatz

- Euroscheckkarten, Geldautomaten
- Geldverkehr zwischen Banken



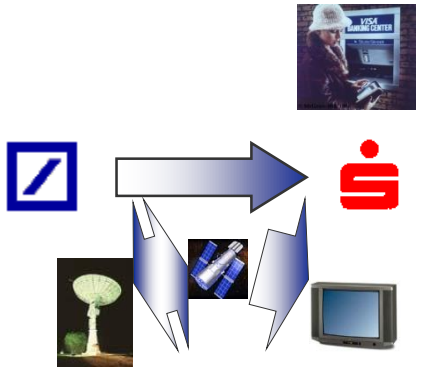
Kryptographie im Einsatz

- Euroscheckkarten, Geldautomaten
- Geldverkehr zwischen Banken
- Satellitenfernsehen, PayTV



Kryptographie im Einsatz

- Euroscheckkarten, Geldautomaten
- Geldverkehr zwischen Banken
- Satellitenfernsehen, PayTV
- Telefon, Handy



Kryptographie im Einsatz

- Euroscheckkarten, Geldautomaten
- Geldverkehr zwischen Banken
- Satellitenfernsehen, PayTV
- Telefon, Handy
- Einkauf im Internet

amazon.com

GALERIA KAUFHOF

neckermann versand

OTTO

Kryptographie im Einsatz

- Euroscheckkarten, Geldautomaten
- Geldverkehr zwischen Banken
- Satellitenfernsehen, PayTV
- Telefon, Handy
- Einkauf im Internet
- und vieles mehr ...

napster ?!

Emailsicherheit

Geheime Botschaften

Steganologie

- Steganographie
- Steganalyse

Kryptologie

- Kryptographie
- Kryptoanalyse

Steganologie

- **Steganographie**
  - Wissenschaft der verborgenen Übermittlung
  - Altgriechisch
    - **Στεγανός, steganos** = *bedeckt, versteckt*
    - **γράφειν , gráphein** = *schreiben*
  - Daten werden in unverdächtigem „Träger“ versteckt
  - Träger: Bilder, Texte, Ton- und Videodokumente
- **Steganalyse**
  - Analyse von steganographischen Verfahren
  - Ziel
    - Extraktion der Daten
    - Existenznachweis der Daten

Steganographie – Beispiele

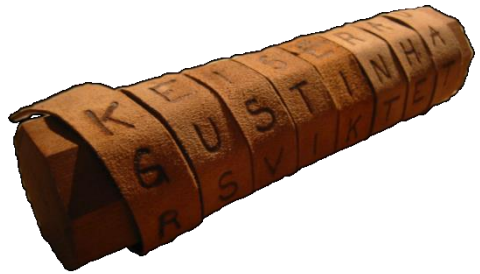
- **Antikes Griechenland: Tätowierung**
  - Nachrichten auf den Kopf tätowieren
  - Haare wachsen lassen/Helm aufsetzen
- **Unsichtbare Tinte**
  - Z. B. Essig oder Zitronensaft
  - Sichtbar durch Erwärmen
- **Steganos Security Suite**
  - Bettet Daten in Bilder- und Audio-Dateien ein
- **Unsichtbare Digitale Wasserzeichen**
  - Urheberschutz
  - Integritätsprüfung

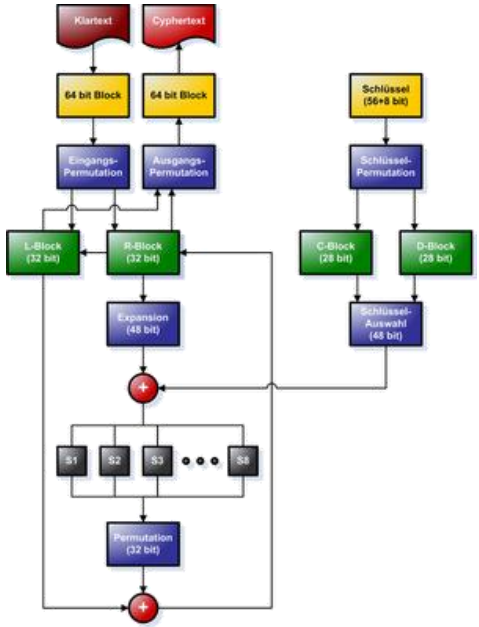
Kryptologie

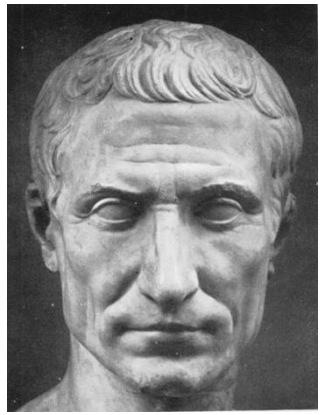
- **Kryptographie**
  - Wissenschaft der Verschlüsselung von Informationen
  - Griechisch
    - **κρυπτός, kryptós** = *verborgen, geheim*
    - **γράφειν, gráphein** = *schreiben*
  - Nur autorisierte Person kann Nachricht lesen
  - Ziele
    - Vertraulichkeit, Integrität, Authentizität, Verbindlichkeit
- **Kryptoanalyse**
  - Gewinnung von Informationen aus verschlüsselten Texten
  - Analyse von kryptographischen Verfahren
    - Brechen
    - Sicherheit nachweisen, quantifizieren

Kryptographie – Beispiele

- **Einfach**
  - Skytale
  - Caesar
- **Mechanisch**
  - Enigma
  - SIGABA
- **Modern**
  - DES, AES
  - RSA

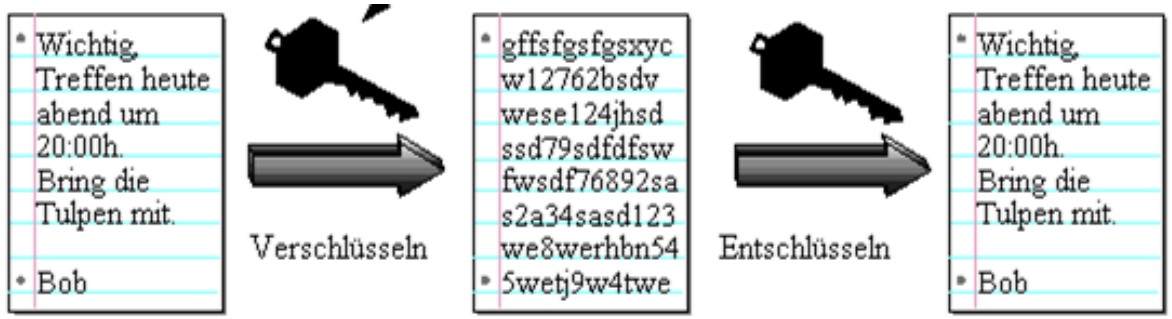




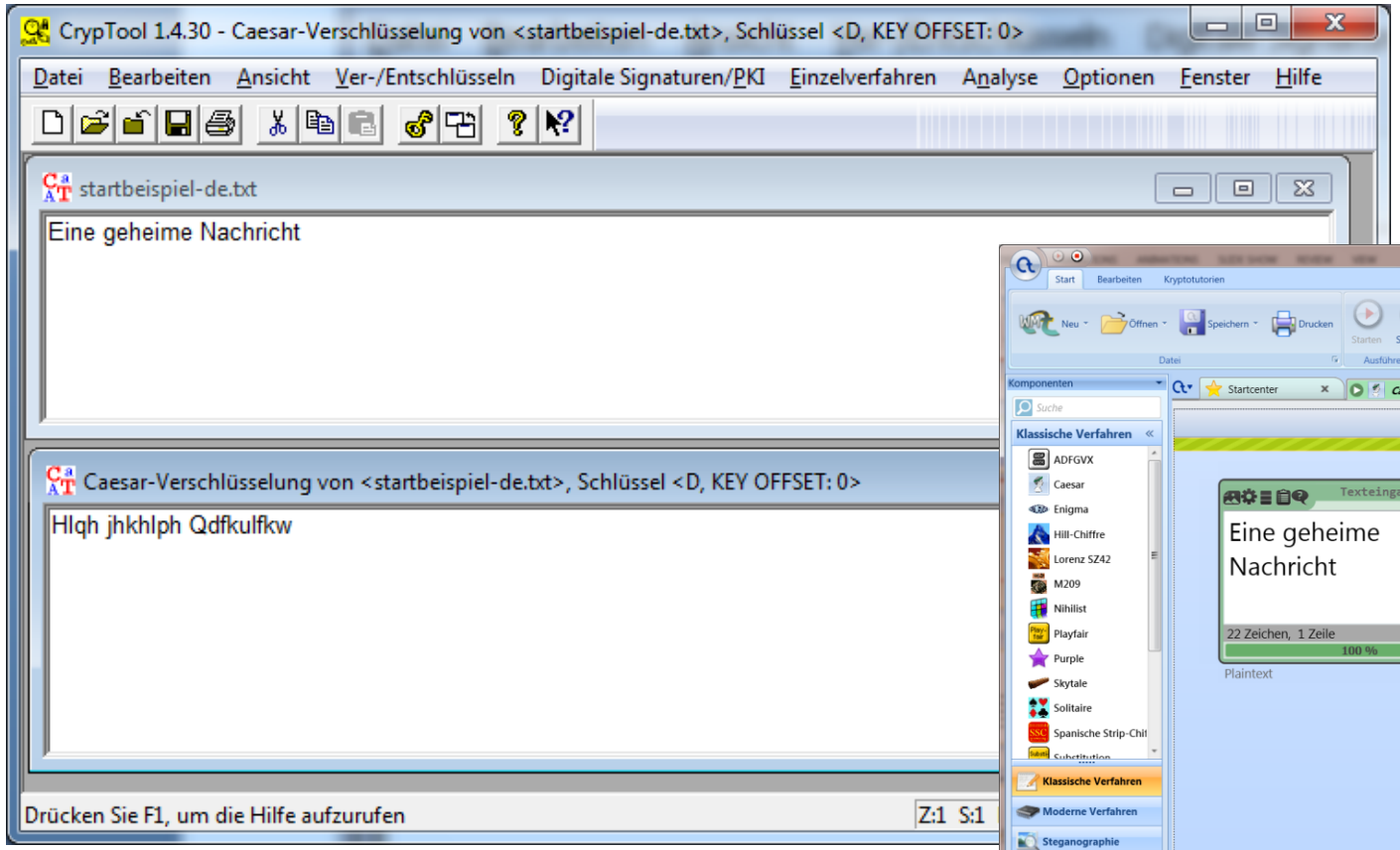


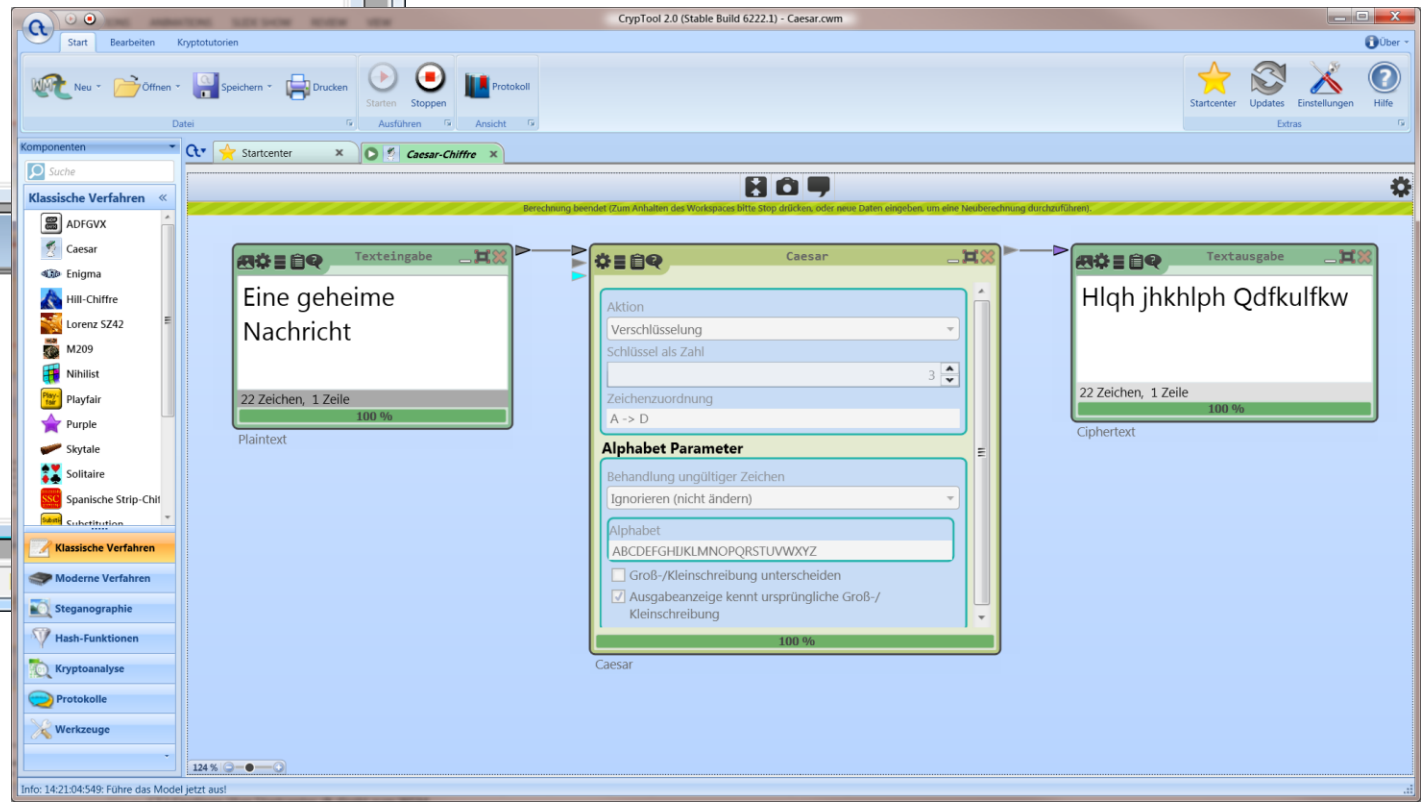
Verschlüsselung allgemein

- **Klartext mit einem Schlüssel verschlüsseln**
  - Wie = Verschlüsselungsverfahren
  - Schlüssel = Geheimnis
- **Verschlüsselte Nachricht (Geheimtext, Chiffrat) übermitteln**
  - Funk
  - Internet
  - Zettel …
- **Chiffrat mit Schlüssel entschlüsseln**
  - Gleiches Verschlüsselungsverfahren wie beim Verschlüsseln
  - Meist auch gleicher Schlüssel



Demo: CrypTool 1.4.40 & CrypTool 2.1





UNIKASSEL VERSITÄT

Angewandte Informations Sicherheit

SFN

Einfache Verschlüsselung

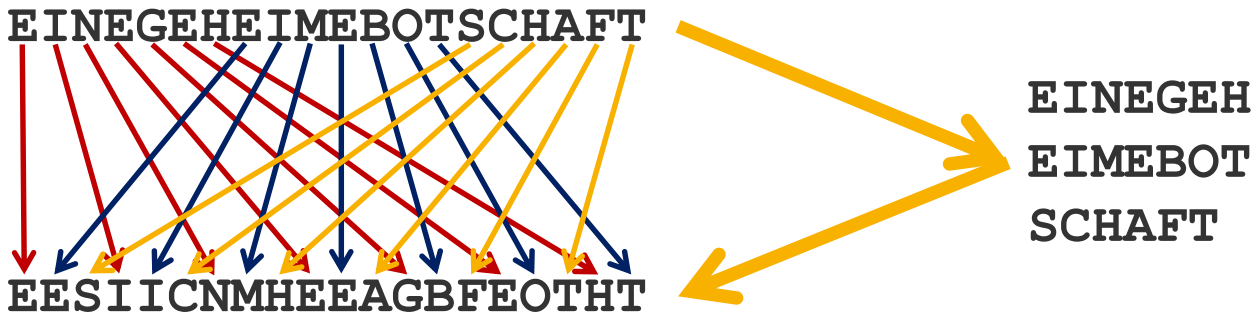
Schülerkrypto 2017

Die spartanische Skytale

- **Ca. 400 v. Chr.**
- **Einsatz für militärische Zwecke**
- **Funktionsweise**
  - Stab aus Holz mit bestimmtem Radius
  - Pergament (Papier, Leder) wird auf den Stab gewickelt
  - Nachricht wird nun auf das Pergament auf dem Stab geschrieben
  - Pergament wird abgewickelt und dem Kurier gegeben
  - Ohne den Stab machen die Buchstaben auf dem Streifen keinen Sinn
  - Der Empfänger wickelt den überbrachten Pergamentstreifen auf seinen Stab aus Holz

Die Skytale – Kryptographischer Hintergrund

- Klasse der **Transpositionsverfahren**
- Alle Buchstaben bleiben gleich
- Die Position der Buchstaben ändert sich

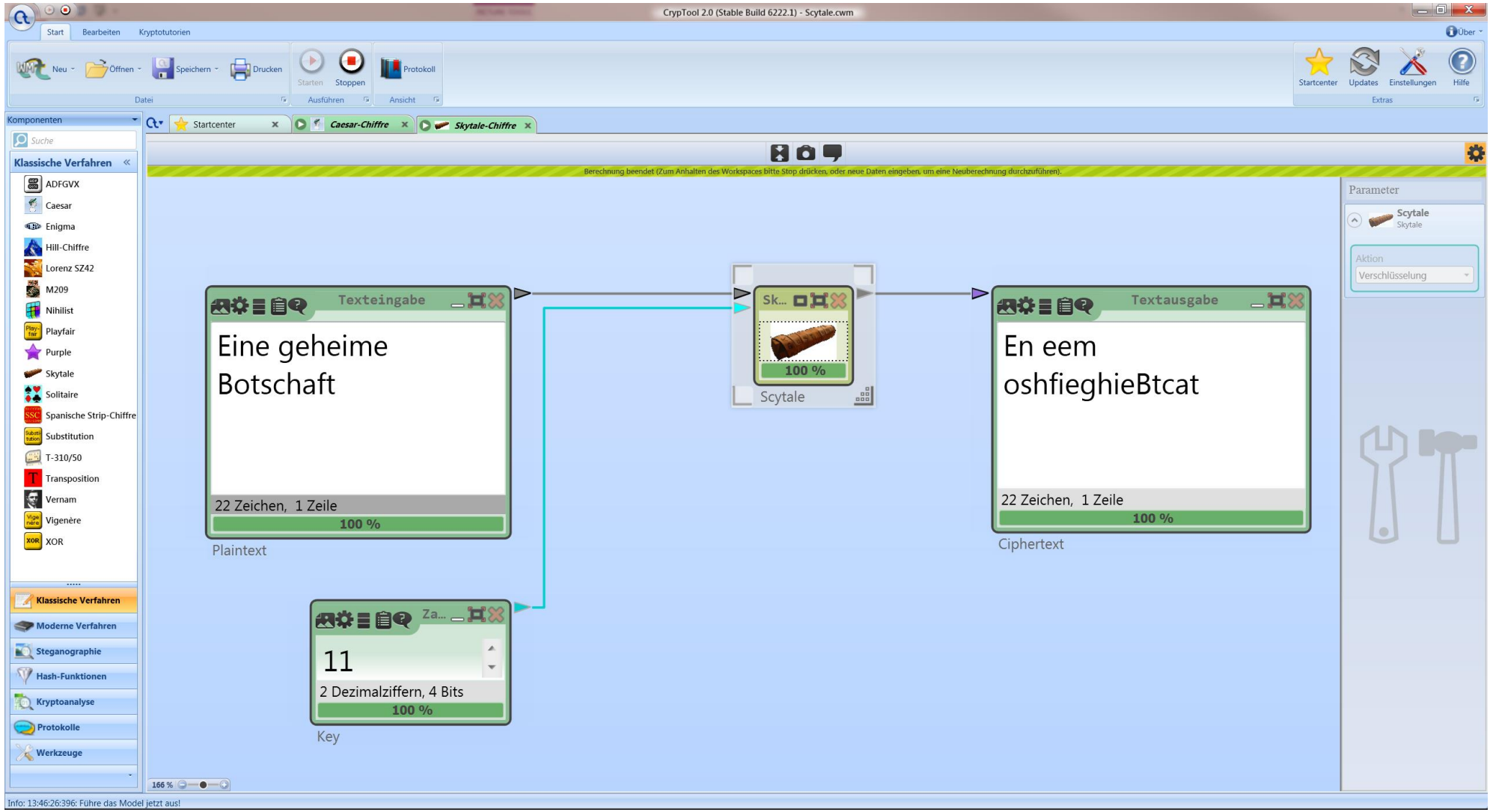


- Mathematiker sprechen von einer „**Permutation des Textes**“

Die Skytale – Kryptoanalyse

- **Länge des Textes: n Zeichen**
- **Maximaler Radius**
  - n Zeichen passen auf Umfang (=2πR)
  - $R_{max} = n/2\pi$
- **Angriffsansatz:**
  - Alle Radien x/2π mit x=1…n probieren (also linear)
  - Textuell: Umbrüche nach 1…n Zeichen
- **Kann von Hand in Minuten gebrochen werden**
- **Unbrauchbar, sobald Verfahren bekannt ist**

Demo: Skytale mit CrypTool 2.1



Hands-On: Skytale – Rätsel

Empfangene Nachricht:

```
G R  |E E  |N N E V O  |A O R  |H N D  |
```

2 Spalten:

```
GR
_E
E_
NN
FV
O_
AO
R_
HN
D_
```

3 Spalten:

```
GR_
EE_
NNF
VO_
AOR
_HN
D_
```

4 Spalten

```
GR_E
E_NN
FVO_
AOR_
HND_
```

Entschlüsselte Nachricht: `GEFAHR_VON_NORDEN`

Die Caesar-Verschlüsselung

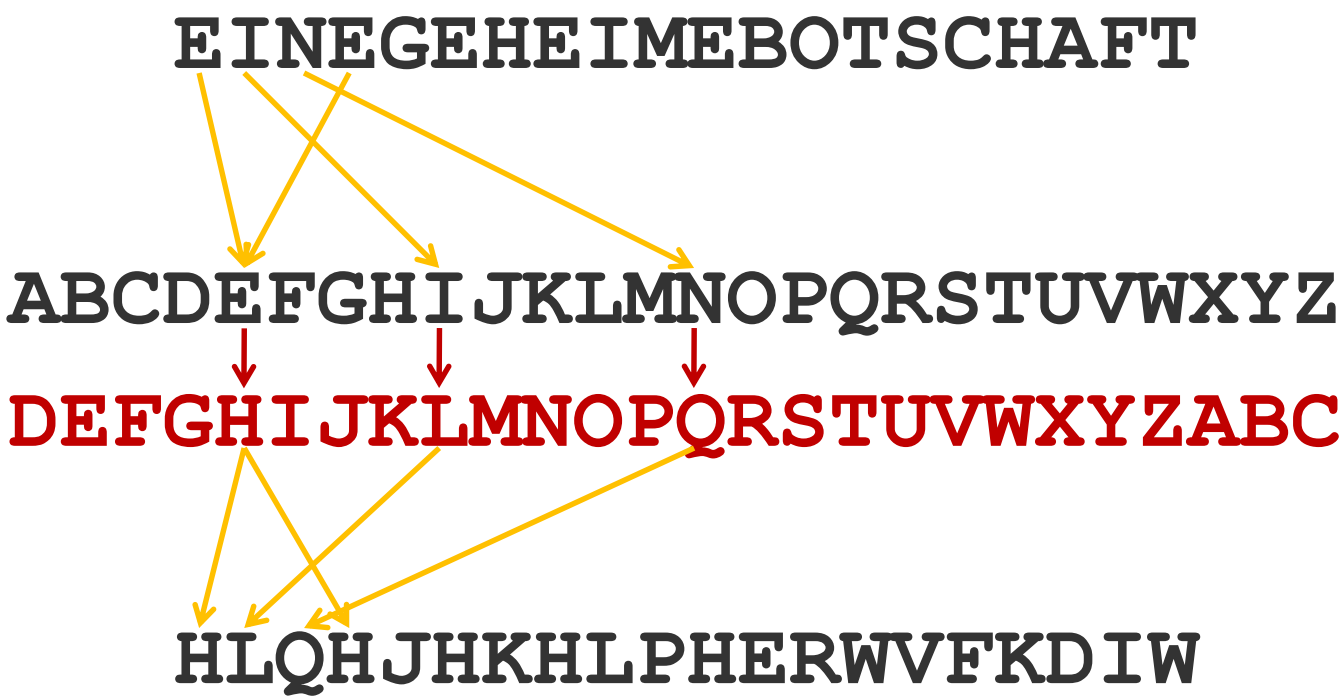
- **Eingesetzt von**
  - Julius Caesar (100 – 44 v.Chr.)
  - Augustus Caesar (63 v.Chr. – 14 n.Chr.)
- **Militärische Zwecke**
- **Funktionsweise**
  - Ersetzung der Buchstaben im Alphabet
    - z.B. anstelle von A schreibt man D, anstelle von B wird E geschrieben usw.
  - Empfänger kennt diese Ersetzung und kann sie rückgängig machen
  - Abgefangene Nachrichten machen keinen Sinn

Caesar – Kryptographischer Hintergrund

- Klasse der **Substitutionsverfahren**
- Ein Zeichen wird durch ein anderes ausgetauscht
- Position der Zeichen ändert sich nicht
- Mathematiker sprechen von einer „**Permutation des Alphabets**“
  - Bei Caesar: Verschiebung (um 3)

Caesar – Beispiel

- **Nachricht: „EINEGEHEIMEBOTSCHAFT“**
- **Schlüssel: 3 (Verschiebung im Alphabet)**



Caesar – Chiffrierscheiben

ABCDEFGHIJKLMNOPQRSTUVWXYZ

DEFGHIJKLMNOPQRSTUVWXYZABC

Verschlüsseln ↓

↑ Entschlüsseln

Giovanni Batista Porta (1563)
De Furtivis Literarum Notis

Caesar – Kryptoanalyse (1/3)

- **Einfachster Angriff**
  - Nur 26 verschiedene Schlüssel (Verschiebungen)
  - Alle probieren (brute force)
- **Statistischer Angriff**
  - Buchstaben einer Sprache haben bestimmte Häufigkeiten
  - Häufigkeiten der Buchstaben im Chiffretext berechnen
  - Buchstabenhäufigkeiten der Sprache mit der der Chiffre vergleichen

Caesar – Kryptoanalyse (2/3)

Statistische Häufigkeitsanalyse

- **Häufigkeitsverteilung von Buchstaben einer Sprache**
- **Kann für jede Sprache berechnet werden**
  - Z. B. ein Buch
  - Allg. „Textkorpus“

Letter	%	Letter	%
A	6.51	N	9.78
B	1.89	O	2.51
C	3.06	P	0.79
D	5.08	Q	0.02
E	17.40	R	7.00
F	1.66	S	7.27
G	3.01	T	6.15
H	4.76	U	4.35
I	7.55	V	0.67
J	0.27	W	1.89
K	1.21	X	0.03
L	3.44	Y	0.04
M	2.53	Z	1.13

Häufigkeitsverteilung der deutschen Sprache

Caesar – Kryptoanalyse (3/3)

Statistische Häufigkeitsanalyse - Beispiel

- **Empfangene Nachricht:**

  „MQOOGP UKG BWT UEJWGNGTMTARVQ!“

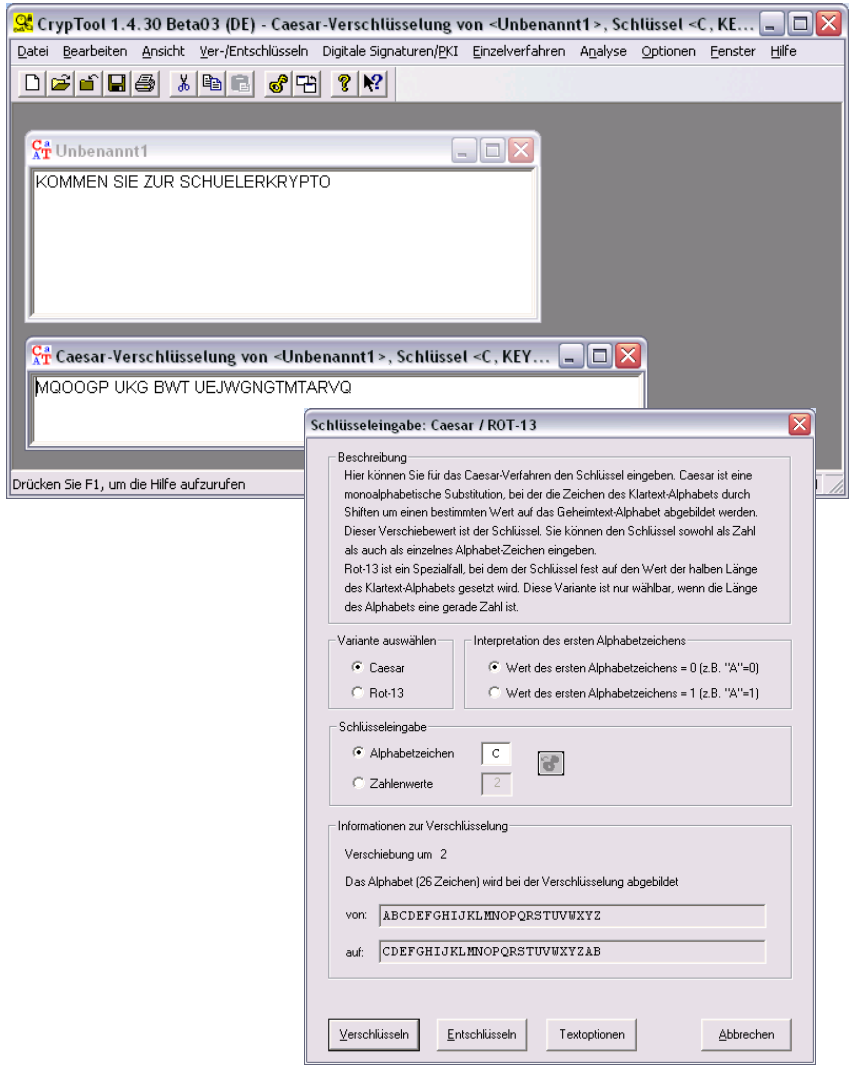
- **Bestimmung der Buchstabenhäufigkeiten**

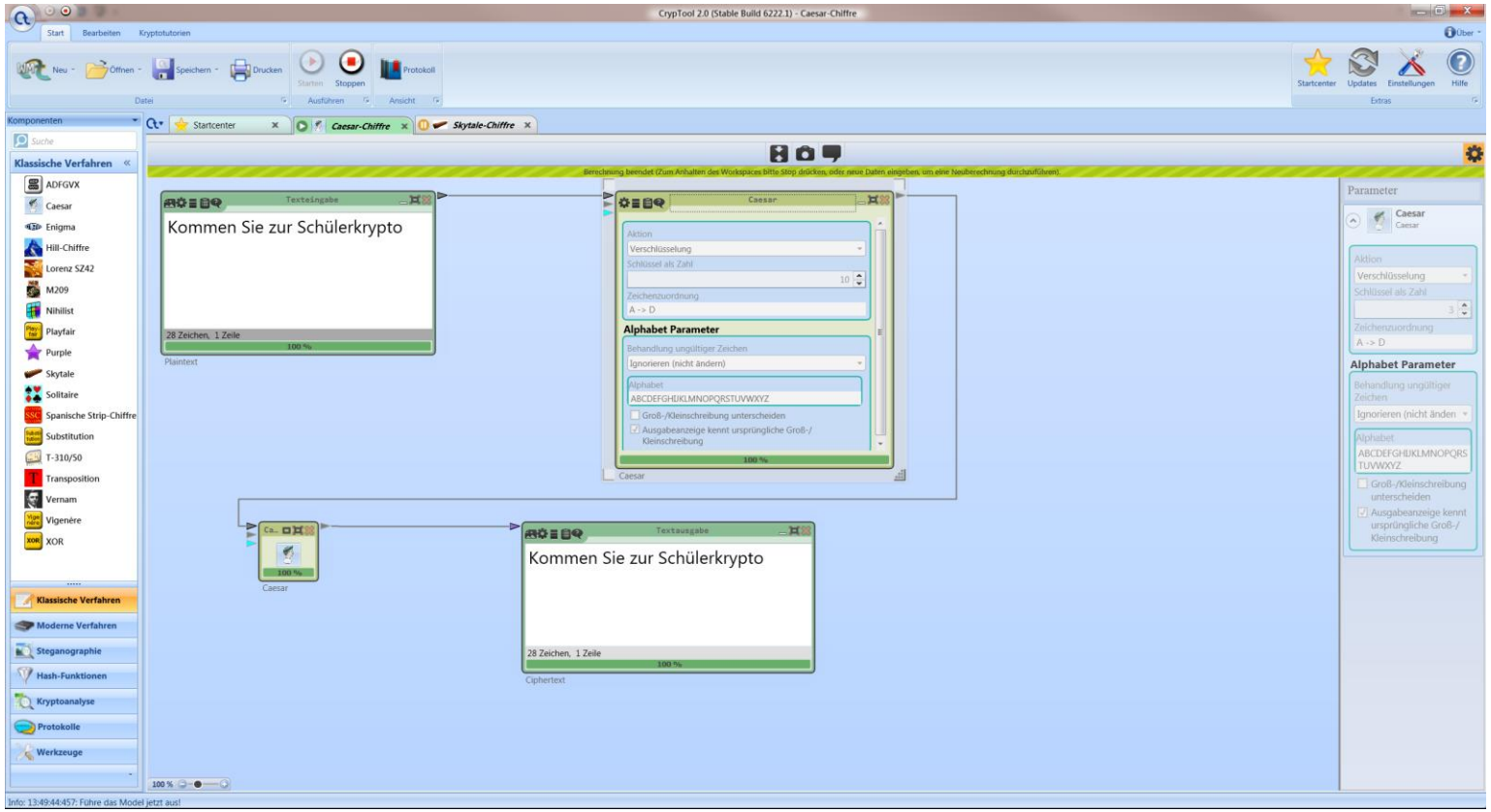
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	1	0	0	1	0	4	0	0	1	1	0	2	1	2	1	2	1	0	3	2	1	2	0	0	0

- **Kryptoanalyse**
  - Annahme: G ↔ E
  - Damit handelt es sich um eine Verschiebung von 2
- **Ergebnis:**

  „KOMMEN SIE ZUR SCHUELERKRYPTO!“

Demo: Caesar mit CrypTool 1.4.40 und 2.1





Hands-On: Caesar – Rätsel

GLH JDOOLHU NRPPHQ!

Caesar – Rätsel: Kryptoanalyse (Variante 1)

- **Bestimmung der Buchstabenhäufigkeiten**

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
0	0	0	1	0	0	1	3	0	1	0	2	0	1	2	2	1	1	0	0	1	0	0	0	0	0

- **Kryptoanalyse von „GLH JDOOLHU NRPPHQ“**
  - Annahme: H = E
  - Also Verschiebung um 3:

DEFGHIJKLMNOPQRSTUVWXYZABC
ABCDEFGHIJKLMNOPQRSTUVWXYZ

- **Ergebnis:**
  „DIE GALLIER KOMMEN!“

Caesar – Rätsel: Kryptoanalyse (Variante 2)

C H D F Z K K H D Q J N L L D M

D I E G A L L I E R K O M M E N !

E J F H B M M J F S L P N N F O

F K G I C N N K G T M Q O O G P

GLH JDOOLHU NRPPHQ!

H M I K E P P M I V O S Q Q I R

I N J L F Q Q N J W P T R R J S

J O K M G R R O K X Q U S S K T

K P L N H S S P L Y R V T T L u

„Running down the alphabet…“

UNIKASSEL VERSITÄT

Angewandte Informations Sicherheit

SFN

Verbesserte Verschlüsselung

Schülerkrypto 2017

Einfache Spaltentransposition

- **Klartext wird in Zeilen fixer Länge geschrieben**
  - Alle Zeilen genau gefüllt → regelmäßige Spaltentransposition
  - Letzte Zeile unvollständig → unregelmäßige Spaltentransposition
- **Spaltenreihenfolge wird verändert (permutiert)**
  - Verwendung eines Schlüsselwortes
  - Lange Schlüsselwörter erhöhen die Sicherheit
- **Spaltenweise auslesen**

Einfache Spaltentransposition – Beispiel (1)

- Klartext: „WE ARE DISCOVERED. FLEE AT ONCE.“
- Schlüssel: ZEBRAS (→ 6 3 2 4 1 5)

ZEBRAS	EVLN
632415	ACDT
WEARED	ESEA
ISCOVE	ROFO
REDFLE	DEEC
EATONC	WIRE
E	E

EVLNA CDTES
EAROF ODEEC
WIREE

Einfache Spaltentransposition – Beispiel (2)

- **Chiffretext: EVLNA CDTES EAROF ODEEC WIREE**
- **Schlüssel: ZEBRAS, also 6 3 2 4 1 5**
- **Vorbereitung (unregelmäßig)**
  - Insgesamt 25 Zeichen in 6 Spalten
    - 5 Spalten mit 4 Zeichen
    - 1 Spalte mit 5 Zeichen

Z	E	B	R	A	S
6	3	2	4	1	5
W	E	A	R	E	D
I	S	C	O	V	E
R	E	D	F	L	E
E	A	T	O	N	C
E					

Spaltentransposition – Kryptoanalyse (1/3)

- **Länge des Schlüssels**
  - Extremfall: Länge des Schlüssel = Länge des Textes
  - In diesem Extremfall n(n-1)(n-2) … 2 = n! Möglichkeiten (Permutationen)
  - Längen > 20 sind schwierig (ohne Klartextkenntnis)
- **Kryptoanalyse besteht aus zwei Schritten**
  - 1. Schüssellänge bestimmen
  - 2. Spaltenpermutation rückgängig machen

Spaltentransposition – Kryptoanalyse (2/3)

Bestimmung der Schlüssellänge

- **Schlüssellänge bestimmen**
  - Ohne Klartextkenntnis
    - Alle probieren von 1 ... n (n= Länge des Textes)
    - Vokale zählen und mit Statistik der Sprache vergleichen
    - Für jede Länge Anagramme suchen
  - (Teil-)Kenntnis des Klartextes
    - Suchen nach Textmuster für alle Längen
    - Wenn Muster gefunden, dann Schlüssellänge möglich
    - Wenn Muster nicht vorhanden, dann Schlüssellänge falsch
- **Beispiel**
  - Annahme wir erwarten **DISCOVERED** im verschlüsselten Text.
  - Chiffretext: EVLNA CDTES EAROF ODEEC WIREE
  - Suche nach
    - Schlüssellänge 2: DSOEE und ICVRD → nicht vorhanden
    - Schlüssellänge 3: DCED , IOR und SVE → nicht vorhanden
    - Schlüssellänge 4: DOE, IVD, SED, CR → nicht vorhanden
    - Schlüssellänge 5: DV, IE, SR, CE, OD → nicht vorhanden
    - Schlüssellänge 6: DE, IR, SE, CD → wahrscheinliche Länge!

Spaltentransposition – Kryptoanalyse (3/3)

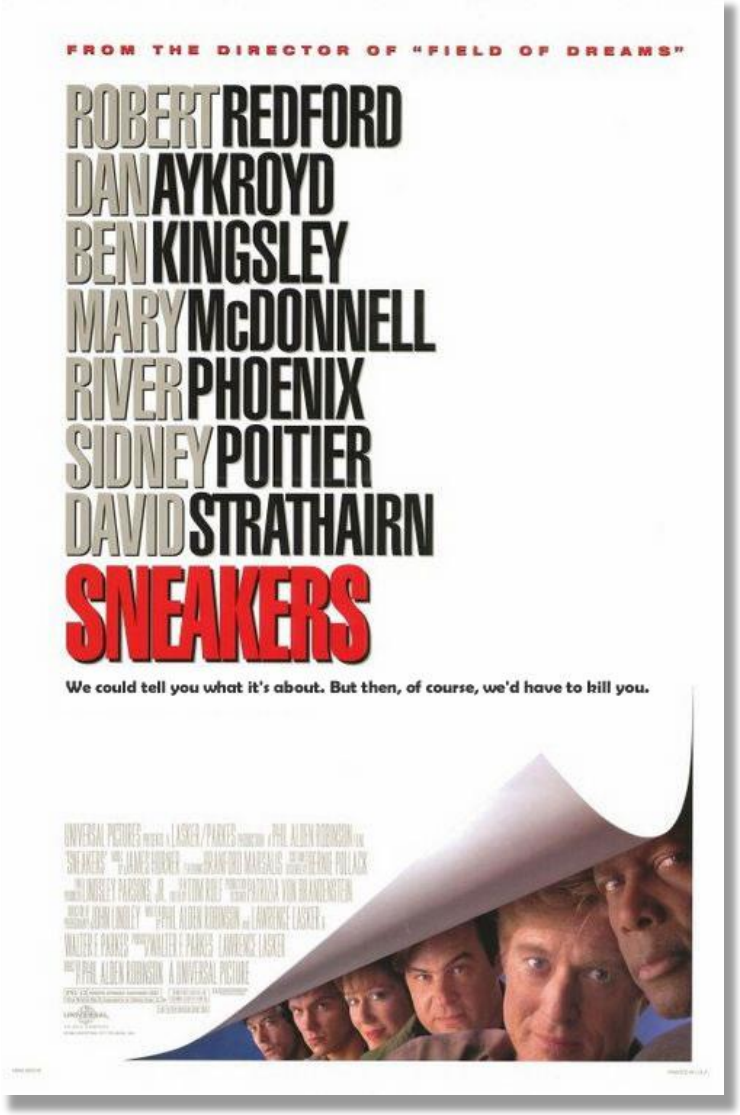
Bestimmung der Spaltenpermutation

- **Kenntnis der Schlüssellänge führt zu**
  - 5 Spalten mit 4 Zeichen
  - 1 Spalte mit 5 Zeichen

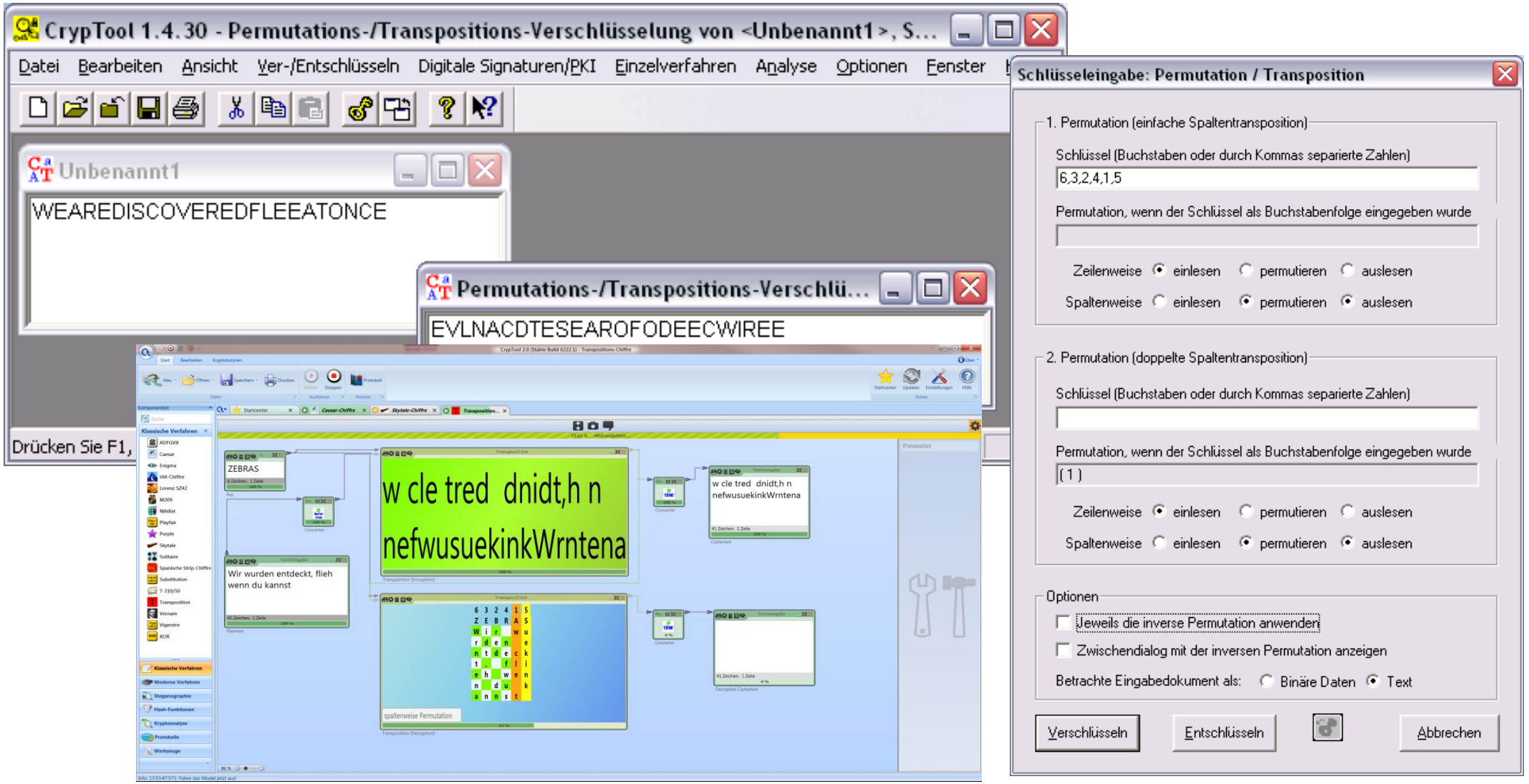
- **Text nach jeweils 4 Zeichen trennen (letzte 5)**
- **Umordnen, um DISCOVERED zu bilden (Anagramm suchen)**

Anagramme

- A TURNIP CURES ELVIS
- A FEW ASTRAL CLERKS
- REPEL NEWARK
- BLOND RHINO SPANIEL
- FORT RED BORDER
- SETEC ASTRONOMY



Demo: Spaltentransp. mit CrypTool 1.4.40 / 2.1



Monoalphabetische Substitution

- **Definition:**
  Ein Klartextbuchstabe wird immer gleich ersetzt

- **Beispiele:**
  - Caesar (Verschiebung)
  - Allgemeine Permutation des Alphabets, z. B.
    - Schlüssel = {Wort: GEHEIMSCHRIFT; Startposition: E}
    - Doppelte Buchstaben entfernen: GEHIMSCRFT
    - Permutation des Alphabets wie folgt erstellen:

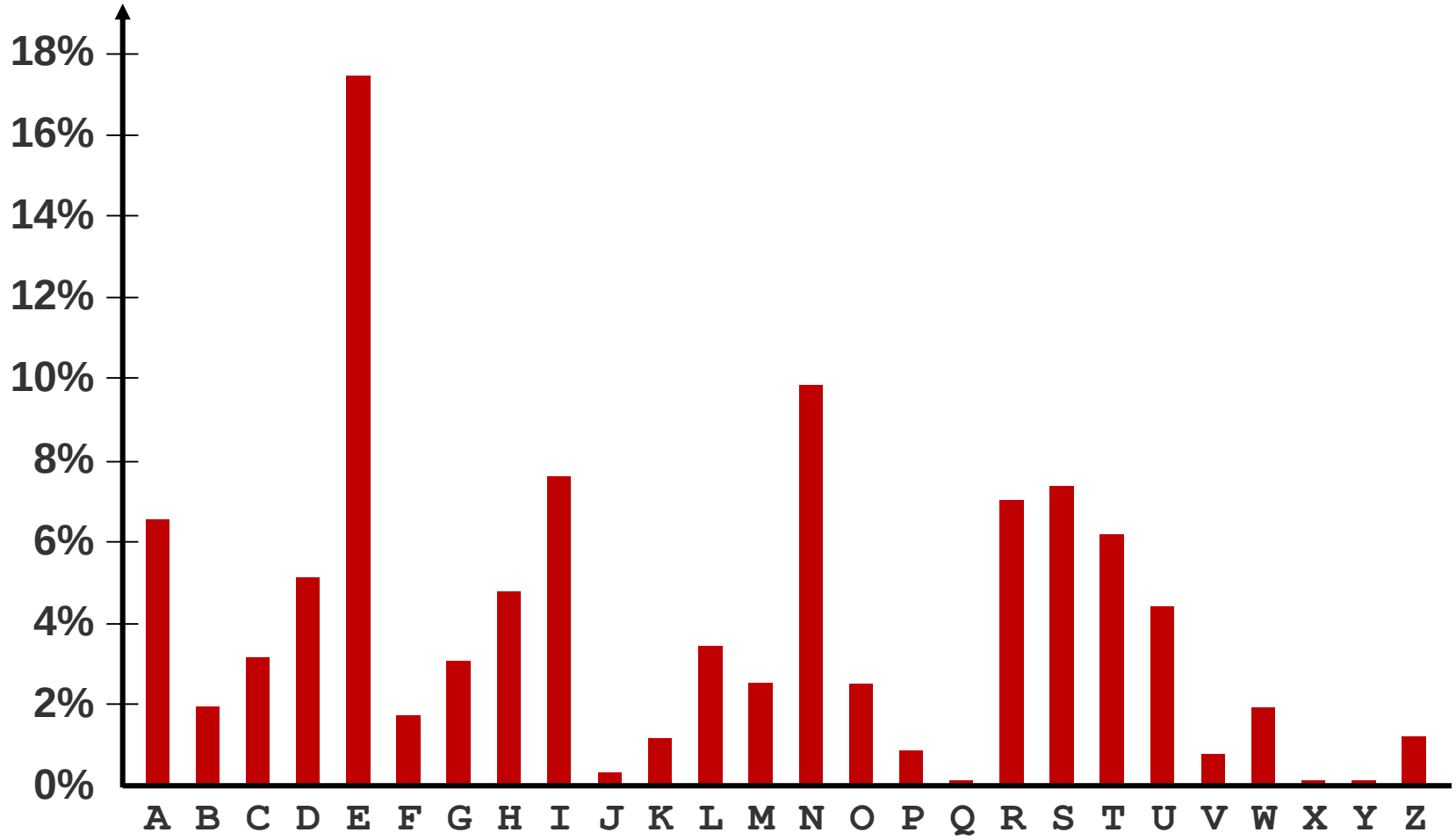
a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
W	X	Y	Z	G	E	H	I	M	S	C	R	F	T	A	B	D	J	K	L	N	O	P	Q	U	V

Substitution – Kryptoanalyse (1/2)

- **Es gibt 26·25·24· .. 2·1 = 26! ~ 2^{88} Permutationen**
  - Zu viele, um alle zu probieren (selbst heute!)
- **Annahme: Wir kennen *nur* den verschlüsselten Text (schwierigster Fall für den Kryptoanalytiker)**
- **Idee:**
  - Die 10 häufigsten Buchstaben im Deutschen bilden ca. 75% des gesamten Textes
  - Berechne/analysiere die 10 häufigsten Buchstaben
  - Rate den Rest
- **Beispiel**
  - Die –ehn haeu-i-sten –u-hsta-en i- deuts-hen –i-den drei –ierte- des –esa-tte-tes

Substitution – Kryptoanalyse (2/2)

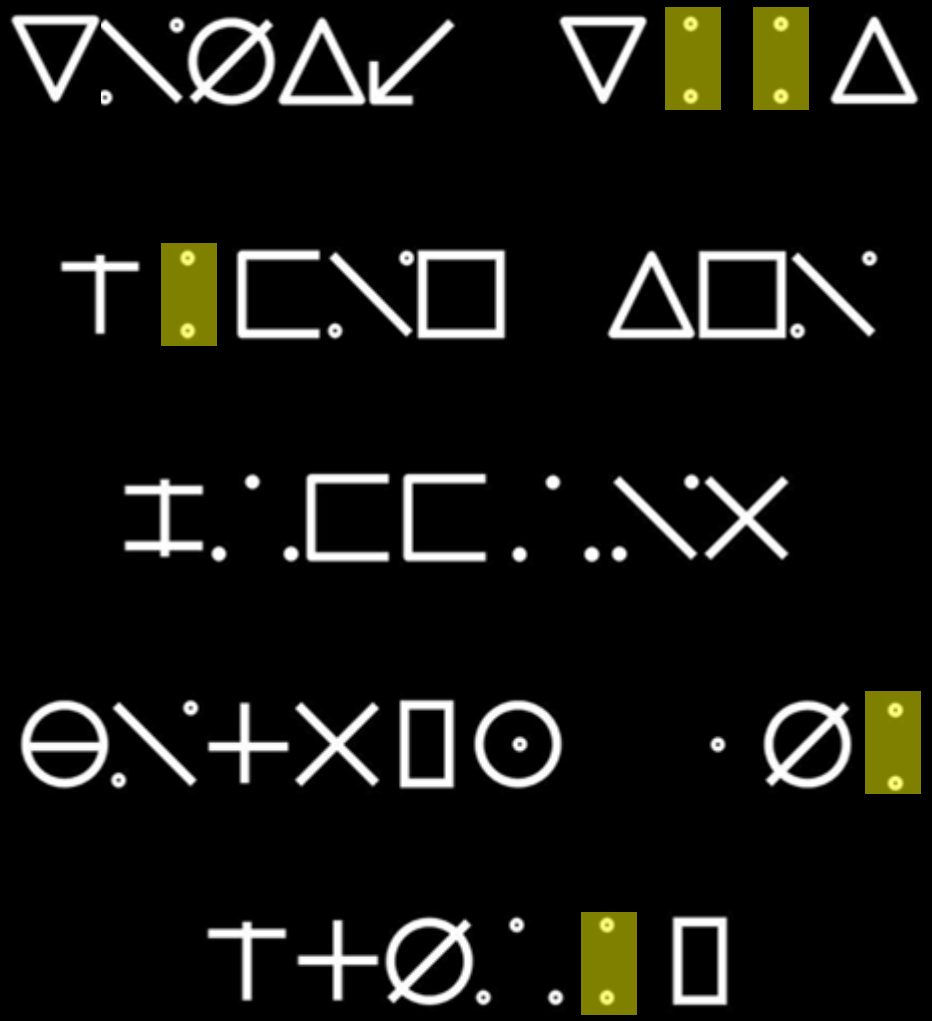
Häufigkeitsverteilung der Buchstaben



Substitution – Beispiel

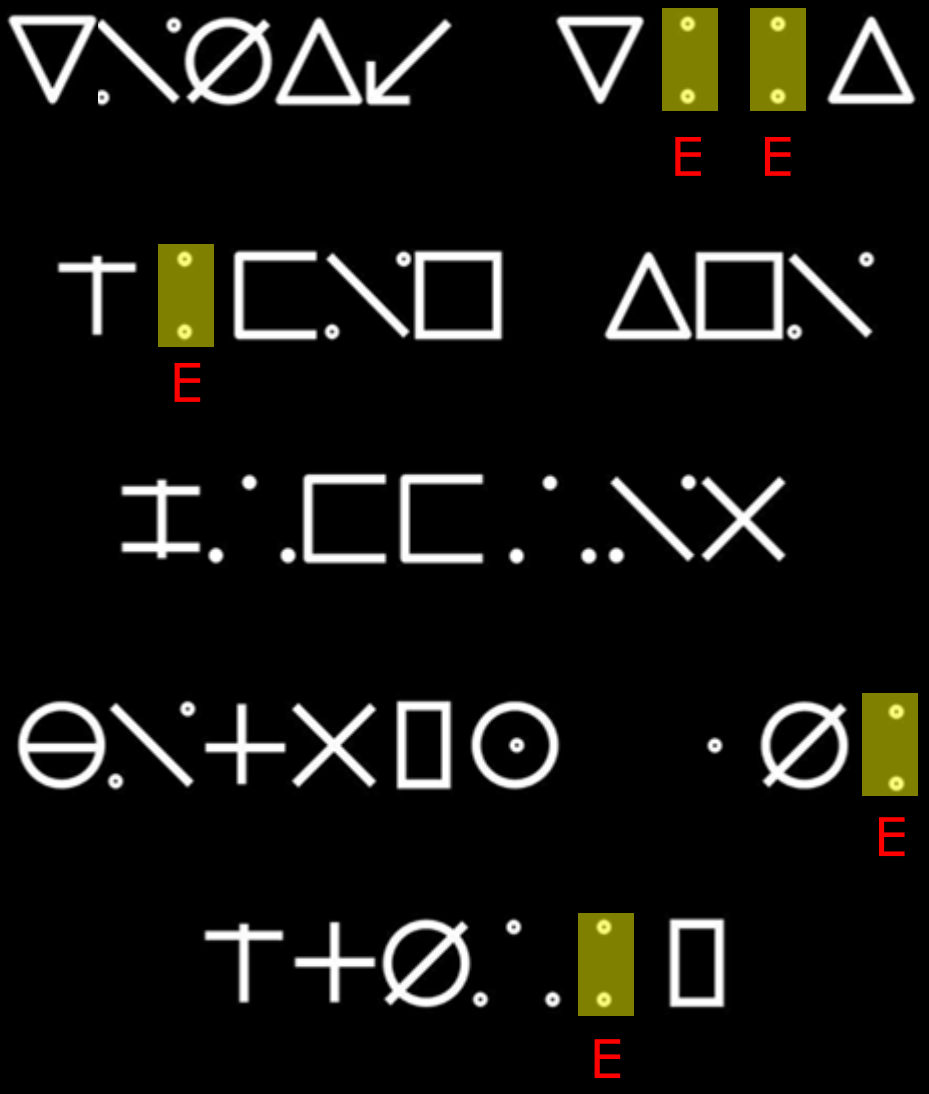
Mit freundlicher Genehmigung
von Klaus Schmeh

Substitution – Beispiel



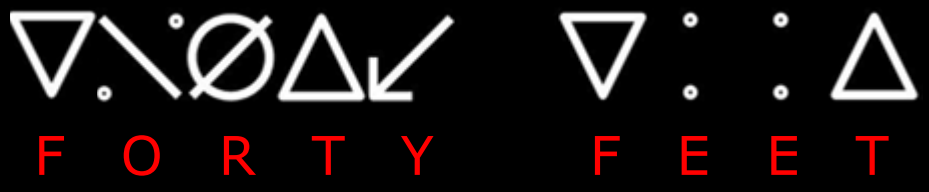
Mit freundlicher Genehmigung
von Klaus Schmeh

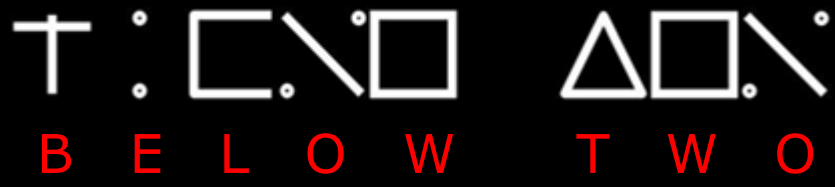
Substitution – Beispiel



Mit freundlicher Genehmigung
von Klaus Schmeh

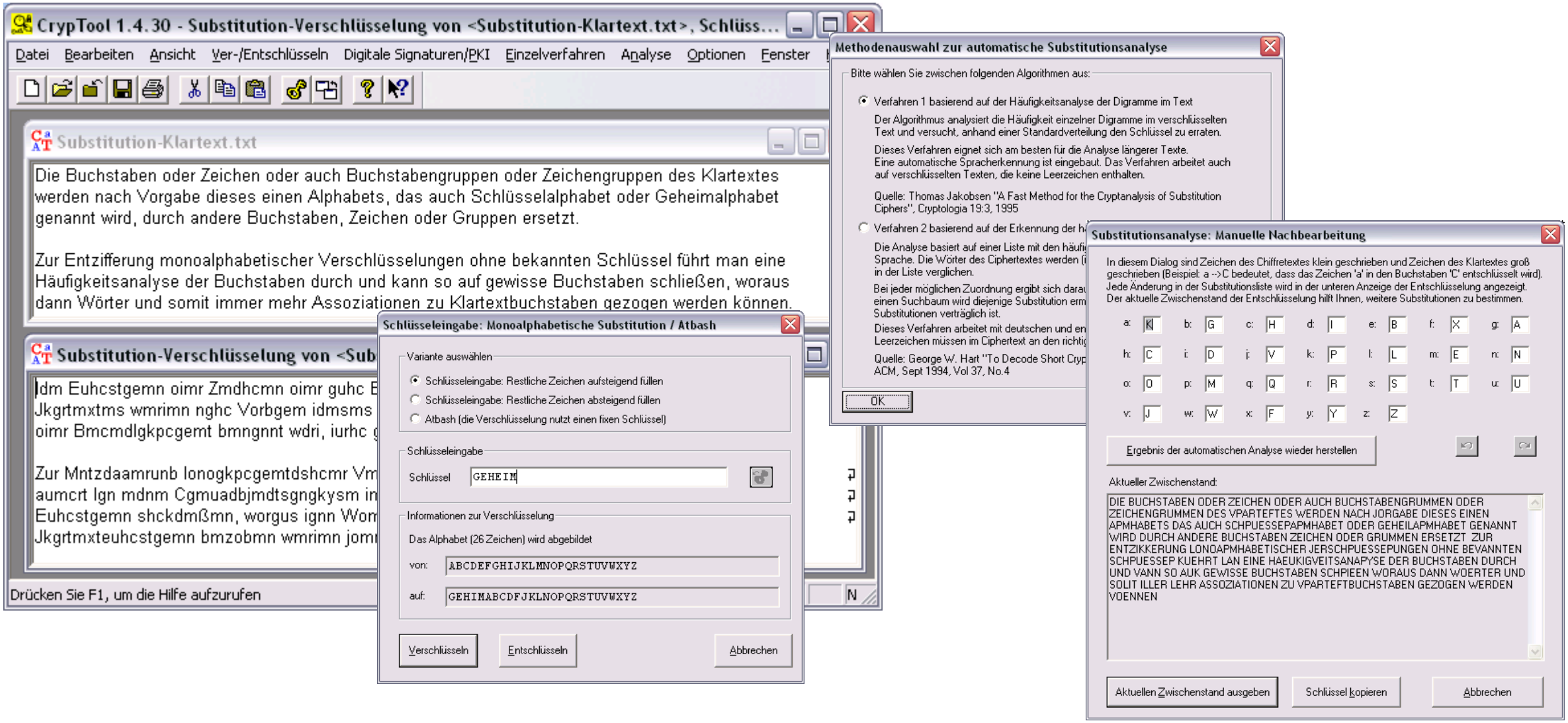
Substitution – Beispiel





Mit freundlicher Genehmigung
von Klaus Schmeh

Demo: Substitution mit CrypTool 1.4



UNIKASSEL VERSITÄT

Angewandte Informations Sicherheit

SFN

Maschinelle Verschlüsselung

Schülerkrypto 2017

Die Enigma

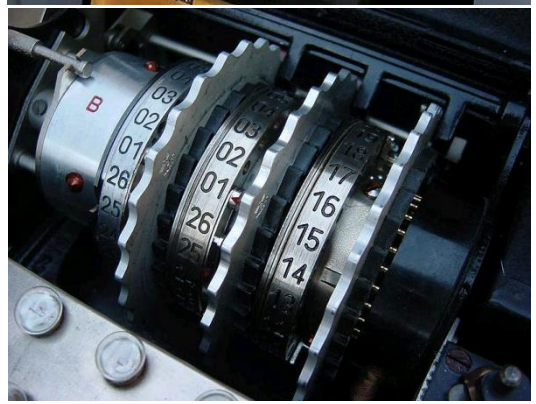
- **Rotor-Schlüsselmaschine aus dem zweiten Weltkrieg**
- **Verwendet von:**
  - deutschem Militär
  - Polizei
  - Geheimdiensten
  - …
- **„Enigma“ (αίνιγμα) [Griech.] = Rätsel**

Enigma – Die Entstehungsgeschichte

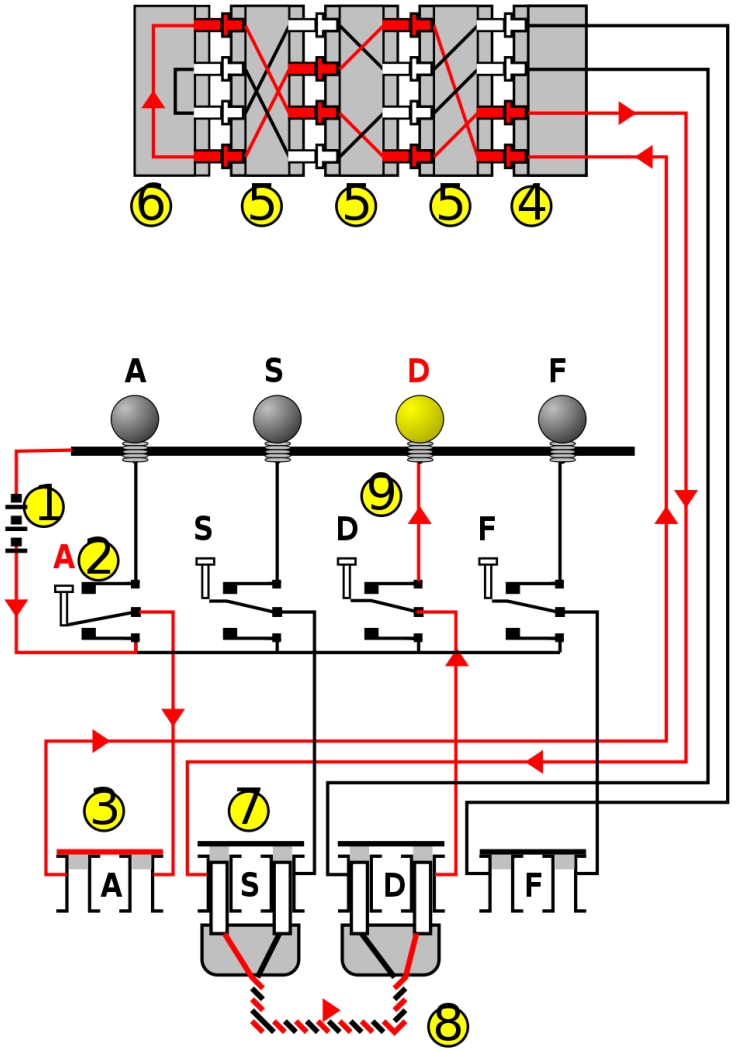
- **Erfunden von Arthur Scherbius (1878-1929)**
  - Erstes Patent vom 23. Feb. 1918
  - Gründung der Firma Chiffriermaschinen AG (1923)
- **Konzipiert als ziviles Chiffriersystem**
  - Vorgestellt (und zum Verkauf angeboten) auf Messen
    - Postkongress in Bern (1923)
- **Verschwand Ende der 1920er vom zivilen Markt**
  - Verstärktes militärisches Interesse
- **Es wurden über 30.000 Maschinen produziert**
  - Sehr viele unterschiedliche Modelle
  - Meistgebrauchte: ENIGMA I (Reichswehr, Wehrmacht)

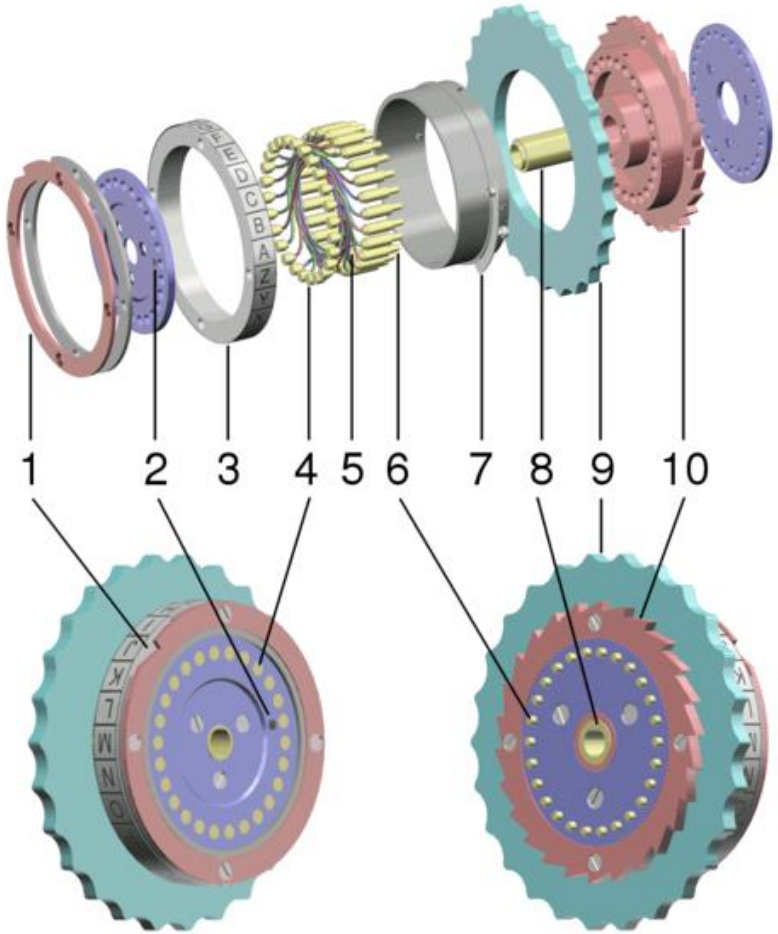
Enigma – Bestandteile

- **Tastatur (Eingabe)**
- **Lampenfeld (Ausgabe)**
- **Walzensatz (polyalphabetische Verschlüsselung)**
  - Wichtigstes Element
  - 26 Kontakte auf beiden Seiten
  - Unregelmäßig verbunden
  - Dreht mit jedem Buchstaben weiter
  - Austauschbar
- **Steckerbrett (monoalphabetische Verschlüsselung)**
  - Vertauscht einzelne Buchstaben



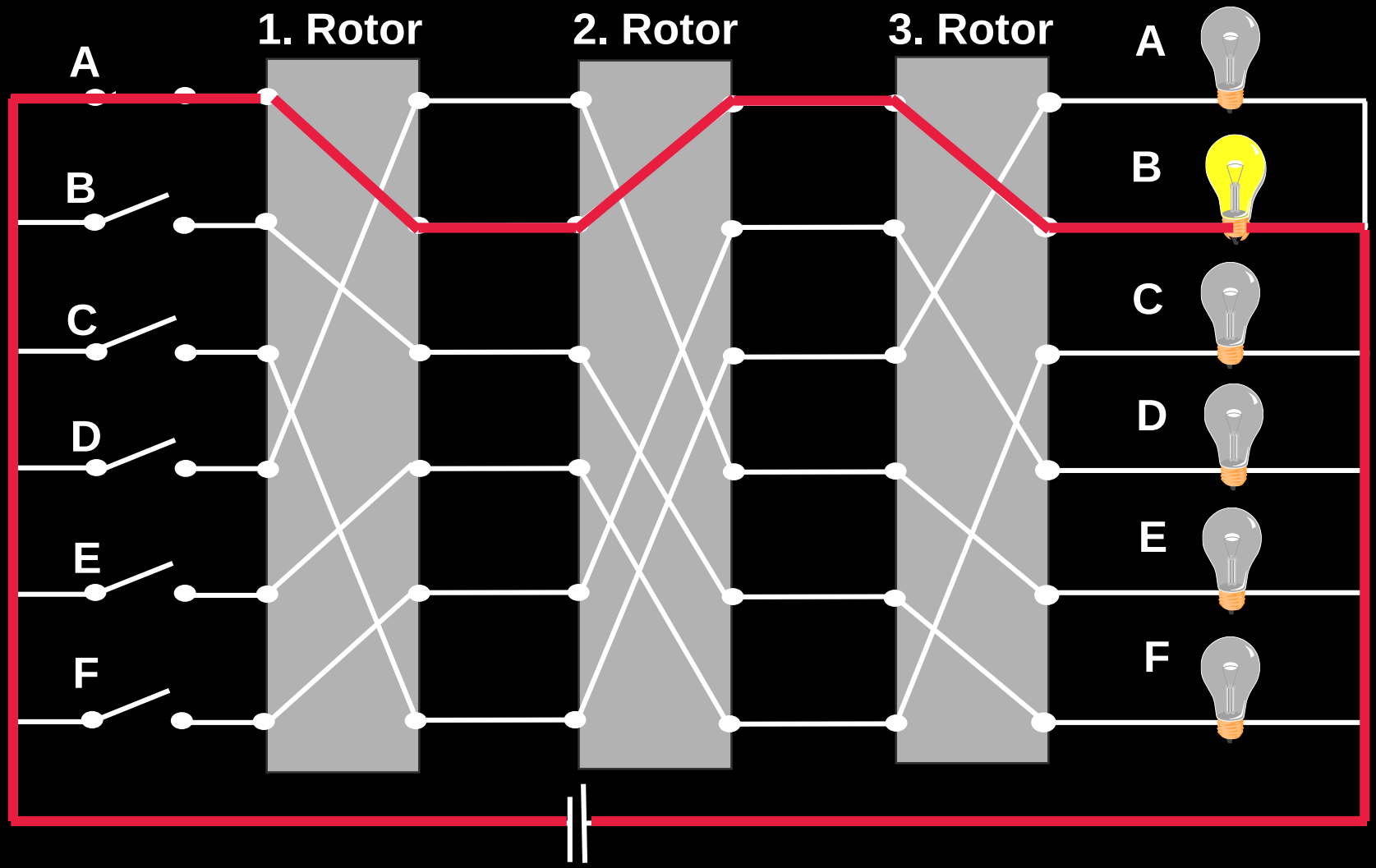
Enigma – Aufbau und Funktionsweise





Quelle: Wikipedia

Enigma – Stromlauf



Mit freundlicher Genehmigung
von Klaus Schmeh

Enigma – Vorbereitung

- **Tagesschlüssel besteht aus**
  - Auswahl von 3 Walzen (insgesamt gab es 5, bei M4 8)
  - Steckerverbindungen
  - Ringstellung
- **Beispiel einer Schlüsseltafel:**

```
Tag UKW Walzenlage Ringstellung ---- Steckerverbindungen ----
31   B   I   IV III 16 26 08    AD CN ET FL GI JV KZ PU QY WX
30   B   II  V  I   18 24 11    BN DZ EP FX GT HW IY OU QV RS
29   B   III I  IV  01 17 22    AH BL CX DI ER FK GU NP OQ TY
```

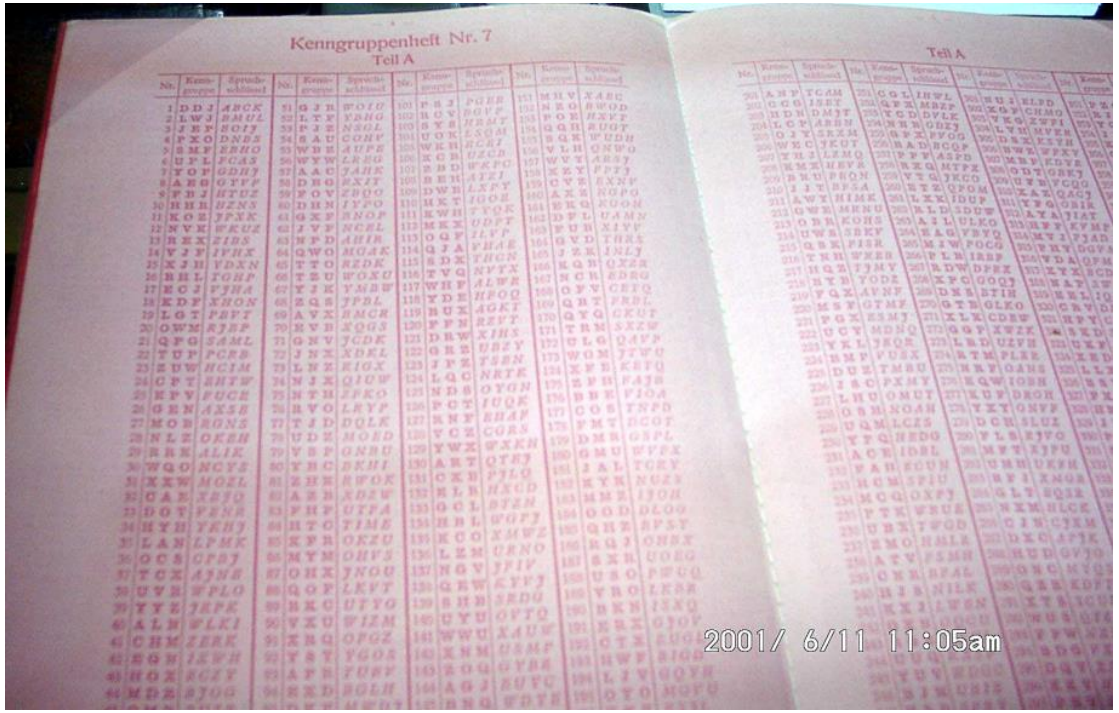
Enigma – Funkspruch (1/3)

- **Verwendung eines Spruchschlüssels**
  - Ändert sich mit jeder Nachricht
  - Prozedur zur Erstellung wurde ein paarmal geändert
- **Prozedur für Spruchschlüssel**
  - Wahl einer zufälligen Grundstellung, z. B. „QWE“
  - Wahl eines zufälligen Schlüssels, z. B. „RTZ“
  - „RTZ“ verschlüsseln, man erhält „EWG“
  - Grundstellung und *verschlüsselter* Spruchschlüssel werden im Kopf der Nachricht versendet

```
22:20   -   204   -   QWE EWG
```

Enigma – Funkspruch (2/3)

- **Kenngruppe**
  - Aus Kenngruppenbücher
  - Dient als Empfänger-Identifikation, z. B. „NOW“
  - Kenngruppe wurde permutiert, z. B. „OWN“
  - Aufgefüllt mit beliebigen Buchstaben zu 5 Zeichen, z.B. XYOWN
  - Diese 5 Zeichen wurden unverschlüsselt an den Anfang der Nachricht gestellt
- **Vorbereiten der Nachricht**
  - Enigma kann nur 26 Buchstaben verschlüsseln
  - Satzzeichen werden zu X
  - Eigennamen verdoppelt und mit X eingeschlossen
  - Zahlen ausgeschrieben
  - „ch“ als Q geschrieben



Enigma – Funkspruch (3/3)

```
Das Oberkommando der Wehrmacht gibt bekannt: Aachen ist
gerettet. Durch gebündelten Einsatz der Hilfskräfte konnte
die Bedrohung abgewendet und die Rettung der Stadt gegen
18:00 Uhr sichergestellt werden.
```

Nachricht vorbereiten

```
DASOB ERKOM MANDO DERWE HRMAQ TGIBT BEKAN NTXAA CHENX AACHE
NXIST GERET TETXD URQGE BUEND ELTEN EINSA TZDER HILFS KRAEF
TEKON NTEDI EBEDR OHUNG ABGEW ENDET UNDDI ERETT UNGDE RSTAD
TGEGE NXEIN SXAQT XNULL XNULL XUHRS IQERG ESTEL LTWER DENX
```

Nachricht verschlüsseln

```
22:20                        - 204 -                        QWE EWG
XYOWN LJPQH SVDWC LYXZQ FXHIU VWDJO BJNZX RCWEO TVNJC IONTF
QNSXW ISXKH JDAGD JVAKU KVMJA JHSZQ QJHZO IAVZO WMSCK ASRDN
XKKSR FHCXC MPJGX YIJCC KISYY SHETX VVOVD QLZYT NJXNU WKZRX
UJFXM BDIBR VMJKR HTCUJ QPTEE IYNYN JBEAQ JCLMU ODFWM ARQCF
OBWN
```

Enigma – Filmausschnitt

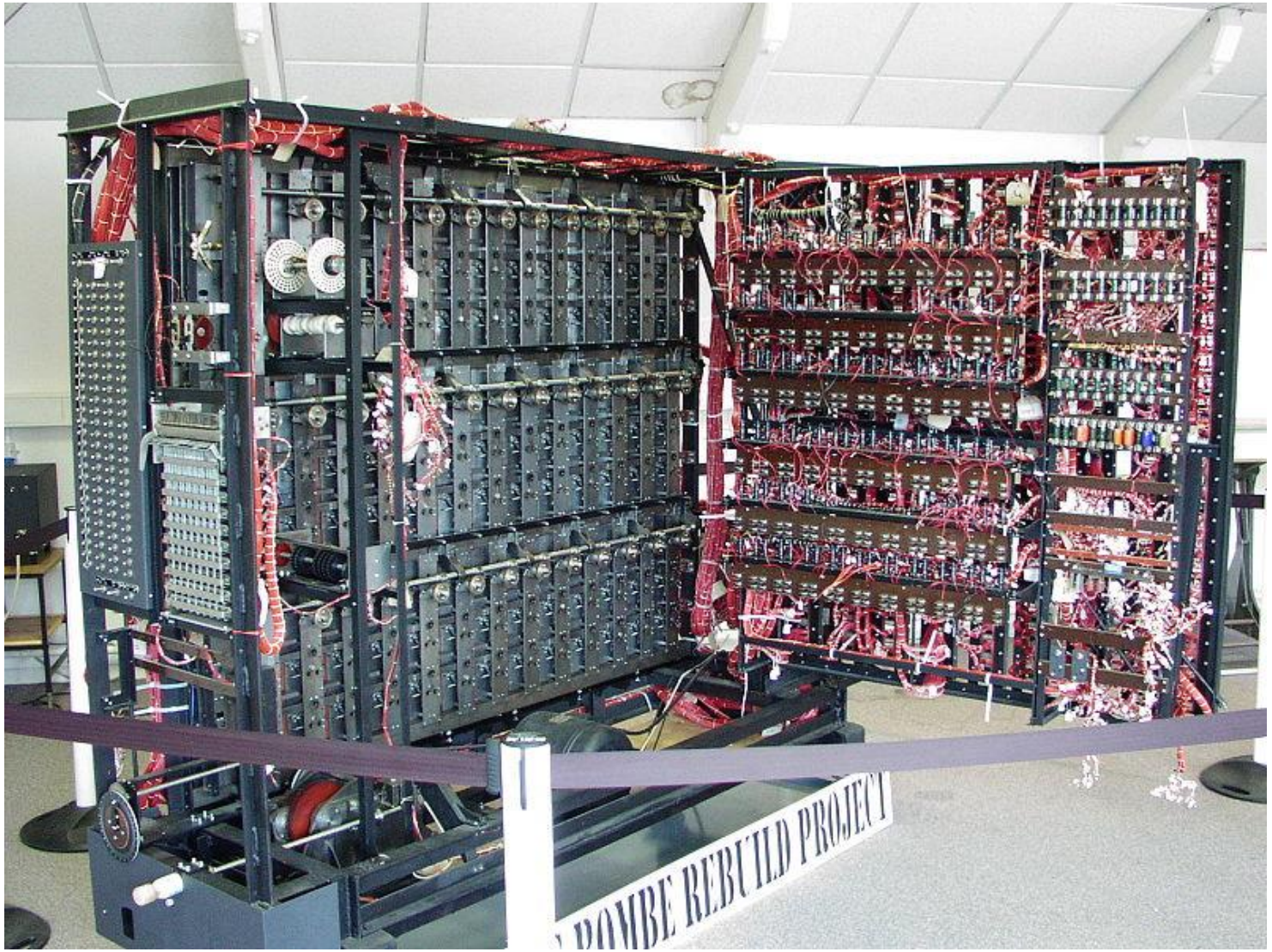
Enigma – Kryptoanalyse

- **Erfunden in den 1920er – sicher bis ca. 1930**
- **Maschinelle Verschlüsselung**
- **Unangreifbar durch damalige Verfahren**
  - Periodenbestimmung unsinnig, da Periodenlänge 19.900 (bei 3 Walzen)
  - Häufigkeitsanalyse unbrauchbar
- **Entscheidend für die Sicherheit**
  - Geheimhaltung der Walzenverdrahtung
  - Anzahl der Walzen
  - Anzahl der Steckverbindungen

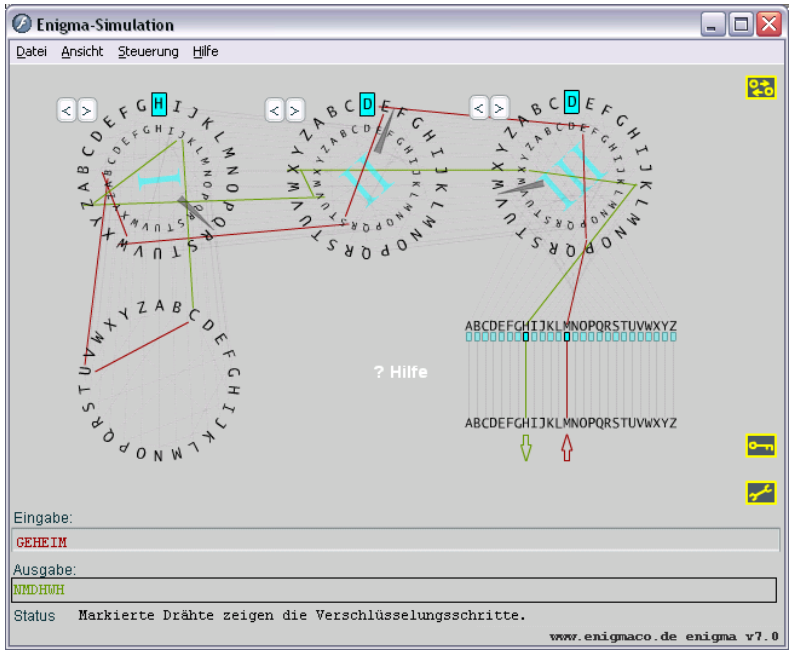
Enigma – Kryptoanalyse

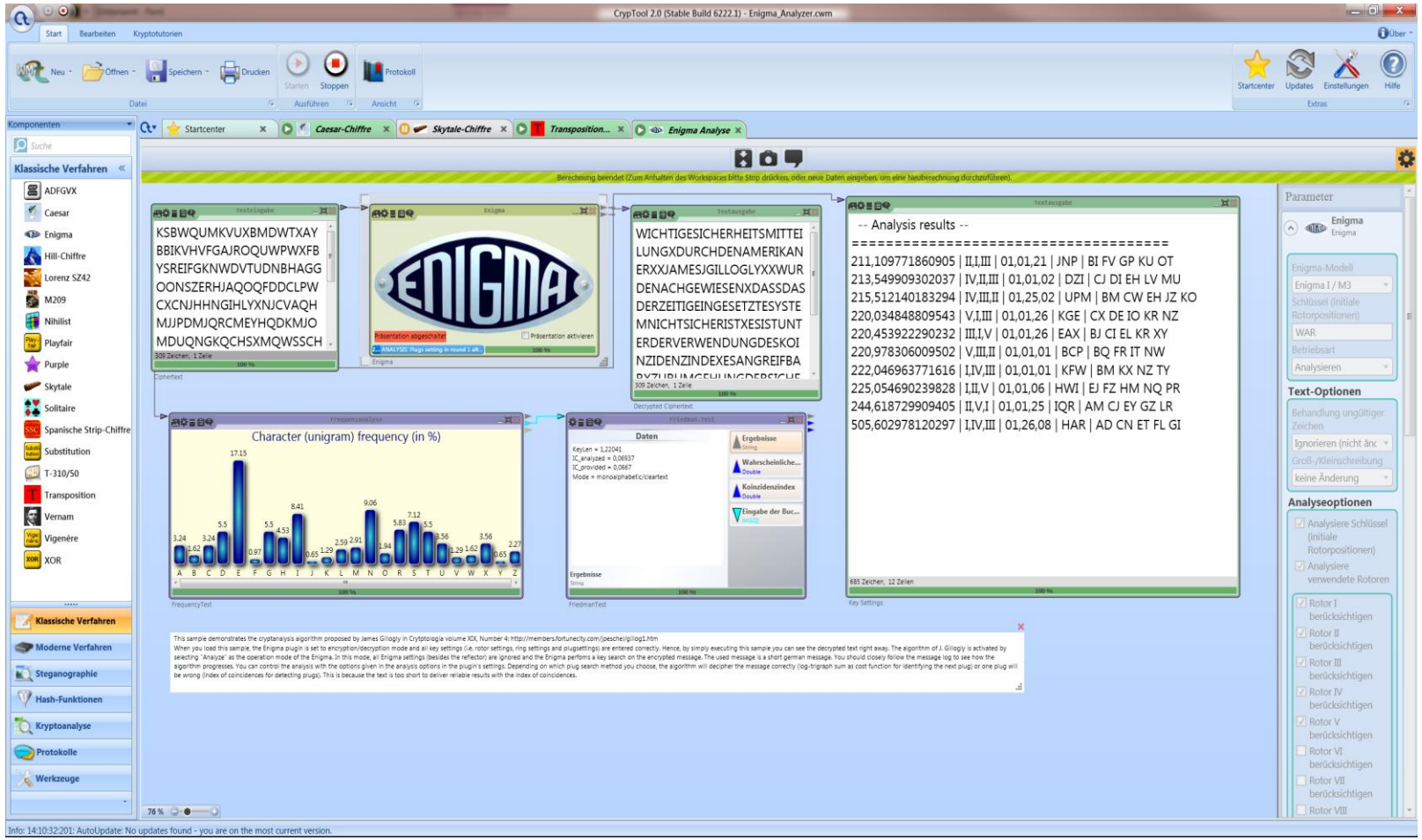
Enigma – Kryptoanalyse

Die Turing-Bombe



Demo: Enigma mit CrypTool 1.4.40 und CrypTool 2.1





UNIKASSEL VERSITÄT

Angewandte Informations Sicherheit

SFN

Moderne Verschlüsselung

Schülerkrypto 2017

Beginn der Computerverschlüsselung

- **Erfindung des Computers**
  - Die ersten Computer waren mechanisch (Relais)
  - 1938 – 1948: Z1, Z3, Atanasoff-Berry, Colossus, ENIAC
  - Lösten erst in den 70er Jahren die mechanischen Verschlüsselungsgeräte ab
- **Was ist nun anders?**
  - Aus Buchstaben werden Bits
    - Text wird in ein binäres Format gewandelt (z.B. ASCII)
    - Zeichenvorrat/Alphabet steigt von 26 auf 256 (1 Byte)
    - Bits werden substituiert/transponiert
  - Geschwindigkeit nimmt drastisch zu → komplexere Algorithmen
- **Was bleibt gleich?**
  - Substitution und Transposition (Permutation)
  - Gleicher Schlüssel zum Ver- und Entschlüsseln (zunächst): **Symmetrische Kryptographie**

Der Data Encryption Standard (DES)

Geschichtlicher Hintergrund (1/4)

- **Beteiligte US Regierungsstellen**
  - NBS: National Bureau of Standards
  - NIST: National Institute of Standards and Technology (ersetzte das NBS)
  - NSA: National Security Agency
    - Manchmal auch als “No Such Agency” bezeichnet
    - Weltgrößter Arbeitgeber für Mathematiker und Kryptologen
- **Industrie**
    - IBM

Der Data Encryption Standard (DES)

Geschichtlicher Hintergrund (2/4)

- **1973: Ausschreibung des NBS für einen nationalen Chiffrierstandard:**
  - Hohe Sicherheit
  - Vollständig spezifiziert und einfach zu verstehen
  - Sicherheit liegt nur im Schlüssel (Kerkhoffs‘ Prinzip)
  - Für alle verfügbar
  - Anpassbar für unterschiedliche Anforderungen
  - Ökonomisch/günstig integrierbar in elektronische Geräte
  - Einfach zu benutzen
  - Überprüfbar
  - Exportierbar

Der Data Encryption Standard (DES)

Geschichtlicher Hintergrund (3/4)

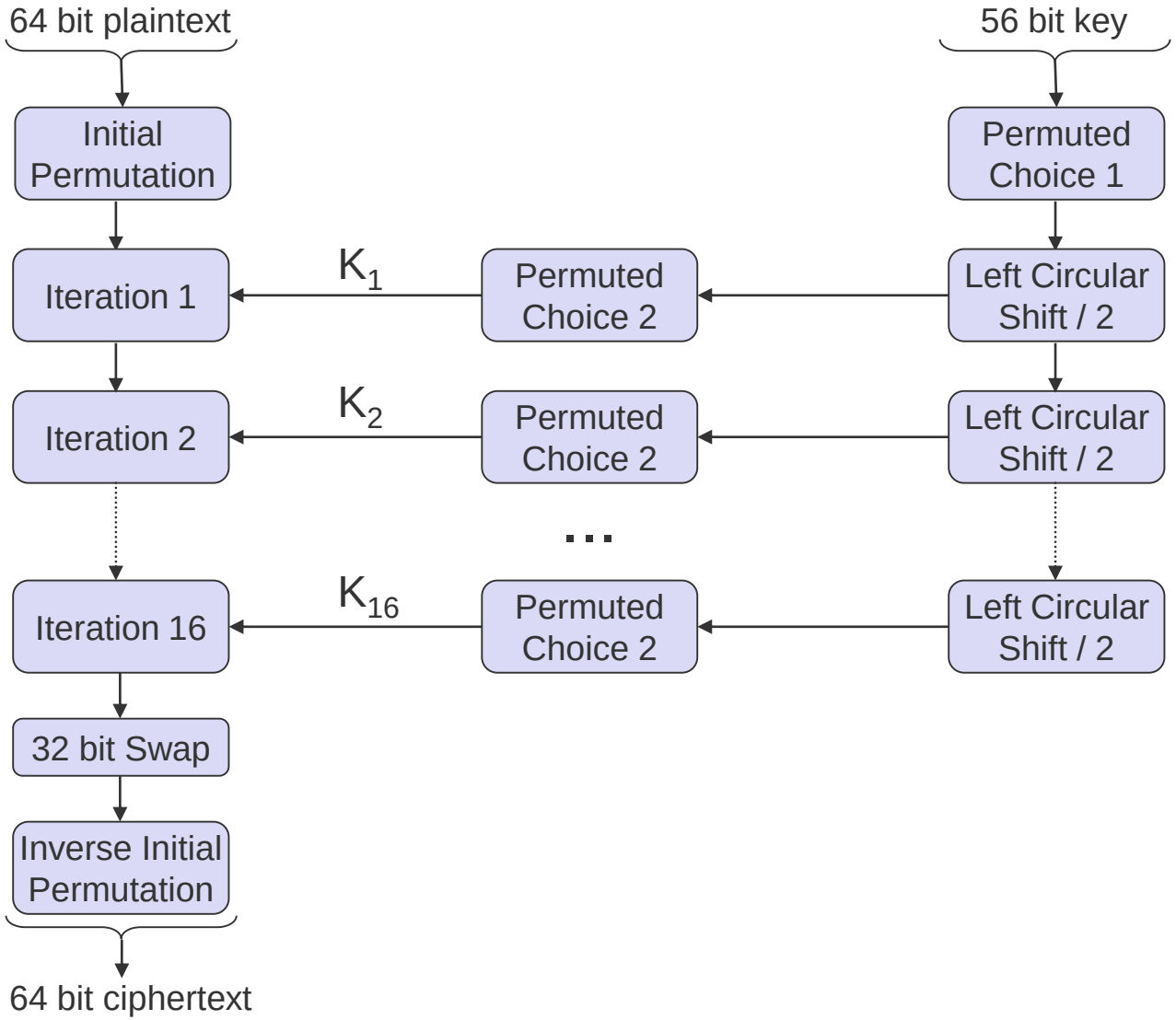
- **Erste Einreichungen entsprachen alle nicht den geforderten Kriterien**
- **IBM trat mit LUCIFER an**
  - Symmetrische Blockchiffre
  - Blockgröße: 128 Bit
  - Schlüssellänge: 128 Bit
- **NSA untersucht LUCIFER … und verändert ihn**
  - DES verhält sich genau wie LUCIFER, aber
  - Blockgröße: 64 Bit
  - Schlüssellänge: 56 Bit (Blockgröße != Schlüssellänge)
  - Warum? Hat die NSA eine Hintertür eingebaut?

Der Data Encryption Standard (DES)

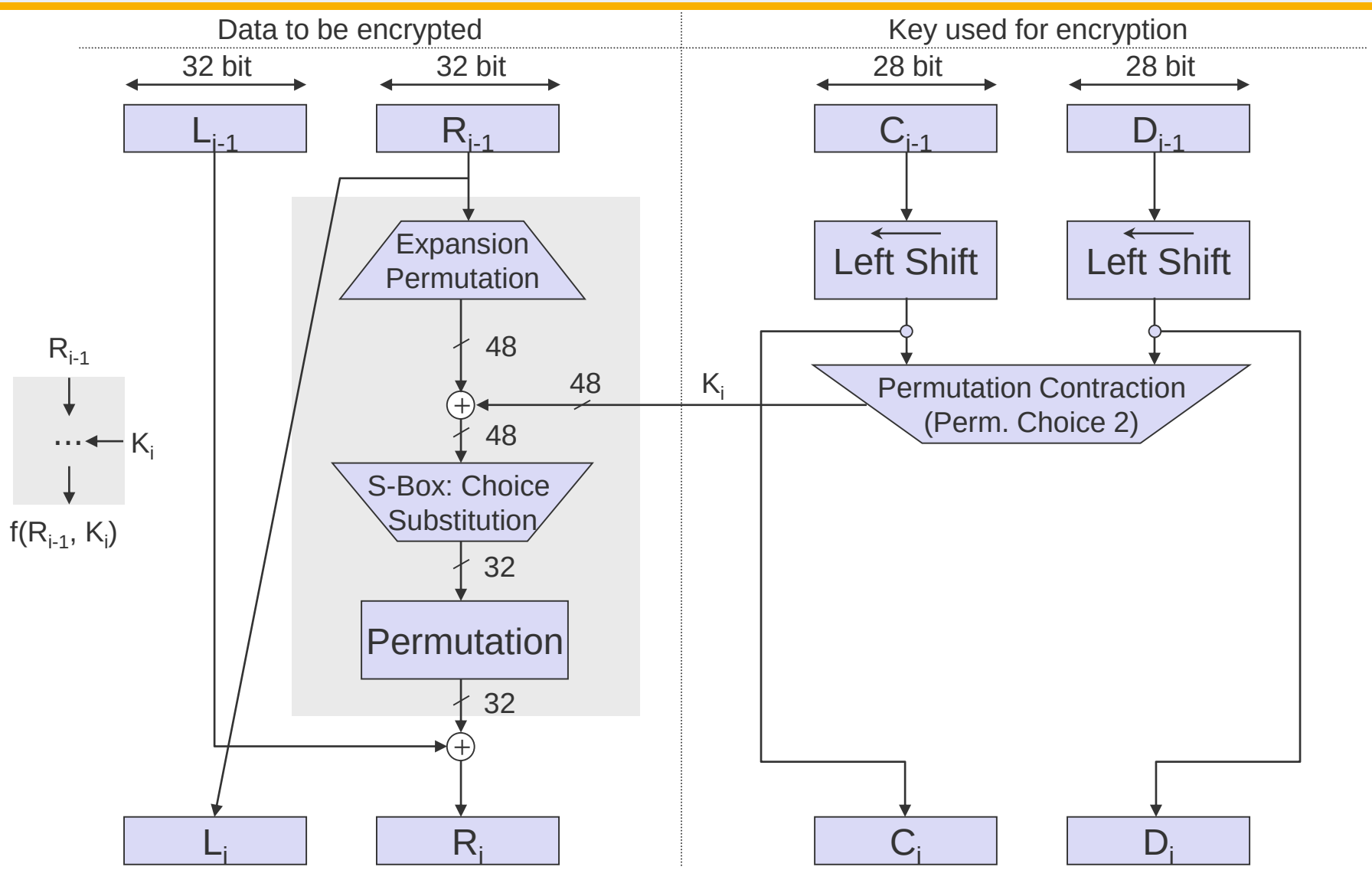
Geschichtlicher Hintergrund (4/4)

- **Verschwörungstheorie**
  - Die NSA veränderte die sogenannten S-Boxen (da kommen wir gleich dazu)
  - Kein Kryptologe konnte damals sagen, warum (die, die bei der NSA angestellt waren, durften nicht)
  - Grundlage für viele Verschwörungstheorien
- **Was wirklich geschah**
  - NSA kennt die „differentielle Kryptoanalyse“ seit den 70ern
  - Durch die Änderungen wurde DES davor geschützt
  - In den 90ern wurde die differentielle Kryptoanalyse (nochmal) entdeckt – durch öffentliche Einrichtungen
  - Jetzt verstand die Welt, was die wirklichen Gründe waren
    - Die neue S-Box verstärkte den DES
    - Die gekürzte Schlüssellänge schwächte ihn

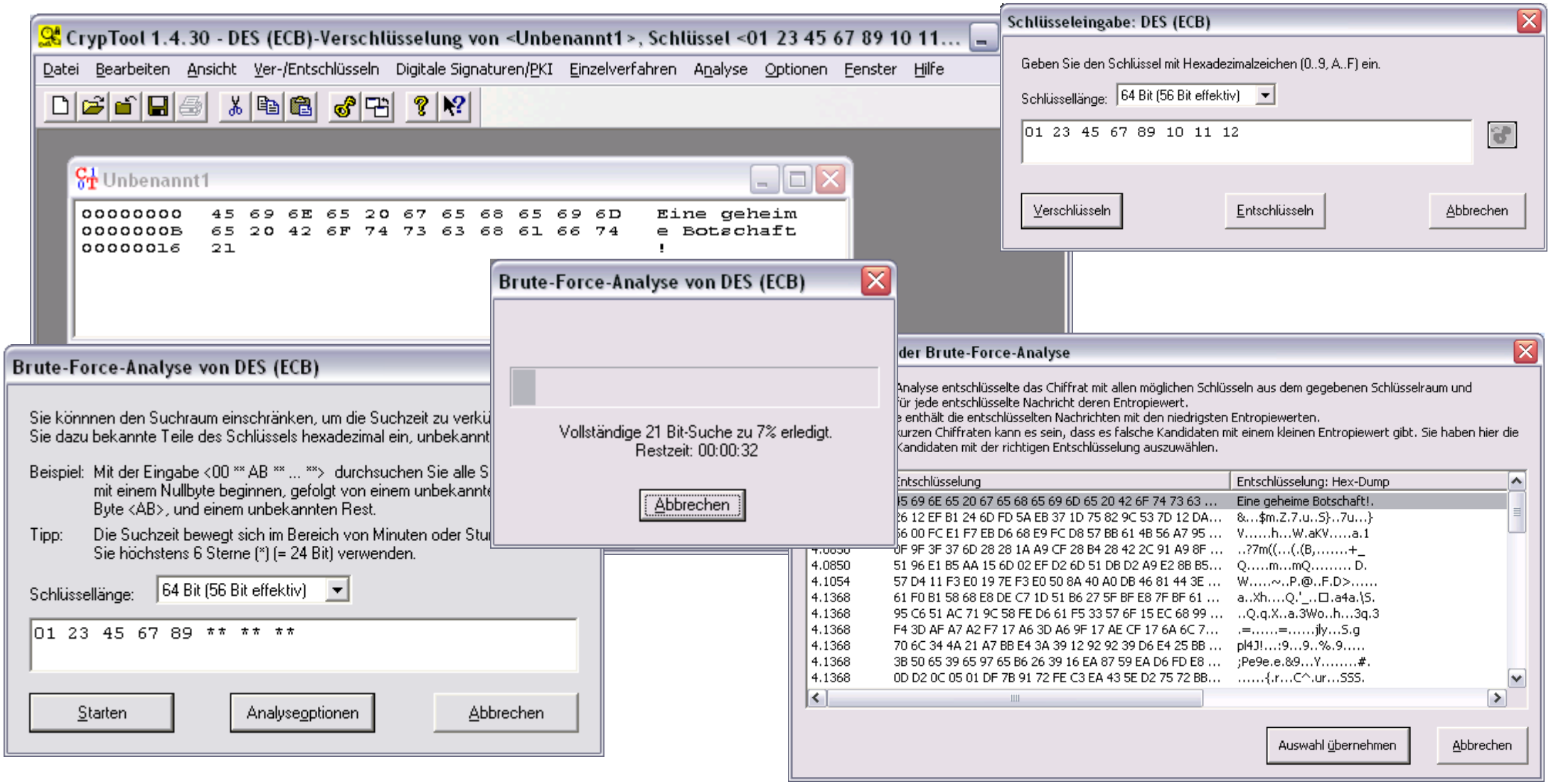
DES-Algorithmus Übersicht



Eine DES-Iteration (Runde)



Demo: DES mit CrypTool 1.4



Der Advanced Encryption Standard (AES)

- **Jan 1997: Das NIST veröffentlicht die Absicht, einen DES-Nachfolger einzuführen**
  - Verwendung bei Regierung
  - Verwendung in der Industrie
- **Sep 1997: Öffentliche Ausschreibung**
  - Offizieller DES-Nachfolger, genannt AES
  - Jeder auf der Welt kann einen Algorithmus einreichen
  - Algorithmus muss offen und ohne Gebühren weltweit verwendbar sein

Der Advanced Encryption Standard (AES)

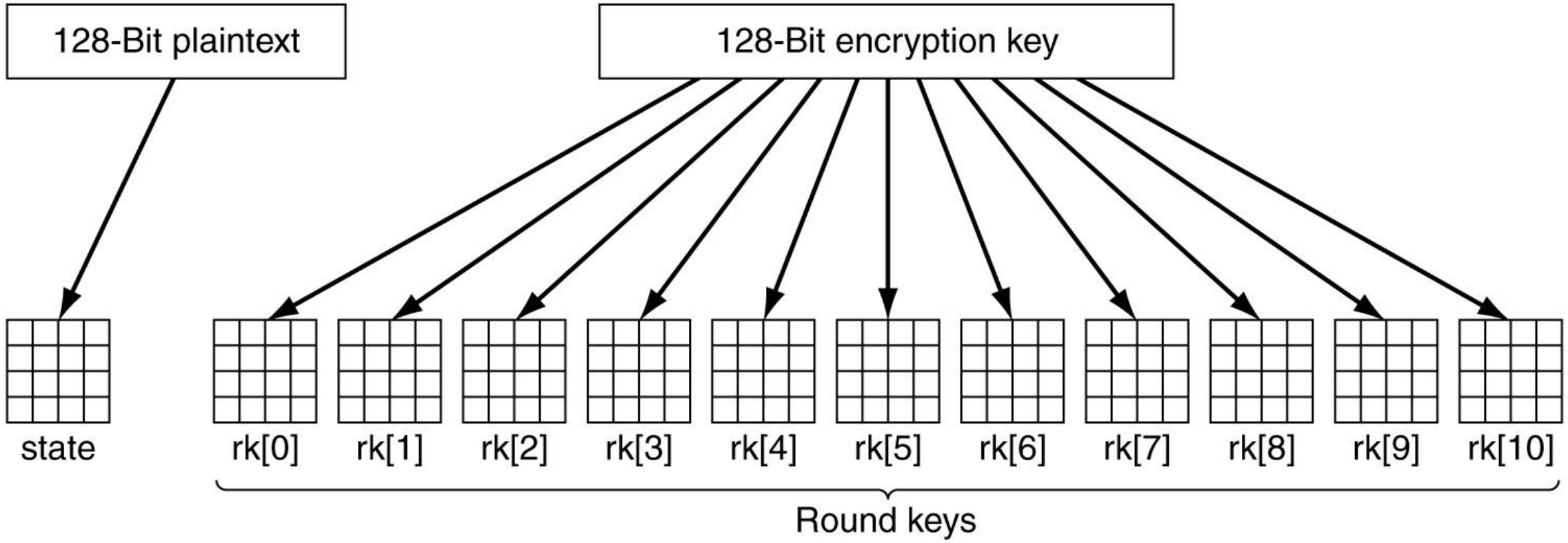
- **Aug 1998: Erste AES Konferenz**
  - Die besten 15 Kandidaten wurden gewählt
- **Mär 1999: Zweite AES Konferenz**
  - Analyse der Kandidaten durch Kryptologen
- **Apr 1999: Fünf „Finalisten“ werden gewählt**
  - MARS, RC6, Rijndael, Serpent, und Twofish
- **Okt 2000: Rijndael (=AES) wird offizieller DES-Nachfolger**

Der Advanced Encryption Standard (AES)

Details

- **Schlüssel- und Blocklängen**
  - Schlüssellänge: 128, 192 oder 256 Bit (Rijndael zusätzlich: 160, 224)
  - Blocklänge: 128 Bit (Rijndael: 160,192,224,256)
- **AES ist somit ein 128 Bit Blockchiffre**
  - Genau wie DES arbeitet auch AES in Runden (10)
- **Der Algorithmus arbeitet auf (128 Bit Schlüssel):**
  - state [4,4]: Byte-Tabelle mit 4 Zeilen und 4 Spalten
  - key[4,4]: Byte-Tabelle mit 4 Zeilen und 4 Spalten
    - Ein Schlüssel für jede Runde

Der Advanced Encryption Standard (AES)

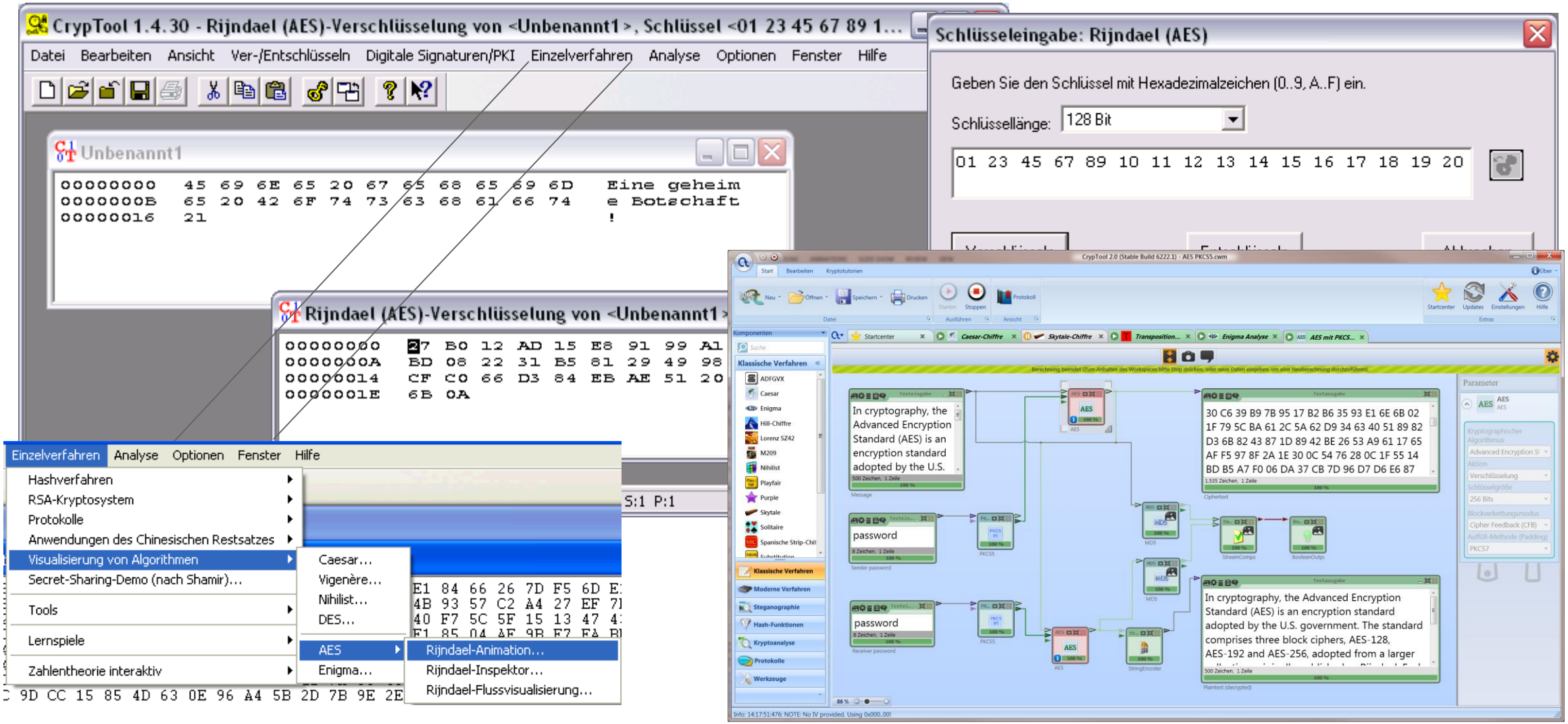


Erstellen des *state* und des *rk* arrays

Der Advanced Encryption Standard (AES)

- **Runde 1 – 9**
  - ByteSub: eine nicht-lineare Substitution (S-Box)
  - ShiftRow: Die Zeile der state-Tabelle werden zyklisch geschoben (rotiert) – mit verschiedenen offsets
  - MixColumn: Man betrachtet die Spalten der state-Tabelle als Polynome im GF(2^8) und multipliziert diese
  - RoundKey: Der Rundenschlüssel wird mit dem state XOR-verknüpft
- **Runde 10 ist ohne MixColumn**

Demo: AES mit CrypTool 1.4.40 & CrypTool 2.1



Das Schlüsselaustauschparadoxon

- „Austausch von geheimen Botschaften ohne vorherigen Austausch eines Geheimnisses“
- Die meisten Kryptologen glaubten nicht an eine Lösung des Schlüsselaustauschparadoxons

- Das folgende Beispiel gab Hoffnung:

Demo: Schlüsselaustausch

Schlüsselaustausch

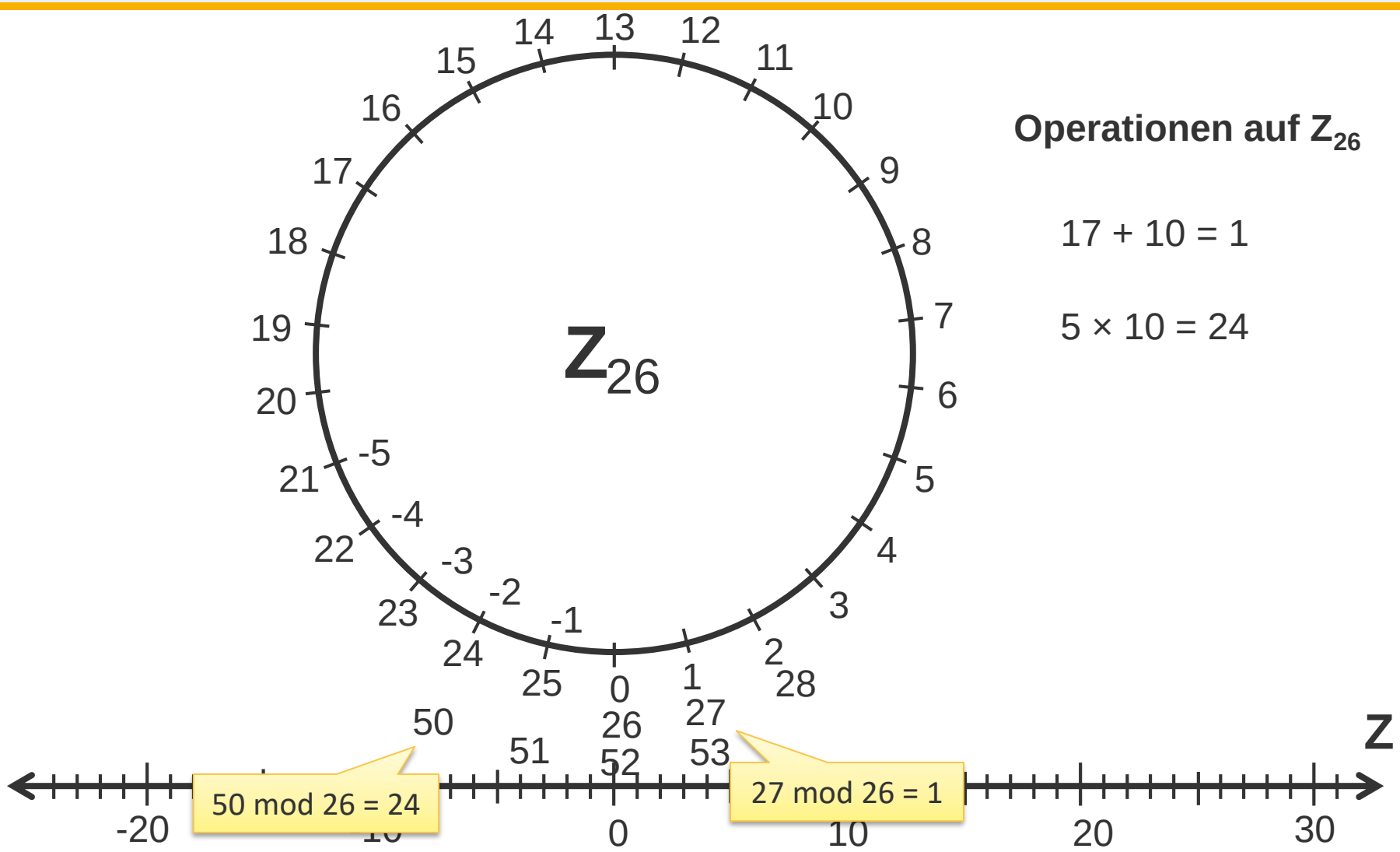
- **Problem: Reihenfolge ist wichtig bei Verschlüsselung**
- **Zweifache Verschlüsslung einer Nachricht (2 Schlösser)**
  - $c = E_{C2}(E_{C1}(m))$
- **Entschlüsselung muss in der richtigen Reihenfolge sein!**
  - $m = D_{C1}(D_{C2}(c))$
  - Allgemein gilt $E_{C2}(E_{C1}(m)) \neq D_{C2}(D_{C1}(c))$!!
  - Nur wenige Ausnahmen, z.B. Caesar

- **Suche nach speziellen mathematischen Funktionen**

➔Falltürfunktionen (einfach in eine Richtung, schwer in die andere)

➔Rechnen in Ringen

Rechnen in Ringen (1)

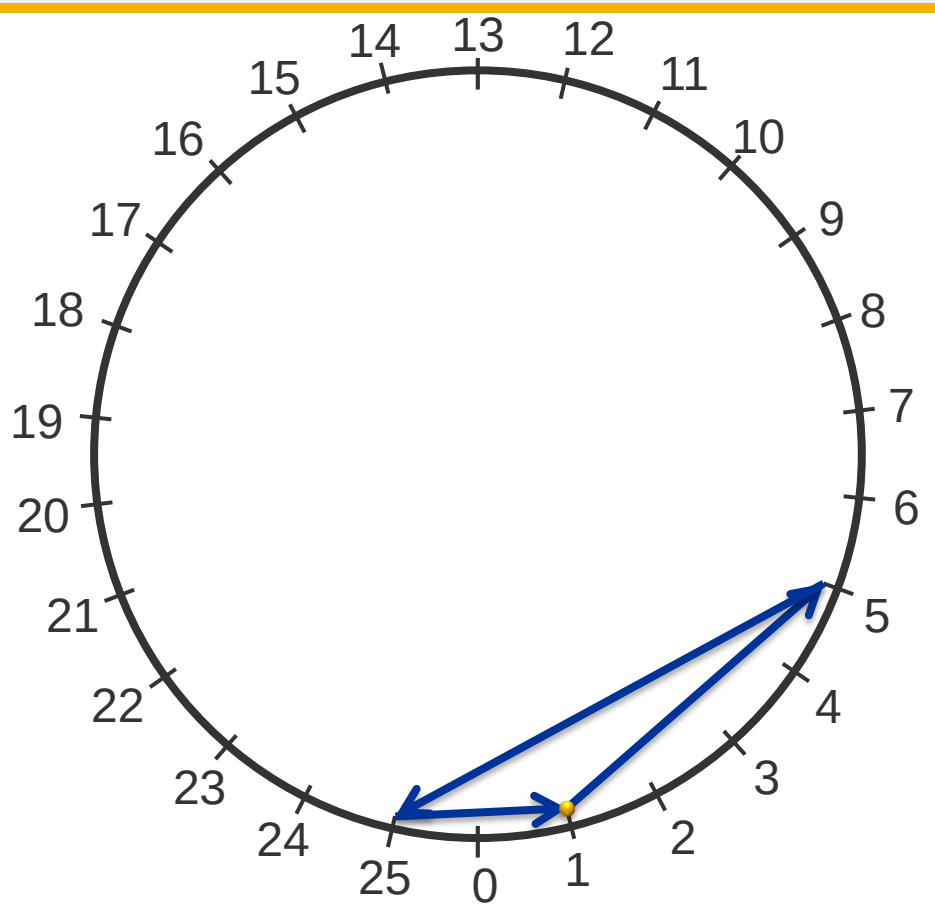


Operationen auf Z_{26}

$17 + 10 = 1$

$5 \times 10 = 24$

Rechnen in Ringen (2)



5^n in Z_{26}

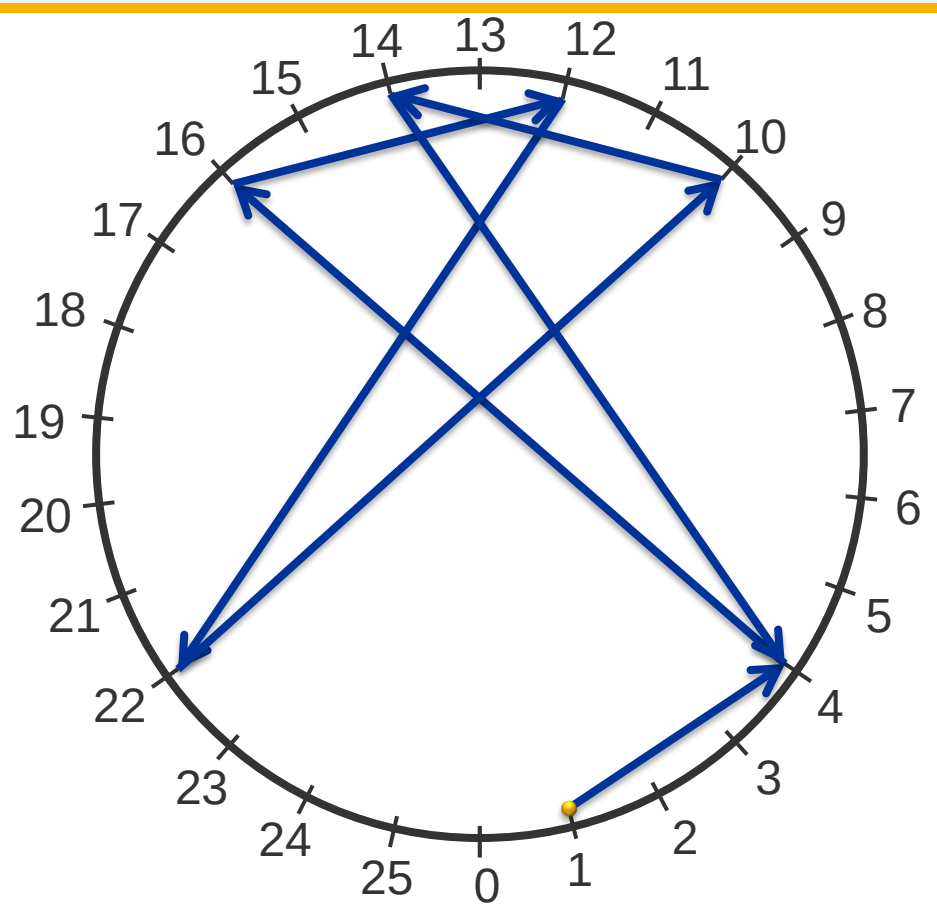
$5^0 = 1 \bmod 26 = 1$

$5^1 = 5 \bmod 26 = 5$

$5^2 = 25 \bmod 26 = 25$

$5^3 = 125 \bmod 26 = 1$

Rechnen in Ringen (3)



4^n in Z_{26}

$4^0 = 1 \bmod 26 = 1$

$4^1 = 4 \bmod 26 = 4$

$4^2 = 16 \bmod 26 = 16$

$4^3 = 64 \bmod 26 = 12$

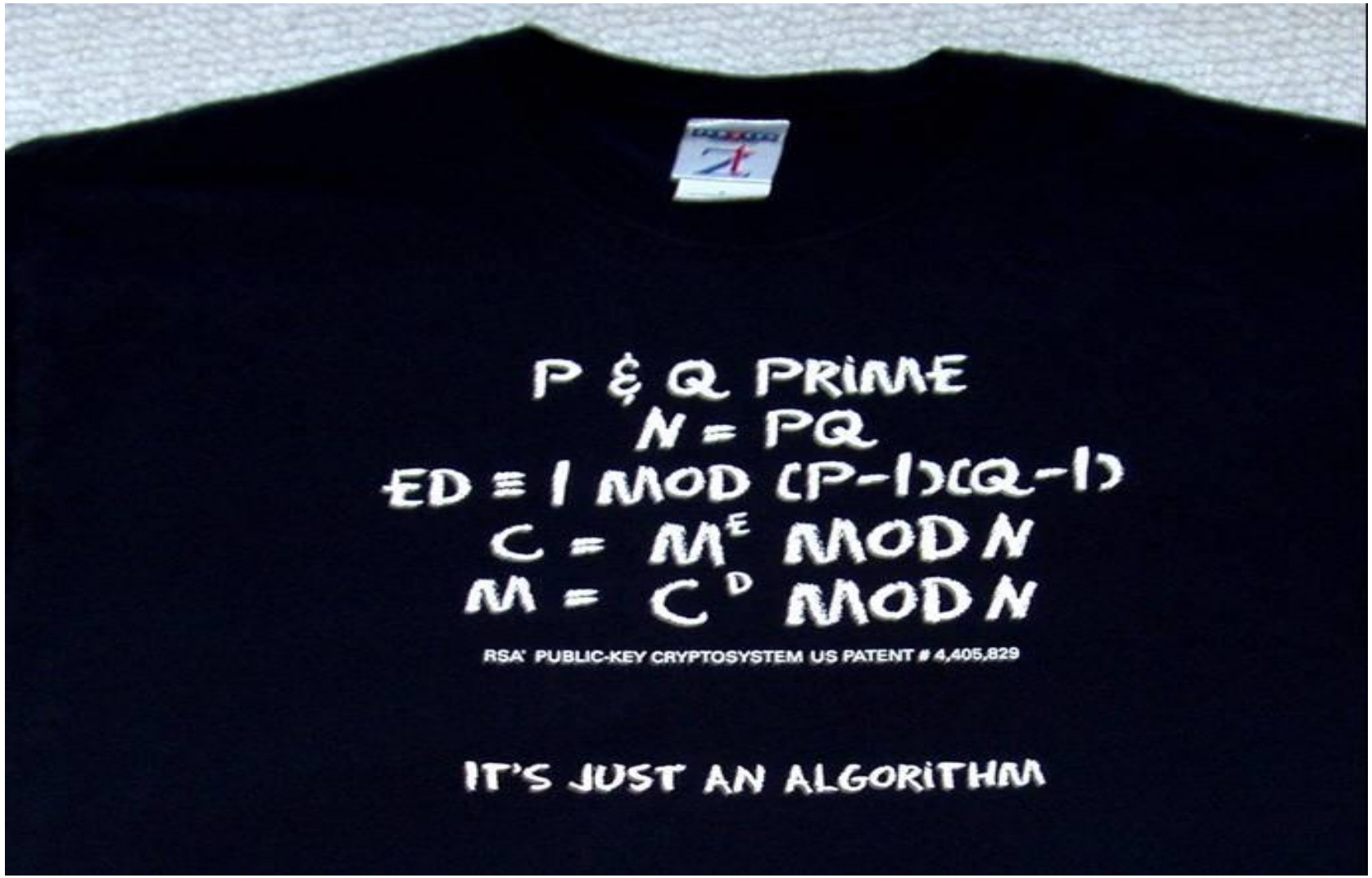
$4^4 = 256 \bmod 26 = 22$

$4^5 = 1024 \bmod 26 = 10$

$4^6 = 4096 \bmod 26 = 14$

$4^7 = 16384 \bmod 26 = 4$

RSA


P & Q PRIME
N = PQ
ED ≡ 1 MOD (P-1)(Q-1)
C = M^E MOD N
M = C^D MOD N
RSA' PUBLIC-KEY CRYPTOSYSTEM US PATENT # 4,405,829
IT'S JUST AN ALGORITHM

RSA Schlüsselerzeugung (1)

1. **Wähle zwei große Primzahlen *p,q***
   - Jeweils mindestens 200 Dezimalstellen
2. **Berechne $n = p \cdot q$**
3. **Berechne $\Phi(n) = \Phi(p,q) = (p-1)(q-1)$**
4. **Wähle eine Zahl *e* teilerfremd zu $\Phi(n)$**
   - Mathematisch: $ggT(e, \Phi(n))=1$
   - Jede Primzahl $<\Phi(n)$ kann verwendet werden
5. **Berechne *c,d* mit dem erweiterten euklidischen Algorithmus:**

   $$e \cdot d + c \cdot \Phi(n) = 1 \quad \text{oder} \quad e \cdot d = k \cdot \Phi(n) + 1$$

   - **Somit gilt: $e \cdot d \bmod \Phi(n) = 1$**

RSA Schlüsselerzeugung (2)

- **Öffentlicher Schlüssel: (*e*,*n*)**
- **Privater Schlüssel: (*d*,*n*)**

- **Lösche die Primzahlen *p*,*q***
- **Warum?**
  - Angenommen ein Angreifer kennt *p*,*q*
  - Somit kennt er sofort $\Phi(n) = (p-1)(q-1)$
  - Jetzt kann er *d* berechnen
  - Der private Schlüssel ist nicht mehr geheim ☹

→ **RSA ist sicher,**
solange es in der Praxis zu aufwändig ist, *p*,*q* zu berechnen

RSA Ver- und Entschlüsselung

- Sei $m < n$ eine zu verschlüsselnde Nachricht
- Verschlüsselung

  $c = m^e \bmod n$
- Entschlüsselung

  $m' = c^d \bmod n$
- Derselbe Algorithmus für Ver-/Entschlüsselung
- $m = m'$ ist mathematisch beweisbar

  → RSA ist formal korrekt ☺

RSA Beispiel – Überblick

Alice schickt eine geheime Nachricht an Bob

1. **Bob muss ein Schlüsselpaar generieren**
2. **Alice muss mit Bobs öffentlichem Schlüssel die Nachricht verschlüsseln**

RSA Beispiel – Schlüsselerzeugung

- **Wir erzeugen ein Schlüsselpaar für Bob**
- **Wähle zwei Primzahlen, z. B. *p=3* und *q=11***
  - Sehr kleine Primzahlen im Beispiel
- **Berechne *n = 3 · 11 = 33***
- **Berechne *Φ(33) = (3-1)(11-1) = 20***
- **Wähle e teilerfremd zu *Φ(33) = 20, z. B. e = 3***
- **Berechne ein *d<Φ(33)*, sodass *3 · d = k · 20+1***
  - Bei *k=1* ist *d=7*, denn *3 · 7 = 1 · 20+1*
- **Bobs öffentlicher Schlüssel ist *(e, n) = (3, 33)***
- **Bobs privater Schlüssel ist *(d, n) = (7, 33)***

RSA Beispiel – Verschlüsselung

- **Alice möchte die Zahl *4* verschlüsseln**
  - Somit ist die Nachricht ***m=4***
- **Alice kennt Bobs öffentlichen Schlüssel**
  - *(e,n) = (3,33)*
- **Alice berechnet Chiffretext $c = m^e \bmod n$**
  - $c = 4^3 \bmod 33 = 64 \bmod 33 = 31$
- **Alice sendet *31* an Bob**

RSA Beispiel – Verschlüsselung

- **Bob empfängt *c = 31***
- **Nur Bob kennt seinen privaten Schlüssel**
  - *(d,n) = (7,33)*
- **Bob berechnet Klartext *m = c^d mod n***
  - ***m*** *= 31^7 mod 33 = 27512614111 mod 33* ***= 4***

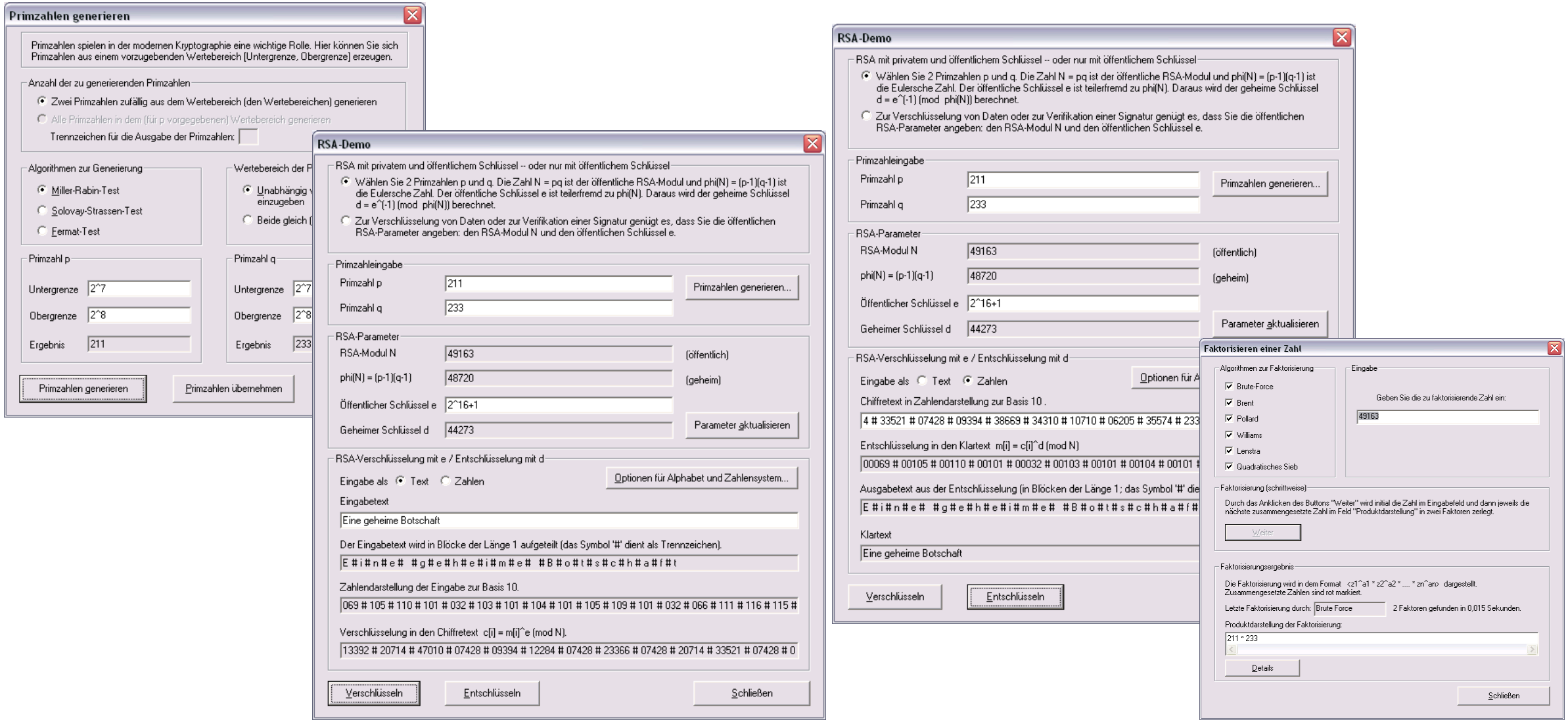
RSA Beispiel – Kryptoanalyse

- **Und Dave? Er kennt**
  - Bobs öffentlichen Schlüssel *(e,n) = (3,33)*
  - Die verschlüsselte Nachricht *c = 31*
- **Um c zu entschlüsseln braucht er aber *(d,n)***
- **Dave ist nicht dumm:**
  - Er faktorisiert $n = 33 = 3 \cdot 11$
  - Nun berechnet er $\Phi(33) = (3-1)(11-1) = 20$
  - .. und d so dass $3 \cdot d = k \cdot 20+1$, und findet $d=7$!
  - Mit $d=7$ kann er die Nachricht auch entschlüsseln

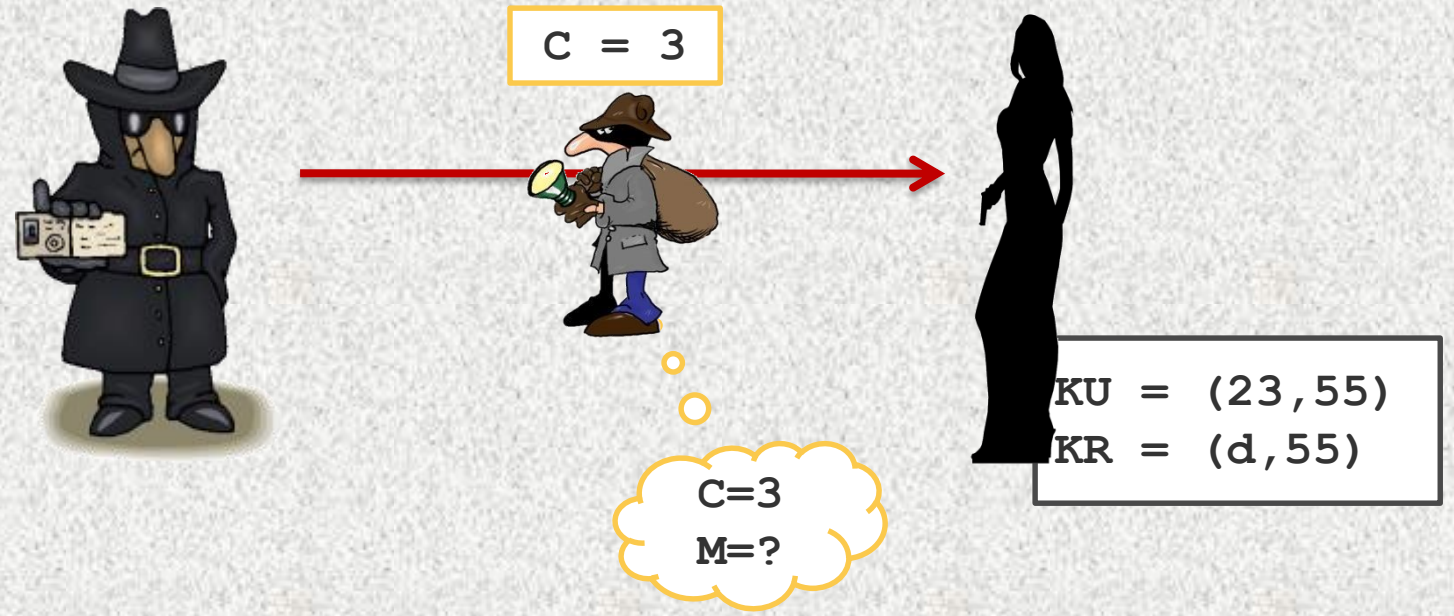
RSA – Kryptoanalyse

- **RSA ist so schwierig wie Faktorisieren**
  - Wenn man Faktorisieren kann, kann man RSA brechen
- **Algorithmen zur Faktorisierung**
  - Probedivision (langsam für wenig Primfaktoren)
  - Kettenbruchmethode, CFRAC (besser)
  - Quadratisches Sieb, QS (ziemlich gut)
  - Allgemeines Zahlenfeldsieb, GNFS (bester bekannter Algorithmus)
- **Programme zur Faktorisierung**
  - CrypTool 1.4.40 (QS, Probedivision) – langsam
  - CrypTool 2.1 (QS, Probedivision) – schnell (msieve) & verteilt
  - ggnfs (GNFS) – Projekt wird nicht mehr gepflegt
  - msieve (QS, GNFS) – QS schnell (nicht verteilt), GNFS noch beta

Demo: RSA mit CrypTool 1.4.40



Das RSA – Rätsel



Welche Nachricht hat Bob an Alice gesendet?

Kryptoanalyse – RSA-Rätsel

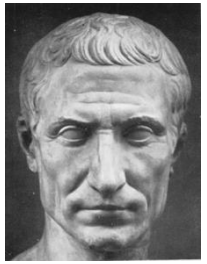
- **Faktorisierung von $n = p \cdot q$**
  - $55 = \mathbf{5 \cdot 11}$
- **Aus p und q berechnet man $\Phi(n) = (p-1)(q-1)$**
  - $\mathbf{\Phi(55)} = (5-1)(11-1) = 4 \cdot 10 = \mathbf{40}$
- **Finde d so dass gilt $e \cdot d = k \cdot \Phi(n) + 1$**
  - $23 \cdot d = k \cdot 40 + 1$
  - Durch probieren, mit $k = 1,2,3..$ findet man $k=4$
  - $23 \cdot d = 4 \cdot 40 + 1 = 161$ ➔ **$d=161/23 = 7$**
- **Entschlüsseln: $M = C^d \bmod n$**
  - $M = 3^7 \bmod 55$
  - **$M = 2187 \bmod 55 = 42$**

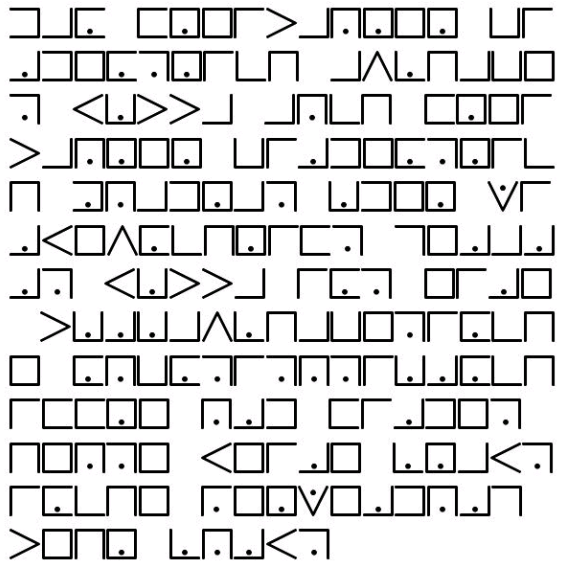
Zusammenfassung

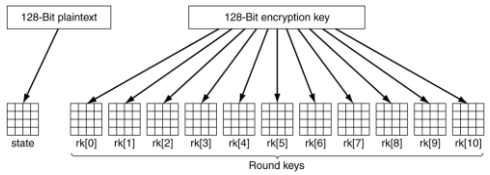
Schülerkrypto 2017

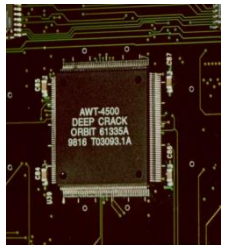
Zusammenfassung

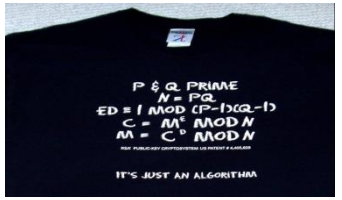
- **Einfache Verschlüsselung**
  - Skytale
  - Caesar
- **Verbesserte Verschlüsselung**
  - Spaltentransposition
  - Substitution
- **Maschinelle Verschlüsselung**
  - Enigma
- **Moderne Verschlüsselung**
  - Symmetrisch: DES, AES
  - Asymmetrisch: RSA











Vielen Dank
für Ihre Aufmerksamkeit!

Prof. Arno Wacker
arno.wacker@uni-kassel.de