

# **Einführung in die Kryptologie mit CrypTool**

## **Übung Teil I – Bedienung CrypTool**

**Workshop  
INFOS 2009**



[www.cryptool.com](http://www.cryptool.com)  
[www.cryptool.de](http://www.cryptool.de)  
[www.cryptool.org](http://www.cryptool.org)  
[www.cryptool.pl](http://www.cryptool.pl)

# CrypTool

## CrypTool ist eine Desktop-Anwendung

The screenshot shows the CrypTool 1.4.30 desktop application. The main window is titled "CrypTool 1.4.30 - Autokorrelation von <Vigenère-Verschlüsselung von <startbeispiel-de.txt>, Schlüssel <TEST>>". It features a menu bar with options: Datei, Bearbeiten, Ansicht, Ver-/Entschlüsseln, Digitale Signaturen/PKI, Einzelverfahren, Analyse, Optionen, Fenster, and Hilfe. Below the menu bar is a toolbar with various icons. The main content area displays a document titled "startbeispiel-de.txt" with the following text:

CrypTool

CrypTool ist ein umfangreiches Lernprogramm zu den Themen Kryptographie und Kryptoanalyse.

Di VvqiMsge

1) VvqiMsge bwl xbr mfyefzkiavaik Exvfxsyktqe sn hwg Mlwfyr Ckrtlhzyviamw ngh Ckrtlhtsrww.

"H Wbik blx wbgj Lxqxvtmia, fbv vxk Wax Bljx xvkmxr Kyavammi ebm GjriXghe qsvaif dögrwg.

Öf

2) 1) Wif uxwixg Üfwkupavd üfwk www.Fägnvawhmfefr UktLhnp thvewm www.Lmeimliamx mfwww Ohahnp Sfobw Ahnpx cy

Sy UktLhnp. Nhg hwk Lxskm

ASCII-Histogramm von <Vigenère-Verschlüsselung von <startbeispiel-de.txt>, Schlüssel <TEST>> (1161 ...

xkwvbwfwa Lmw üuxv ytl Qv

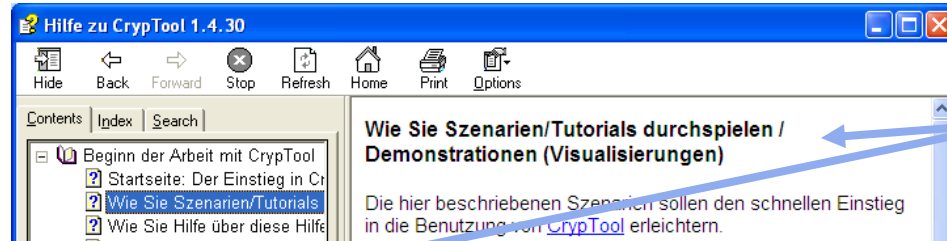
Below the document, there is a window titled "Autokorrelation von <Vigenère-Verschlüsselung von <startbeispiel-de.txt>, Schlüssel <TEST>>". It displays a line graph titled "Autokorrelation von <Vigenère-Verschlüsselung von <startbeispiel-de.txt>, Schlüssel <TEST>>". The y-axis is labeled "Anzahl der übereinstimmenden Zeichen" and ranges from 30 to 110. The x-axis is labeled "Verschiebung" and ranges from 1 to 180. The graph shows a periodic pattern with peaks at intervals of approximately 16 characters. To the right of the graph is an ASCII histogram titled "Schlüssel <TEST>> (1161 Zeichen)". The x-axis is labeled "Wert" and shows the letters k, m, o, q, s, u, w, y. The histogram shows the frequency of these letters in the key.

Annotations with arrows point to the following elements:

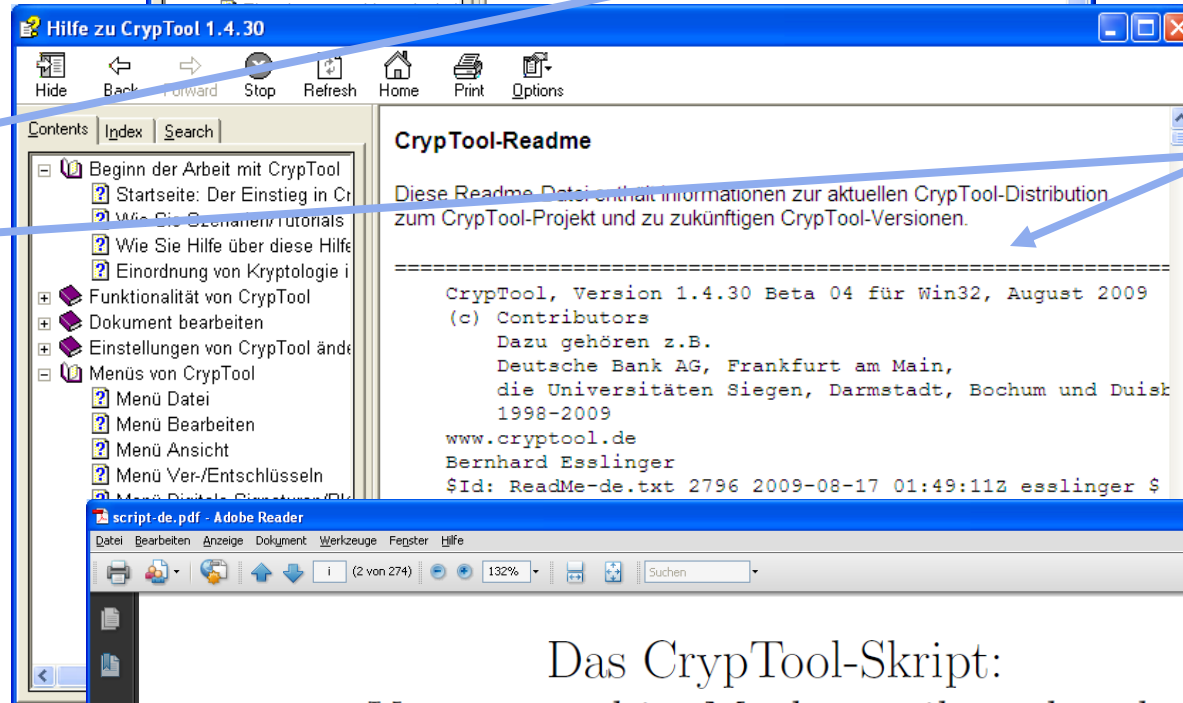
- Menü**: Points to the menu bar.
- Dokument**: Points to the document window.
- Statusleiste mit Hinweisen**: Points to the status bar at the bottom, which contains the text "Drücken Sie F1, um die Hilfe aufzurufen".

# CrypTool

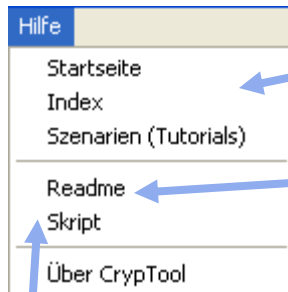
## CrypTool Online-Hilfe



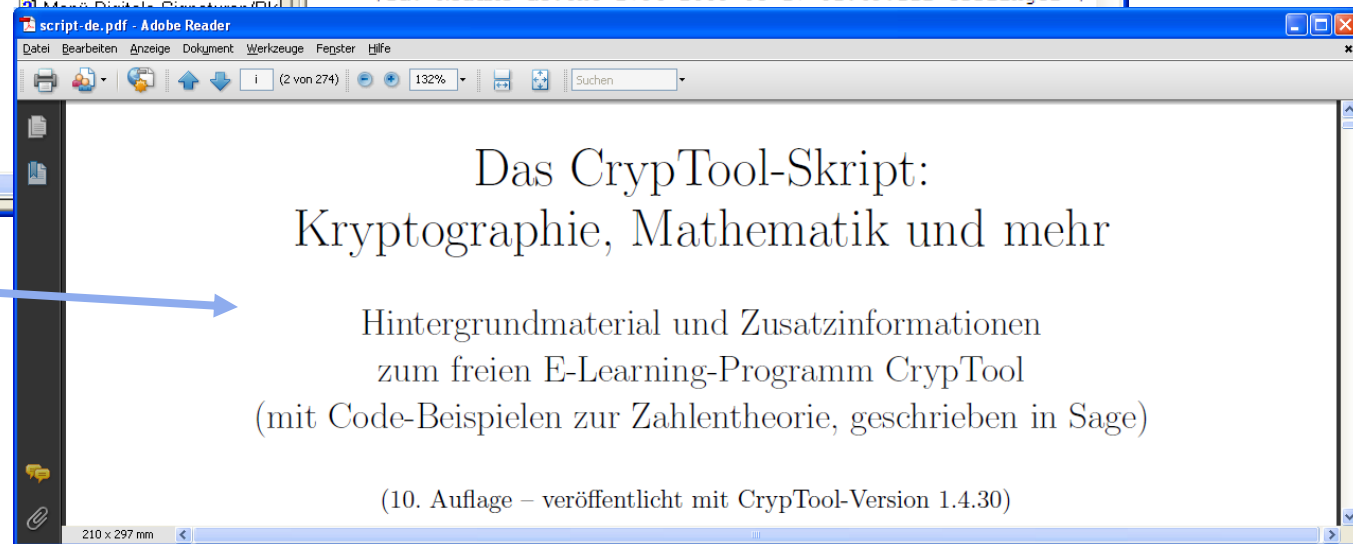
Online-Hilfe



Readme



Skript zu CrypTool



# Einführung in CrypTool

## Strukturierte Hilfe zu den Verfahren: F1 bei Menüeintrag

The screenshot shows the CrypTool 1.4.10 application window with the menu 'Ver-/Entschlüsseln' open, and the 'Hill...' option selected. A blue box labeled 'F1' points to this menu entry. Another blue box labeled 'Allgemeine Informationen zum Menüeintrag' points to the help window. The help window displays the 'Hill-Verschlüsselungsverfahren (Menü [Ver-/Entschlüsseln](#) \ Symmetrisch (klassisch))' page. A blue box labeled 'Verweis auf Dialog-Informationen' points to the 'Schlüssel für Hill Verschlüsselungsverfahren' link in the help text.

**CrypTool 1.4.10 - startbeispiel-de.txt**

File Edit View Ver-/Entschlüsseln Digitale Signaturen/PKI Einzelverfahren Analyse

Symmetrisch (klassisch) Symmetrisch (modern) Asymmetrisch Hybrid

Caesar / Rot-13... Vigenère... Hill... Substitution / Atbash...

**F1**

**Allgemeine Informationen zum Menüeintrag**

**Hilfe zu CrypTool 1.4.10**

Hide Back Forward Stop Refresh Home Print Options

Contents Index Search

**Hill-Verschlüsselungsverfahren (Menü [Ver-/Entschlüsseln](#) \ Symmetrisch (klassisch))**

Das Hill-[Verschlüsselungsverfahren](#) wurde 1929 von Lester Hill erfunden. Es war eines der ersten Verfahren, welche sich der Mathematik bedienten (lineare Abbildungen, die in Matrixform geschrieben werden können). Durch die Benutzung der Mathematik verspricht man sich ein Mehr an Sicherheit.

Das Hill-Verschlüsselungsverfahren benötigt einen Schlüssel und den Klartext. Auch der Schlüssel darf nur aus den Zeichen des Klartextalphabetes (siehe Dialog [Textoptionen](#)) bestehen. Außerdem ist der Schlüssel eine quadratische Matrix, d.h. die Matrix hat genauso viele Zeile wie Spalten. Diese Anzahl bezeichnet man auch als Dimension der Matrix. Der Schlüssel muss im Dialog [Schlüssel für Hill Verschlüsselungsverfahren](#) eingegeben werden.

Der [Klartext](#) wird in Blöcke gleicher Größe (ein Block besteht aus so vielen Zeilen, wie der Schlüssel Zeilen hat) unterteilt.

Der letzte Block besteht unter Umständen aus zu wenigen Zeichen: In diesem Fall wird auf die Länge der Matrixdimension aufgefüllt -- und zwar standardmäßig mit den kleinsten Zeichen des benutzten Alphabets (das muss nicht das Zeichen mit dem kleinsten [ASCII](#)-Wert sein, z.B. wenn das Alphabet folgendermaßen definiert ist:

# Einführung in CrypTool

## Strukturierte Hilfe zu den Verfahren: F1 bei geöffnetem Dialog

The screenshot shows the CrypTool 1.4.10 interface. The main window is titled "CrypTool 1.4.10 - startbeispiel-de.txt". A dialog box titled "Schlüssel eingabe: Hill" is open, showing the Hill cipher settings. The dialog includes a description of the Hill cipher, a list of used alphabet characters (A-Z), a grid for the Hill key matrix (5x5), and buttons for "Verschlüsseln", "Entschlüsseln", "Hill-Optionen", and "Textoptionen".

A callout box labeled "F1" points to the F1 key on the keyboard. Another callout box labeled "Informationen zur Dialogbedienung" points to the "Hilfe zu CrypTool 1.4.10" window. This window shows the "Dialog Schlüssel eingabe: Hill" in the "Contents" list, with a link to "Hilfe zu CrypTool 1.4.10".

The "Hilfe zu CrypTool 1.4.10" window contains the following text:

**Dialog Schlüssel eingabe: Hill**

Sie erreichen diesen Dialog über den Menüeintrag [Ver-/Entschlüsseln \ Symmetrisch \ Hill](#).

In diesem Dialog wird der [Schlüssel](#) für das [Hill-Verschlüsselungsverfahren](#) eingegeben.

Nachdem Sie im Feld **Dimension** die Größe des Schlüssels ausgewählt und den Schlüssel eingegeben haben, können Sie das [Dokument verschlüsseln](#), indem Sie den Knopf **Verschlüsseln** klicken oder die **Eingabetaste** betätigen. Wenn Sie das [entschlüsseln](#) wollen, wählen Sie den Knopf **Entschlüsseln**.

Mit dem Knopf können Sie einen im [Schlüsselspeicher](#) gespeicherten Schlüssel direkt einfügen (falls der Knopf blass dargestellt ist, steht für dieses Verfahren kein Schlüssel im Schlüsselspeicher).

Es kann vorkommen, dass der eingegebene Schlüssel nicht zu verwenden ist. Dies ist der Fall, wenn die dem Schlüssel entsprechende Matrix nicht invertierbar ist. In diesem Fall erscheint ein Meldungsfenster "Schlüssel nicht zu verwenden". Dann muss ein anderer Schlüssel gewählt werden.

Das benutzte Alphabet können Sie über den Button **Textoptionen** einstellen.

# Einführung in CrypTool

## Szenarien: Hilfe zum Einstieg

The screenshot shows the CrypTool 1.4.10 help window. The title bar reads 'Hilfe zu CrypTool 1.4.10'. The menu bar includes 'Hide', 'Back', 'Forward', 'Stop', 'Refresh', 'Home', 'Print', and 'Options'. The left sidebar contains a 'Contents' pane with a tree view of the help topics. The main content area displays the 'Szenario für das Triple DES-Verschlüsselungsverfahren im CBC-Modus'. The text describes the scenario for Triple DES encryption in CBC mode, mentioning the use of a text document and the encryption process. It also includes a section for loading the help text 'Wie Sie starten' from the file 'CrypTool-de.txt'. Below the text, there are two inset windows: 'CrypTool.txt' showing the introduction to the program, and 'ASCII Histogramm von <CrypTool> (1191 Zeichen)' showing a frequency distribution of characters.

**Szenario für das Triple DES-Verschlüsselungsverfahren im CBC-Modus**

Im folgenden wird ein [Szenario](#) für das [Triple DES Verschlüsselung](#) im [CBC-Modus](#) vorgestellt. Die Veranschaulichung durch viele Bildschirmfotos erleichtert das Nachvollziehen der mit [CrypTool](#) durchgeführten Schritte.

Anhand eines [Textdokuments](#) wird die [Verschlüsselung](#) und die [Entschlüsselung](#) mittels des [Triple DES Verfahrens](#) im [CBC-Modus](#) vorgestellt. Außerdem wird anhand der [Häufigkeitsverteilung](#) und der [Autokorrelation](#) der Buchstaben im verschlüsselten [Dokument](#) gezeigt, dass ein Angriff auf das [Triple DES Verschlüsselung](#) im [CBC-Modus](#) schwieriger ist als ein Angriff auf die klassischen [Verschlüsselungsverfahren](#), siehe dazu beispielsweise die [Szenarien](#) für das [Cäsar Verschlüsselungsverfahren](#) oder die [Verschlüsselung](#) durch [binäre Addition](#). Es besteht die Möglichkeit, einen kurzen [Schlüssel](#) durch einen [Brute-Force Angriff](#) zu finden. Dies gilt ebenfalls, wenn man die Menge, aus der der [Schlüssel](#) stammt, nicht sehr viele Schlüssel enthält.

Zuerst laden wir einen Teil des Hilfetextes "Wie Sie starten" zu [CrypTool](#), welcher sich in der [Datei](#) `CrypTool-de.txt` befindet. Dieses [Dokument](#) wird in CrypTool (über das Menü [Datei](#) \ [Öffnen](#)) geöffnet.

**CrypTool.txt**

CrypTool ist ein Programm, mit dessen Hilfe Sie kryptografische Verfahren anwenden und analysieren können. So können Sie neue Dokumente erstellen und bestehende Dokumente öffnen und weiter bearbeiten.

Ein Dokument kann mittels verschiedener Verschlüsselungsverfahren ver- und entschlüsselt werden. Es stehen sowohl klassische (zum Beispiel das Caesar-Verschlüsselungsverfahren) als auch moderne Verschlüsselungsverfahren (beispielsweise das RSA- und das DES-Verfahren sowie auf elliptischen Kurven basierende Verfahren) zur Verfügung. Eine Übersicht über alle Verschlüsselungsverfahren in CrypTool findet man auf der Hilfeseite zum Menü [Ver-/Entschlüsseln](#).

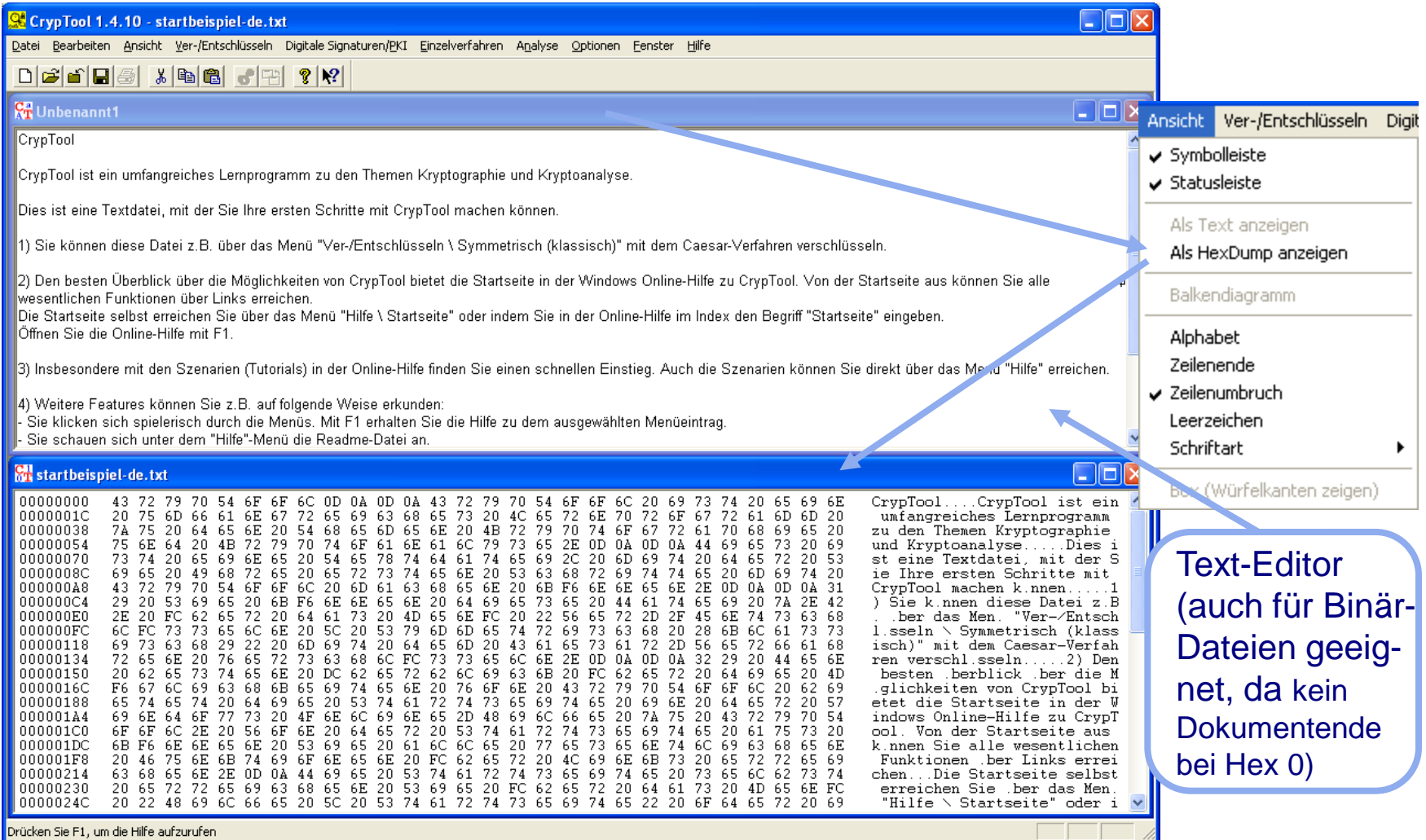
Bevor das [Dokument verschlüsselt](#) wird, werfen wir (über das [Menü Analyse \ Allgemein \ Histogramm](#)) einen Blick auf die [Häufigkeitsverteilung](#) der Zeichen, das [Histogramm](#).

**ASCII Histogramm von <CrypTool> (1191 Zeichen)**

Häufigkeit [%]

# Einführung in CrypTool


## Dokumentansicht: Textansicht / HexDump-Ansicht





# Einführung in CrypTool

## Zusatzprogramme – Interaktives Skript für Zahlentheorie

 ZT

Rechner Navigation Verzeichnisse Hilfe

### 1.1 Teilbarkeit

Seite 1 von 21

**Definition:** Seien  $d, n \in \mathbb{IN}$ . (Blauer Text reagiert auf die Maus.)

- $d$  ist ein **Teiler** von  $n$ , wenn eine Zahl  $z \in \mathbb{IN}$  existiert mit  $d \cdot z = n$ .
- Ist  $d$  ein Teiler von  $n$ , dann heißt  $\frac{n}{d}$  **Komplementärteiler** zu  $d$ .

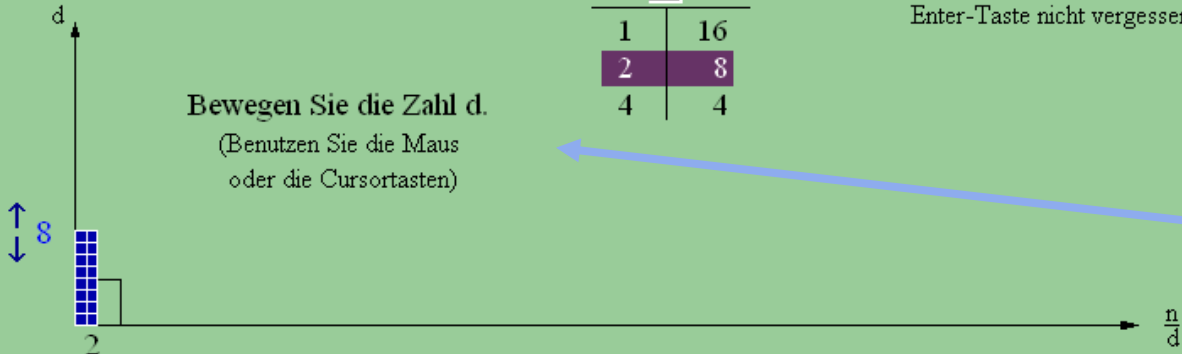
Auf der Suche nach Teilern von  $n$  muss man nur die Teiler  $\leq \sqrt{n}$  bestimmen, die übrigen Teiler sind deren Komplementärteiler.

Beispiel: Paare komplementärer Teiler von  $n = 16$


Sie können  $n$  neu eingeben.  
Enter-Taste nicht vergessen!

1	16
2	8
4	4

Bewegen Sie die Zahl  $d$ .  
(Benutzen Sie die Maus oder die Cursortasten)



Die Anzahl der Teiler ist bei Quadratzahlen ungerade, weil ein Teiler "doppelt auftritt", bei allen anderen Zahlen gerade.

(Go on to the next page.)

Interaktive  
Übungen.  
Beispiel: Paare  
komplementärer  
Teiler von  $n = 16$



# Einführung in CryptTool

## Zusatzprogramme – Visualisierung Elliptischer Kurven mit Punktaddition

**Punktaddition auf Elliptischen Kurven über den reellen Zahlenraum R**

$y^2 = x^3 - 10,00x + 15,00$

$a = -10,00$   $b = 15,00$  Zoom:  $2 * P$   $P + Q$  Lösche Punkte Log-Datei

**Wählen Sie den Zahlenraum**

☒ Reeller Zahlenraum R  
☐ Diskrete Gruppe über Fp

Dieses Programm visualisiert verschiedene Elliptische Kurven und ermöglicht es, Punktadditionen auf diesen durchzuführen. Die Kurven können entweder über dem Zahlenraum der reellen Zahlen oder über der diskreten Gruppe über Primzahlen zwischen 3 und 97 erzeugt werden. Die Kurvenparameter a und b können Sie mit den Reglern verändern.

Die Gerade durch die Punkte P und Q schneidet die Kurve im Punkt -R. Die Spiegelung von -R an der x-Achse ist der Punkt R. R ist das Ergebnis der Addition von P und Q.

**P = (4,05/6,38)**  
**Q = (-0,41/4,36)**  
**R = (-3,43/2,99)**

**Hilfe zu CryptTool 1.4.30**

Show Back Forward Stop Refresh Home Print Options

**Punktaddition auf einer Elliptischen Kurve (Menü Einzelverfahren \ Zahlentheorie interaktiv)**

Dieses Programm visualisiert verschiedene Elliptische Kurven und ermöglicht es, Punktadditionen auf diesen durchzuführen. Die Kurven können entweder über dem Zahlenraum der reellen Zahlen oder über der diskreten Gruppe über Primzahlen zwischen 3 und 97 erzeugt werden. Wenn Sie das amodale Fenster mit den Log-Ausgaben öffnen, können Sie Ihre Aktionen (z.B. fortgesetzte Additionen) parallel verfolgen.

**Log-Datei: Punktaddition auf Elliptischen Kurven**


----- Berechnung im reellen Zahlenraum R -----

Gewählte Kurve:  
 $y^2 = x^3 - 10,00x + 15,00$

# Einführung in CryptTool


## Zusatzprogramme – Zahlenhai-Spiel

**Zahlenhai - Version 1.1.0**



Shell square (blue means: free to choose; red means: already used)

1-20



Einstellungen für ein neues Spiel

Zahlenvorrat von 1 bis:

Jetzt kannst Du Dir und mit dem Spiel b

Bei 20 Zahlen werden insgesamt 210 Punkte an den Zahlenhai und an Dich ve


**Zahlenhai - Version 1.1.0**

Spielverlaufstabelle [ In der Tabelle sind die Primzahlen mit "(prim)" markiert ]

Zug	Deine Zahlen	Zahlenhai-Zahlen	Deine Punkte	Hai-Punkte	Rest-Zahlen
1	19(prim)	1	19	1	18
2	0	17(prim)	19	18	17
3	0	13(prim)	19	31	16
4	0	11(prim)	19	42	15
5	9	3(prim)	28	45	13
6	6	2(prim)	34	47	11
7	12	4	46	51	9
8	14	7(prim)	60	58	7
9	15	5(prim)	75	63	5
10	16	8	91	71	3
11	20	10	111	81	1
12	0	18	111	99	0

Shell square (blue means: free to choose; red means: already used)

1-20



000:00

Spielregeln

Hilfe

Verstrichene

02:17

Haifutter

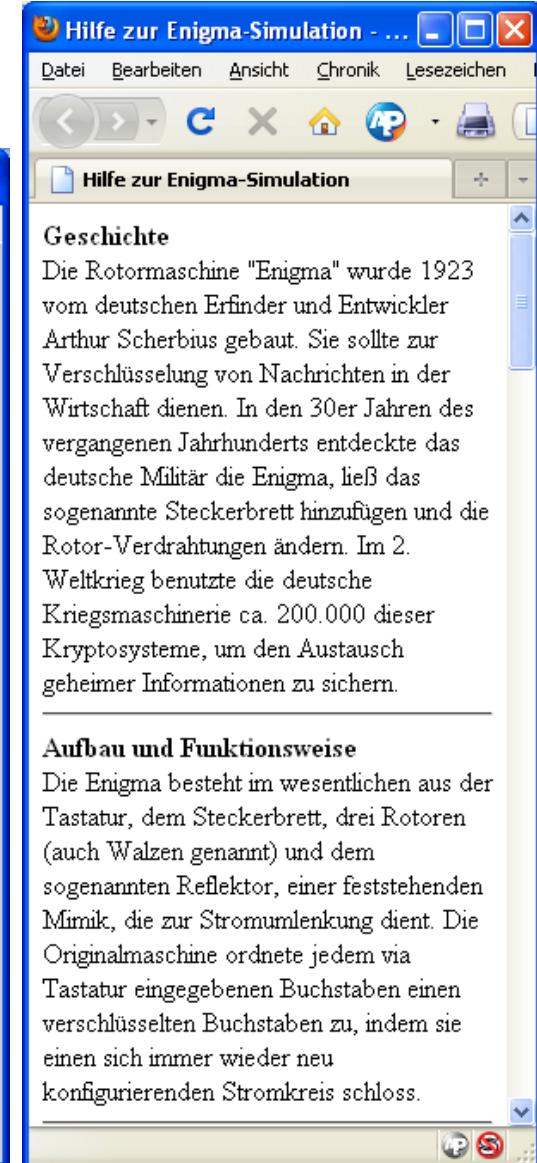
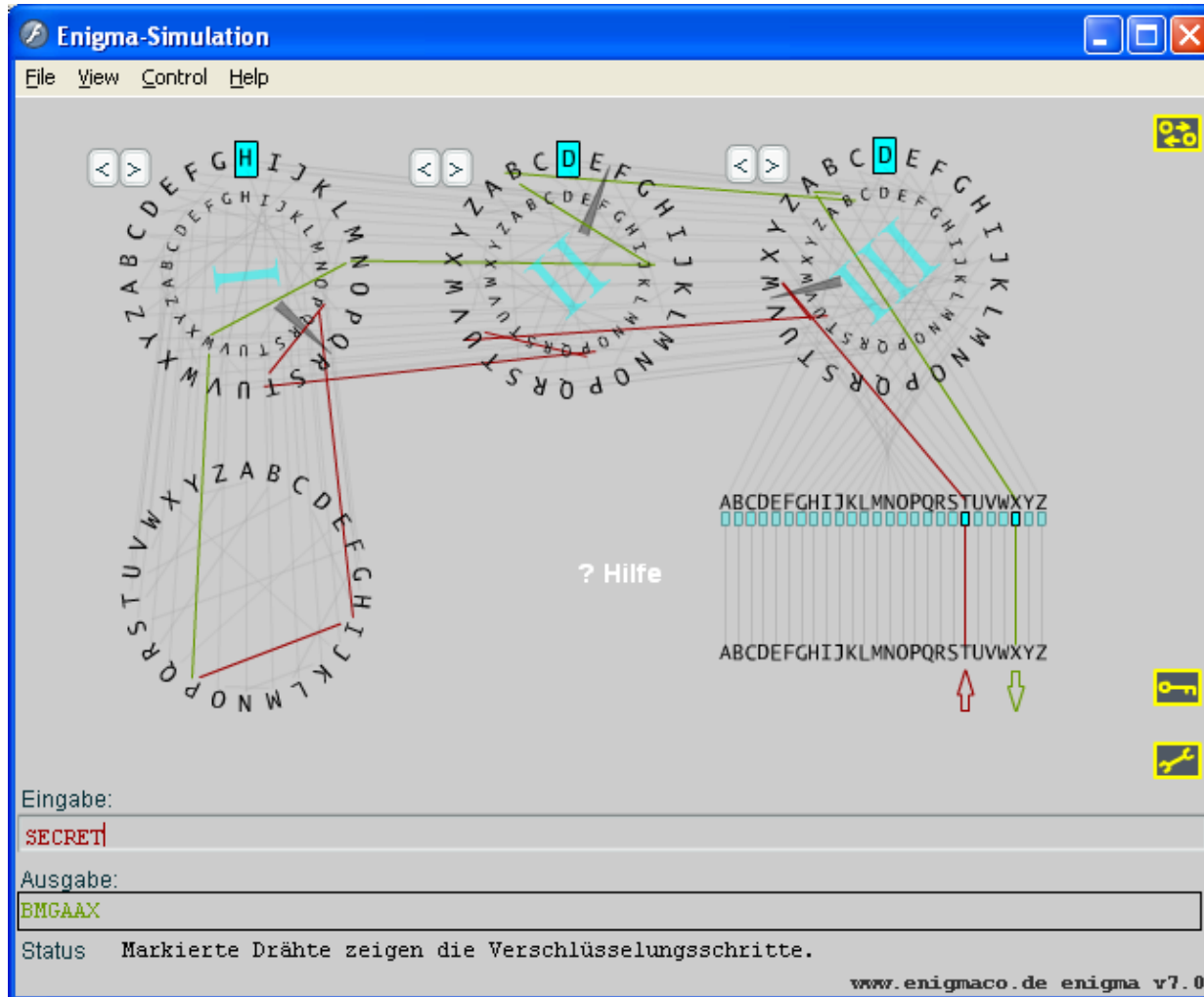
Weitere Möglichkeiten

Neues Spiel

Beenden

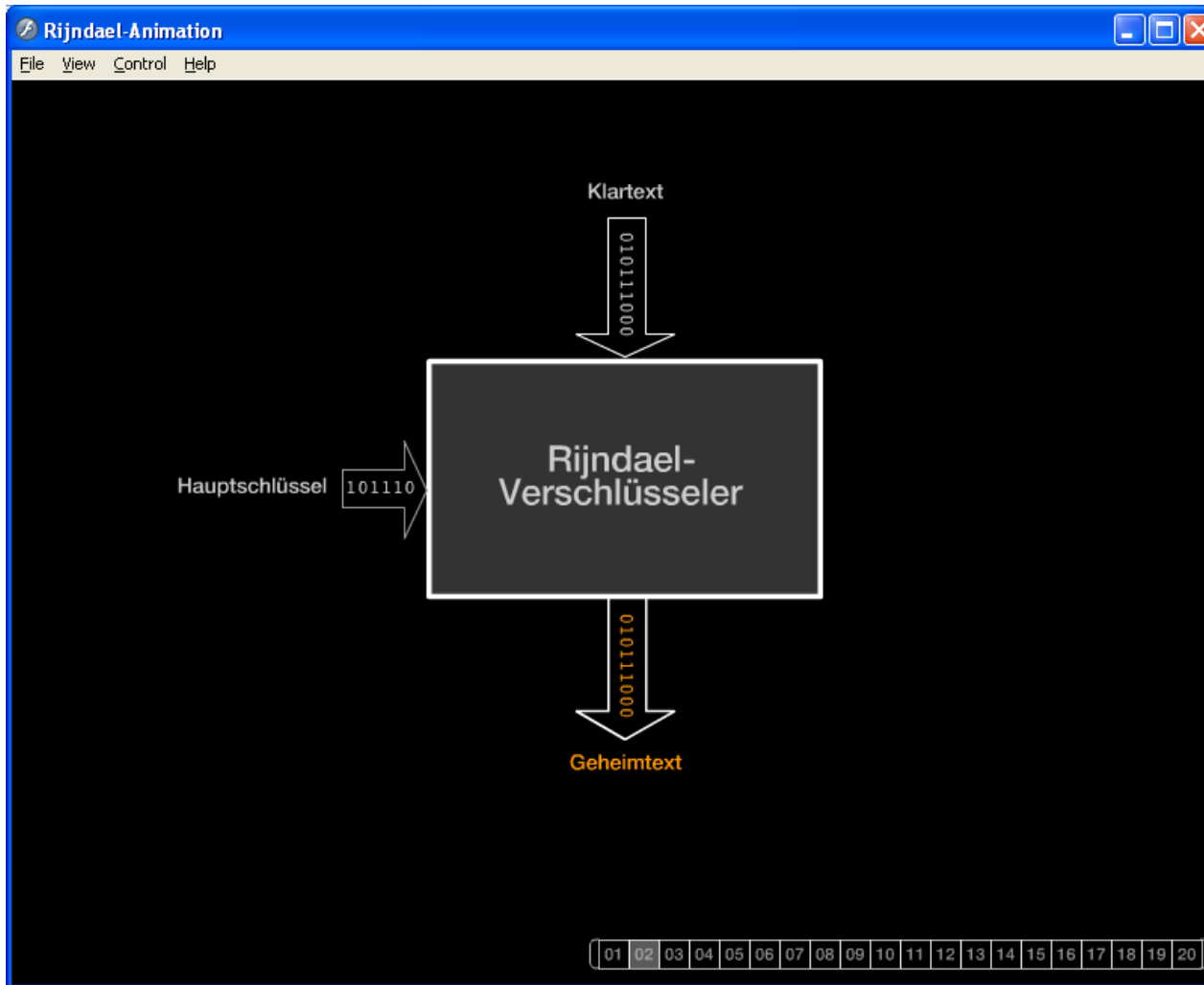
# Einführung in CryptTool

## Zusatzprogramme – Enigma-Simulation



# Einführung in CrypTool

## Zusatzprogramme – AES-Verschlüsselung



**Hilfe zu CrypTool 1.4.30**

**Rijndael-Animation (Menü Einzelverfahren \ Visualisierung von Algorithmen \ AES)**

Dieses Flash-Programm visualisiert die Details des AES-Algorithmus für einen fest gewählten Datensatz. Im Gegensatz dazu können Sie mit dem [Rijndael-Inspector](#) die Daten frei wählen.

[AES](#) ist der aktuelle Standard moderner symmetrischer Verschlüsselungsverfahren.

Der AES ist ein standardisierter Spezialfall des Rijndael-Verschlüsselungsverfahrens, das mit variabler Blocklänge für die Daten (insbesondere 128 Bit) und mit variabler Schlüssellänge (128, 192 und 256 Bit) arbeitet.

In der Visualisierung von Enrique Zabala wird das AES-Verfahren mit der Animationssoftware Flash demonstriert. Dabei werden fest vorgegebene Daten verwendet. Sowohl die Klartextnachricht (in der Spezifikation "state" genannt) als auch der benutzte Hauptschlüssel haben eine Länge von jeweils 128 Bit (= 16 Byte).

Die Animation zeigt dann schrittweise die Weiterverarbeitung: sowohl den eigentlichen, auf den Datenblock angewandten Verschlüsselungsprozess, als auch den Prozess der Generierung der Teilschlüssel aus dem Hauptschlüssel.

**Input**

# Einführung in CryptTool

## Übersicht über die Funktionen (Menübaum)

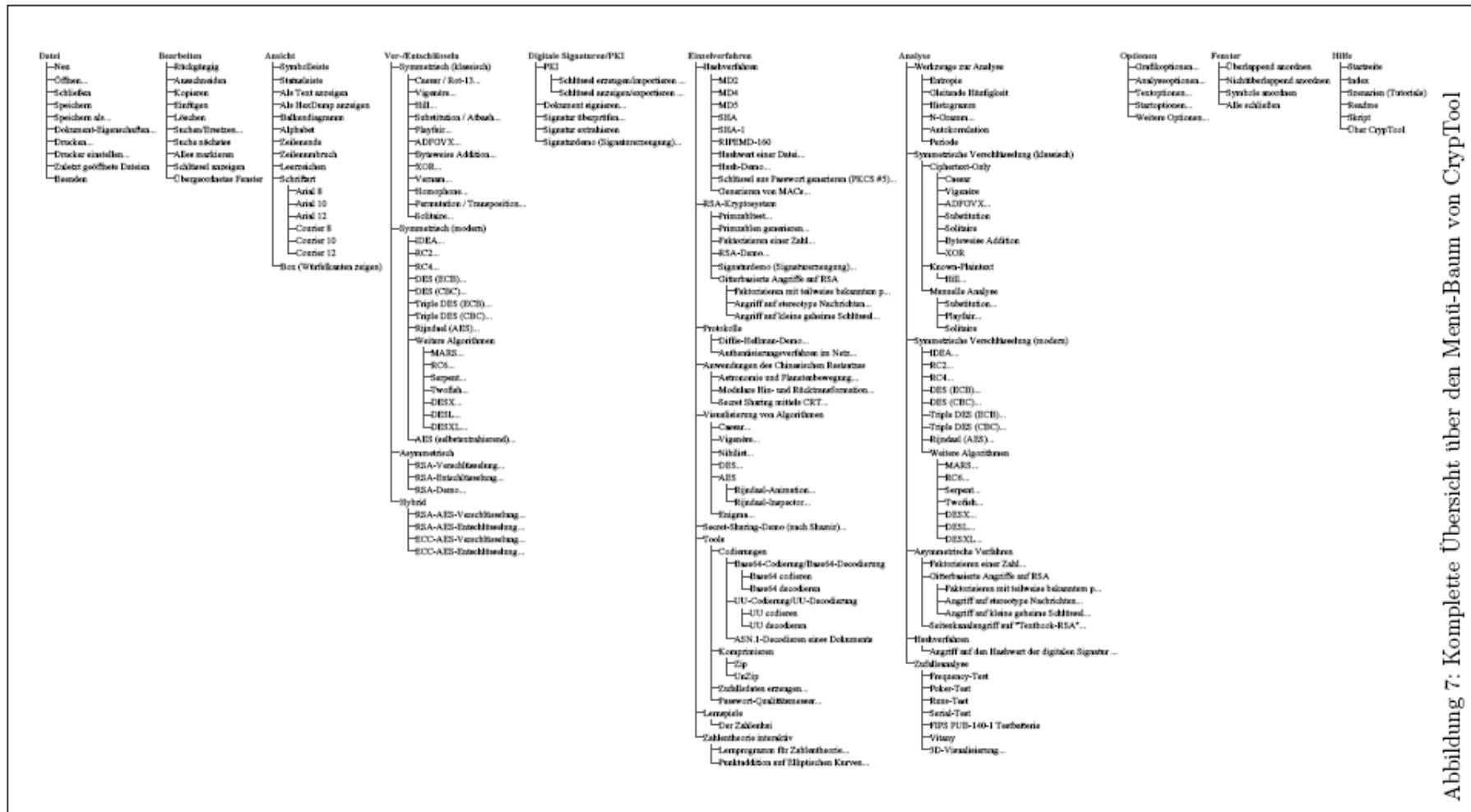


Abbildung 7: Komplette Übersicht über den Menü-Baum von CryptTool

Auszug aus dem CryptTool-Skript zu CT 1.4.20, Anhang A1, S. 203

# Einführung in CryptTool

## Gegenüberstellung von Funktion und zugehöriger Analyse in CryptTool (1)

### Kryptographie

#### Verschlüsselungsklassiker

- Caesar
- Vigenère
- Hill
- Homophone Substitution
- Playfair
- ADFGVX
- Addition
- XOR
- Vernam
- Permutation
- Solitaire

#### Zum besseren Nachvollziehen von Literaturbeispielen ist

- Alphabet wählbar
- Behandlung von Leerzeichen etc. einstellbar

### Kryptoanalyse

#### Angriffe auf klassische Verfahren

- Ciphertext-only
  - Caesar
  - Vigenère
  - Addition
  - XOR
  - Substitution
  - Playfair
- Known-plaintext
  - Hill
- Manuell (unterstützt)
  - Monoalphabetische Substitution
  - Playfair
  - ADFGVX
  - Solitaire

#### Unterstützende Analyseverfahren

- Entropie, gleitende Häufigkeit
- Histogramm, n-Gramm-Analyse
- Autokorrelation
- Perioden
- Zufallszahlenanalyse
- Base64 / UU-Encode

# Einführung in CrypTool

## Gegenüberstellung von Funktion und zugehöriger Analyse in CrypTool (2)

### Kryptographie

#### Moderne symmetrische Verschlüsselung

- IDEA, RC2, RC4, RC6, DES, 3DES, DESX, DESL
- AES-Kandidaten der letzten Auswahlrunde (Serpent, Twofish, ...)
- AES (=Rijndael)
- DESL, DESXL

#### Asymmetrische Verschlüsselung

- RSA mit X.509-Zertifikaten
- RSA-Demonstration
  - zum Nachvollziehen von Literaturbeispielen
  - Alphabet und Blocklänge einstellbar

#### Hybridverschlüsselung (RSA + AES)

- visualisiert als interaktives Datenflussdiagramm

### Kryptoanalyse

#### Brute-force-Angriff auf symmetrische Algorithmen

- für alle Algorithmen
- Annahme:
  - Entropie des Klartextes klein oder teilweise Kenntnis der Schlüssels oder Kenntnis des Klartextalphabets.

#### Angriff auf RSA-Verschlüsselung

- Faktorisierung des RSA-Moduls
- Gitterreduktions-basierte Angriffe

#### Angriff auf Hybridverschlüsselung

- Angriff auf RSA oder
- Angriff auf AES (Seitenkanalangriff)



# Einführung in CrypTool

## Gegenüberstellung von Funktion und zugehöriger Analyse in CrypTool (3)

### Kryptographie

#### Digitale Signatur

- RSA mit X.509-Zertifikaten
  - Signatur zusätzlich visualisiert als interaktives Datenflussdiagramm
- DSA mit X.509-Zertifikaten
- Elliptic Curve DSA, Nyberg-Rueppel

#### Hashfunktionen

- MD2, MD4, MD5
- SHA, SHA-1, RIPEMD-160

#### Zufallsgeneratoren

- Secude
- $x^2 \bmod n$
- Linearer Kongruenzgenerator (LCG)
- Inverser Kongruenzgenerator (ICG)

### Kryptoanalyse

#### Angriff auf RSA-Signatur

- Faktorisierung des RSA-Moduls
- praktikabel bis ca. 250 bits bzw. 75 Dezimalstellen (auf Einzelplatz-PC)

#### Angriff auf Hashfunktion / digitale Signatur

- Generieren von Hash-Kollisionen für ASCII-Texte (Geburtsparadox) (bis 40 bit in etwa 5 min)

#### Analyse von Zufallsdaten

- FIPS-PUB-140-1 Test-Batterie
- Periode, Vitany, Entropie\*
- Gleitende Häufigkeit, Histogramm
- n-Gramm-Analyse, Autokorrelation
- ZIP-Kompressionstest

\* Wie alle Begriffe, ist auch **Entropie** in der Online-Hilfe zu CT erklärt:  
Siehe Hilfe zum Menüeintrag: „Analyse \ Werkzeuge zur Analyse \ Entropie des Dokuments berechnen“

# **Einführung in die Kryptologie mit CryptTool**

## **Übung Teil II – Klassische Verfahren**

**Workshop  
INFOS 2009**



[www.cryptool.com](http://www.cryptool.com)  
[www.cryptool.de](http://www.cryptool.de)  
[www.cryptool.org](http://www.cryptool.org)  
[www.cryptool.pl](http://www.cryptool.pl)

# Beispiele aus der klassischen Kryptographie

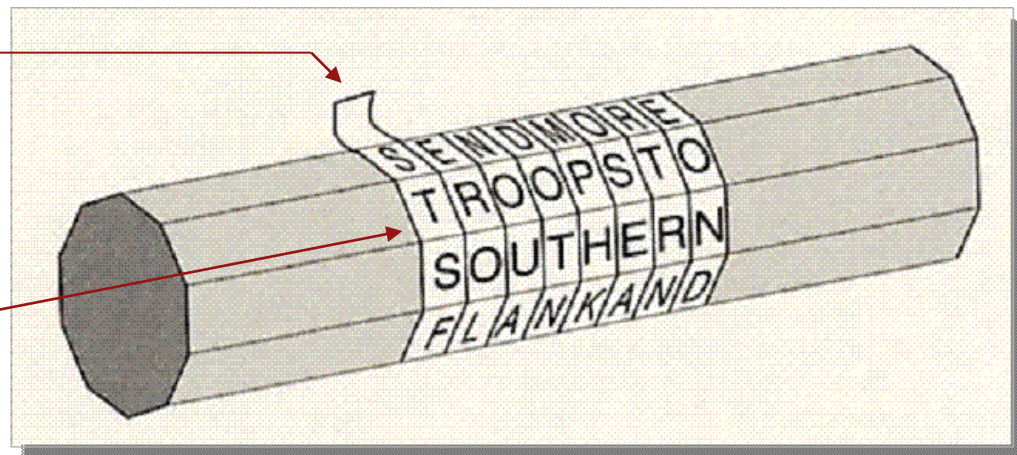
## Älteste bekannte Verschlüsselungsverfahren

- **Kahlgeschorener Sklave**
- **Atbash** (um 600 v. Chr.)
  - Hebräische Geheimschrift, umgedrehtes Alphabet
- **Skytale von Sparta** (etwa 500 v. Chr.)
  - Beschrieben vom griechischen Historiker/Schriftsteller Plutarch (45 - 125 n. Chr.)
  - Zwei Zylinder (Holzstäbe) mit gleichem Durchmesser
  - Transposition (Zeichen des Klartextes werden umsortiert)

Verschlüsselter Text (Chiffre)

Klartext

*„Send more troops to  
southern flank and ...“*



# Aufgabe 1:

**Analysieren von Chiffraten (Geheimtexten), erzeugt mit klassischen Verfahren**

## Vorarbeit:

- Öffnen Sie die Datei „deutsch.txt“ (Unterordner „Reference“).
- Stellen Sie sicher, dass das gewählte Alphabet nur aus Großbuchstaben besteht: „ABCDEFGHIJKLMNOPQRSTUVWXYZ“

## Aufgabe:

1. Bestimmen Sie für diese Datei das Histogramm, Digramm und Trigramm.
2. Verschlüsseln Sie das geöffnete Dokument mittels
  - Caesar (Schlüssel „K“)
  - Einfache Permutation (Schlüssel 4,2,3,1)
  - Vigenère (Schlüssel „VIGENERE“)
  - Hill (4x4-Schlüsselmatrix [C,S,T,T],[Y,R,U,B],[Z,E,E,D],[O,B,S,S])
  - Monoalphabetische Substitution (Schlüssel „SUBKEY“)
3. Bestimmen Sie für diese Chifftrat-Dateien das Histogramm, Digramm und Trigramm. Erklären Sie die Unterschiede in den Ergebnissen.
4. Wie kann man die einzelnen Verfahren „knacken“?

# CrypTool

## Unterschiedliche Chiffretexte – Histogramm / Digramm / Trigramm-Analyse

CrypTool 1.4.10 - Substitution-Verschlüsselung von <deutsch.txt>, Schlüssel <SUBKEYACDFGHIJLMNOPQRTVWXZ>

Datei Bearbeiten Ansicht Ver-/Entschlüsseln Digitale Signaturen/EKI Einzelverfahren Analyse Optionen Fenster Hilfe

deutsch.txt

Umsatzsteuergesetz (UStG)

Caesar-Verschlüsselung von <deutsch.txt>, Schlüssel <K>

Ewckdjcdoeobqocodj (ECdQ)

Permutations-/Transpositions-Verschlüsselung von <deutsch.txt>, Schlüssel <4,2,3,1 PARAMETER: 0>

Atresrrctegnndtsep (GHuT)

Vigenère-Verschlüsselung von <deutsch.txt>, Schlüssel <VIGENERE>

Puyegdjxzcvtijioh (AWgK)

Hill-Verschlüsselung von <deutsch.txt>, Schlüssel <CSTT YRUB ZEED OBSS>

Aewsvmcvnnmieqqoz (HNzF)

Substitution-Verschlüsselung von <deutsch.txt>, Schlüssel <SUBKEYACDFGHIJLMNOPQRTVWXZ>

Ripsqzpqereoaepqz (RPqA)

Eopqeo Supbcjdq  
Pqereoaeejpqsjk rjk Aehqrpaeoedbc

Msosaosmc 1.  
(1) Keo Ripsqzpqereo rjgeohdeaej kde ylhaejkej Ripseqze:  
1. kde Hdeyeorjaej rjk pljpqdaej Hedpqraej, kde edj Rjqeojecieo di Djhsjk aeaej Ejqaehq di Ocsiej pedjep  
Pqereousogedq ejqysehhq jdbcq, vejj  
s) keo Ripsqz sry Aorjk aepeqzhdbeo lkeo uecleokhdbceo Sjlokirja spraeqrecoq vdok lkeo jsbc aepeqz  
adhq lkeo  
u) edj Rjqeojecieo Hdeyeorjaej lkeo pljpqdaej Hedpqraej sj pedje Souedqjecieo lkeo keoej Sjaecleodae sry Aorjk kep Koejppreutseuqjopp  
sryrecoq, yreo kde kde Eimysejaeo keo Hdeyeorja lkeo pljpqdaej Hedpqra (Hedpqraeimeysejaeo) gedj ueplkeop ueoebcjqep Ejqaehq  
sryvejkej. Ksp adhq jdbcq yreo Sryeogpsigedqej;  
2. keo Edaejteouosrbc di Djhsjk. Edaejteouosrbc hdeaq tlo, vejj edj Rjqeojecieo  
s) Aaejpqssejke srp pedjei Rjqeojeciej yreo Zvebge ejajdiq, kde srßeocshu kep Rjqeojeciejp hdeaej,  
u) di Ocsiej pedjep Rjqeojeciejp pljpqdaej Hedpqraej keo dj Msosaosmc 3 Sup. 9 uezedbcjqej Soq yreo Zvebge sryrecoq, kde srßeocshu kep  
Rjqeojeciejp hdeaej,  
b) di Ocsiej pedjep Rjqeojeciejp Sryvejkrjaej qsedaq, kde rjgeo ksp Suzrpteoulq kep Msosaosmc 4 Sup. 5 Psqz 1 Jo. 1 udp 7 lkeo Sup. 7  
lkeo Msosaosmc 12 Jo. 1 keo Edieliajgareoqegat uehkei. Kep adhq idha yreo Aehkaehoeia rjk yreo Haeoqarieruueikraei, pkda

Drücken Sie F1, um die Hilfe aufzurufen

N-Gramm-Liste von Substitution-Verschlüsselung von <deutsch.txt>, Schlüss...

Auswahl

☐ Histogramm

☐ Digramm

☒ Trigramm

☐ 4 -Gramm

Anzeige der 26

häufigsten N-Gramme  
(erlaubte Werte: 1-5000).

Textoptionen

Liste berechnen

Liste speichern

Schließen

Nr.	Zeichen...	Häufigkeit in %	Häufigkeit
1	KED	2.0044	1714
2	RJA	1.7623	1507
3	KDE	1.3273	1135
4	AEJ	1.2045	1030
5	DBC	1.0840	927
6	EDJ	1.0490	897
7	REO	0.9800	838
8	JKE	0.8806	753
9	KEJ	0.8642	739
10	PQE	0.8443	722
11	RJK	0.7975	682
12	PBC	0.7133	610
13	JAE	0.7005	599
14	EJK	0.6911	591
15	YRE	0.6525	558
16	TEO	0.6502	556
17	KEP	0.6432	550
18	Q EJ	0.6233	533
19	DPQ	0.6163	527
20	ORJ	0.6116	523
21	OSA	0.6034	516
22	BCQ	0.5987	512
23	ERE	0.5742	491
24	BCE	0.5648	483
25	QEO	0.5473	468
26	QER	0.5391	461

# CrypTool

## Klartext

Histogrammanalyse				Digrammanalyse		Trigrammanalyse	
Nr.	Zeichen	Häufigkeit (n)	n*(n-1)	Digramm	Häufigkeit	Trigramm	Häufigkeit
1	E	20.952	438.965.352	ER	5356	DER	1714
2	N	13.092	171.387.372	EN	4598	UNG	1507
3	R	10.011	100.210.110	DE	3477	DIE	1135
4	I	8.144	66.316.592	UN	2635	GEN	1030
5	S	7.636	58.300.860	GE	2591	ICH	927
6	T	7.547	56.949.662	CH	2430	EIN	897
7	A	6.777	45.920.952	EI	2117	NDE	753
8	D	6.585	43.355.640	TE	2028	DEN	739
9	U	5.560	30.908.040	IE	1963	STE	722
10	G	5.138	26.393.906	ST	1949	UND	682
11	H	4.491	20.164.590	ND	1904	SCH	610
12	L	3.368	11.340.056	IN	1902	NGE	599
13	B	3.053	9.317.756	NG	1756	VER	556
14	M	2.869	8.228.292	ES	1520	DES	550
15	C	2.558	6.540.806	BE	1506	TEN	533
16	F	2.531	6.403.430	NE	1337	IST	527
17	O	2.070	4.282.830	RA	1286	RUN	523
18	Z	1.862	3.465.182	DI	1215	RAG	516
19	W	1.204	1.448.412	AN	1045	CHT	512
20	V	1.184	1.400.672	RE	944	EUE	486
21	P	1.183	1.398.306	IC	927	CHE	483
22	K	746	555.770	ME	903	UER	478
23	J	165	27.060	AU	834	TER	468
24	Q	5	20	LI	793	TEU	461
25	Y	3	6	IS	785	END	446
26	X	2	2	NT	757	ERU	405
<b>Friedman-Test</b>							
N	118.736		Textlänge				
A	1.113.281.676		Gesamtzahl aller Buchstabenpaare				
I	<b>0,078966682</b>		Koinzidenzindex		(I für Deutsche Sprache = 0,0762)		

# CrypTool

## Caesar-Verschlüsselung

Histogrammanalyse				Digrammanalyse		Trigrammanalyse	
Nr.	Zeichen	Häufigkeit (n)	n*(n-1)	Digramm	Häufigkeit	Trigramm	Häufigkeit
1	O	20.952	438.965.352	OB	5356	NOB	1714
2	X	13.092	171.387.372	OX	4598	EXQ	1507
3	B	10.011	100.210.110	NO	3477	NSO	1135
4	S	8.144	66.316.592	EX	2635	QOX	1030
5	C	7.636	58.300.860	QO	2591	SMR	927
6	D	7.547	56.949.662	MR	2430	OSX	897
7	K	6.777	45.920.952	OS	2117	XNO	753
8	N	6.585	43.355.640	DO	2028	NOX	739
9	E	5.560	30.908.040	SO	1963	CDO	722
10	Q	5.138	26.393.906	CD	1949	EXN	682
11	R	4.491	20.164.590	XN	1904	CMR	610
12	V	3.368	11.340.056	SX	1902	XQO	599
13	L	3.053	9.317.756	XQ	1756	FOB	556
14	W	2.869	8.228.292	OC	1520	NOC	550
15	M	2.558	6.540.806	LO	1506	DOX	533
16	P	2.531	6.403.430	XO	1337	SCD	527
17	Y	2.070	4.282.830	BK	1286	BEX	523
18	J	1.862	3.465.182	NS	1215	BKQ	516
19	G	1.204	1.448.412	KX	1045	MRD	512
20	F	1.184	1.400.672	BO	944	OEO	486
21	Z	1.183	1.398.306	SM	927	MRO	483
22	U	746	555.770	WO	903	EOB	478
23	T	165	27.060	KE	834	DOB	468
24	A	5	20	VS	793	DOE	461
25	I	3	6	SC	785	OXN	446
26	H	2	2	XD	757	OBE	405
<b>Friedman-Test</b>							
N	118.736		Textlänge				
A	1.113.281.676		Gesamtzahl aller Buchstabenpaare				
I	<b>0,078966682</b>		Koinzidenzindex				



# CrypTool

## Permutations-Verschlüsselung

Histogrammanalyse				Digrammanalyse				Trigrammanalyse	
Nr.	Zeichen	Häufigkeit (n)	n*(n-1)		Digramm	Häufigkeit		Trigramm	Häufigkeit
1	E	20.952	438.965.352	1	EN	2322		ENE	417
2	N	13.092	171.387.372	2	NE	2252		ESE	343
3	R	10.011	100.210.110	3	EE	2054		NNE	327
4	I	8.144	66.316.592	4	ER	1883		NEN	275
5	S	7.636	58.300.860	5	SE	1560		ETE	269
6	T	7.547	56.949.662	6	ES	1461		ERE	258
7	A	6.777	45.920.952	7	RE	1451		TER	256
8	D	6.585	43.355.640	8	TE	1381		EUN	246
9	U	5.560	30.908.040	9	ET	1273		PGH	245
10	G	5.138	26.393.906	10	DE	1209		INE	231
11	H	4.491	20.164.590	11	IN	1142		NER	218
12	L	3.368	11.340.056	12	NN	1090		ENN	211
13	B	3.053	9.317.756	13	EU	981		URM	207
14	M	2.869	8.228.292	14	EG	937		NEE	205
15	C	2.558	6.540.806	15	EI	903		IRE	197
16	F	2.531	6.403.430	16	RA	901		EEN	196
17	O	2.070	4.282.830	17	IE	885		EEE	194
18	Z	1.862	3.465.182	18	ND	870		REN	185
19	W	1.204	1.448.412	19	IR	847		ARA	179
20	V	1.184	1.400.672	20	AE	815		ERA	172
21	P	1.183	1.398.306	21	LE	804		EIN	170
22	K	746	555.770	22	NS	782		TEN	167
23	J	165	27.060	23	NR	740		NSE	158
24	Q	5	20	24	ED	727		SEE	157
25	Y	3	6	25	EH	726		EDE	156
26	X	2	2	26	EA	722		ENA	153
<b>Friedman-Test</b>									
N	118.736		Textlänge						
A	1.113.281.676		Gesamtzahl aller Buchstabenpaare						
I	<b>0,078966682</b>		Koinzidenzindex						

# CrypTool

## Vigenère-Verschlüsselung

Histogrammanalyse				Digrammanalyse		Trigrammanalyse	
Nr.	Zeichen	Häufigkeit (n)	n*(n-1)	Digramm	Häufigkeit	Trigramm	Häufigkeit
1	I	12.174	148.194.102	II	1543	JIE	252
2	V	9.933	98.654.556	IE	1435	HRV	238
3	R	8.985	80.721.240	VV	1132	QII	233
4	M	7.899	62.386.302	VR	1091	LRB	221
5	Z	6.699	44.869.902	KV	1078	LKV	218
6	K	6.014	36.162.182	RV	1035	PVM	218
7	E	5.646	31.871.670	IM	997	UIM	218
8	X	5.265	27.714.960	MI	953	HZZ	215
9	Y	4.778	22.824.506	KR	930	YMX	205
10	H	4.064	16.512.032	RR	924	HRX	201
11	A	4.044	16.349.892	MX	846	CTK	200
12	W	3.795	14.398.230	IA	824	HVV	196
13	J	3.614	13.057.382	HR	819	MIM	193
14	L	3.537	12.506.832	MT	810	VMI	192
15	T	3.463	11.988.906	ZZ	791	YAK	192
16	G	3.408	11.611.056	ZV	739	YEK	184
17	Q	3.395	11.522.630	JI	675	YIO	177
18	O	3.136	9.831.360	ZI	675	OKR	168
19	P	2.857	8.159.592	QI	656	ART	165
20	N	2.837	8.045.732	YM	654	III	158
21	F	2.670	7.126.230	IL	646	BMT	157
22	D	2.248	5.051.256	HV	629	KRR	157
23	U	2.236	4.997.460	YI	610	YMT	153
24	B	2.114	4.466.882	HZ	579	YQK	153
25	C	2.008	4.030.056	PV	536	JMR	150
26	S	1.917	3.672.972	UI	536	KVR	148
<b>Friedman-Test</b>							
N	118.736		Textlänge				
A	716.727.920		Gesamtzahl aller Buchstabenpaare		PW-Längen-Schätzung	3,055411584	
I	<b>0,05083855</b>		Koinzidenzindex			(Echte Länge = 8)	

# CrypTool

## Hill-Verschlüsselung

Histogrammanalyse				Digrammanalyse		Trigrammanalyse	
Nr.	Zeichen	Häufigkeit (n)	n*(n-1)	Digramm	Häufigkeit	Trigramm	Häufigkeit
1	N	5.271	27.778.170	AD	404	TQF	204
2	F	5.240	27.452.360	NM	397	SLA	143
3	A	4.853	23.546.756	NN	386	XEB	133
4	P	4.809	23.121.672	CX	374	BAD	129
5	B	4.796	22.996.820	OA	360	ADC	128
6	O	4.752	22.576.752	FS	351	NNM	127
7	X	4.743	22.491.306	NO	346	NNN	127
8	E	4.737	22.434.432	TQ	339	PNO	123
9	S	4.727	22.339.802	QF	332	AEW	122
10	L	4.711	22.188.810	OS	331	WTQ	120
11	R	4.644	21.562.092	FX	324	USL	117
12	D	4.634	21.469.322	SL	321	CXE	115
13	T	4.580	20.971.820	XE	320	PAO	113
14	C	4.559	20.779.922	LA	317	AOA	110
15	Z	4.551	20.707.050	VH	311	NOA	109
16	V	4.525	20.471.100	BA	308	VHK	107
17	H	4.482	20.083.842	BE	306	RGN	105
18	K	4.450	19.798.050	YB	302	AVH	104
19	Y	4.405	19.399.620	DZ	301	DZG	104
20	W	4.331	18.753.230	QP	301	EJI	103
21	M	4.269	18.220.092	FW	299	FYM	103
22	G	4.257	18.117.792	WT	296	ZFY	103
23	J	4.232	17.905.592	LR	291	NMK	101
24	Q	4.173	17.409.756	PN	291	VKN	101
25	I	4.084	16.674.972	AO	285	JTQ	100
26	U	3.921	15.370.320	OR	285	WRG	100
<b>Friedman-Test</b>							
N	118.736		Textlänge				
A	544.621.452		Gesamtzahl aller Buchstabenpaare				
I	<b>0,038630789</b>		Koinzidenzindex				

# CrypTool

## Substitutions-Verschlüsselung

Histogrammanalyse				Digrammanalyse		Trigrammanalyse	
Nr.	Zeichen	Häufigkeit (n)	n*(n-1)	Digramm	Häufigkeit	Trigramm	Häufigkeit
1	E	22.892	524.020.772	EO	5938	KEO	1714
2	J	13.092	171.387.372	EJ	4839	RJA	1507
3	O	10.011	100.210.110	KE	3477	KDE	1135
4	D	8.144	66.316.592	RJ	2635	AEJ	1030
5	P	7.636	58.300.860	AE	2591	DBC	927
6	S	7.566	57.236.790	BC	2430	EDJ	897
7	Q	7.547	56.949.662	ED	2120	REO	838
8	K	6.585	43.355.640	QE	2028	JKE	753
9	R	6.482	42.009.842	DE	1963	KEJ	739
10	A	5.138	26.393.906	PQ	1949	PQE	722
11	C	4.491	20.164.590	JK	1904	RJK	682
12	H	3.368	11.340.056	DJ	1902	PBC	610
13	U	3.053	9.317.756	JA	1756	JAE	599
14	I	2.869	8.228.292	EP	1585	EJK	591
15	B	2.558	6.540.806	UE	1506	YRE	558
16	Y	2.531	6.403.430	RE	1413	TEO	556
17	L	2.299	5.283.102	OS	1378	KEP	550
18	Z	1.862	3.465.182	JE	1337	QEJ	533
19	V	1.204	1.448.412	KD	1215	DPQ	527
20	T	1.184	1.400.672	SJ	1045	ORJ	523
21	M	1.183	1.398.306	EQ	963	OSA	516
22	G	746	555.770	OE	944	BCQ	512
23	F	165	27.060	DB	927	ERE	491
24	N	5	20	IE	903	BCE	483
25	X	3	6	EC	841	QEO	468
26	W	2	2	SR	834	QER	461
<b>Friedman-Test</b>							
N	122.616		Textlänge				
A	1.221.755.008		Gesamtzahl aller Buchstabenpaare				
I	<b>0,081263099</b>		Koinzidenzindex				

# CrypTool

## Caesar – Histogramm-Analyse

**CrypTool 1.4.10 - ASCII-Histogramm von <CIPHER1\_deutsch.txt> (32788 Zeichen)**

Datei Bearbeiten Ansicht Ver-/Entschlüsseln Digitale Signaturen/PKI Einzelverfahren Analyse Optionen Fenster Hilfe

ASCII-Histogramm von <CIPHER1\_deutsch.txt> (32788 Zeichen)

ASCII-Histogramm von <CIPHER1\_deutsch.txt> (32788 Zeichen)

Häufigkeit (%)

Buchstabe	Häufigkeit (%)
A	0.5
C	7.5
E	6.5
G	6.5
I	4.0
K	1.5
M	6.5
O	16.0
Q	3.0
S	8.5
U	4.0
W	10.0

Caesar-Entschlüsselung von <CIPHER1\_deutsch.txt>, Schlüssel <K>

Naturraum

Hauptartikel: Geographie der Vereinigten Staaten

Die Vereinigten Staaten bestehen aus 50 Bundesstaaten, wobei Alaska und Hawaii außerhalb des Kernlandes (continental U.S.) liegen. Alaska und Hawaii sowie die politisch angeschlossenen Außengebiete (beispielsweise Puerto Rico und Guam) liegen außerhalb dieser Zone.

Das Kernland umfasst 48 der 50 Bundesstaaten sowie den District of Columbia (Bundesdistrikt), die innerhalb einer gemeinsamen Grenze liegen (sog. „lower 48“). Es liegt zwischen dem 24. und 49. nördlichen Breitengrad und zwischen dem 68. und 125. westlichen Längengrad und ist in vier

Drücken Sie F1, um die Hilfe aufzurufen

**Schlüsseleingabe: Caesar / ROT-13**

Beschreibung

Hier können Sie für das Caesar-Verfahren den Schlüssel eingeben. Caesar ist eine monoalphabetische Substitution, bei der die Zeichen des Klartext-Alphabets durch Shiften um einen bestimmten Wert auf das Geheimtext-Alphabet abgebildet werden. Dieser Verschiebewert ist der Schlüssel. Sie können den Schlüssel sowohl als Zahl als auch als einzelnes Alphabet-Zeichen eingeben.

Rot-13 ist ein Spezialfall, bei dem der Schlüssel fest auf den Wert der halben Länge des Klartext-Alphabets gesetzt wird. Diese Variante ist nur wählbar, wenn die Länge des Alphabets eine gerade Zahl ist.

Variante auswählen

☒ Caesar

☐ Rot-13

Optionen zur Interpretation des Alphabetszeichens

☒ Wert des ersten Alphabetzeichens = 0 (z.B. "A"=0)

☐ Wert des ersten Alphabetzeichens = 1 (z.B. "A"=1)

Schlüsseleingabe

☒ Alphabetzeichen

☐ Zahlenwerte

Informationen zur Verschlüsselung

Verschiebung um 10

Das Alphabet (26 Zeichen) wird bei der Verschlüsselung abgebildet

von: ABCDEFGHIJKLMNOPQRSTUVWXYZ

auf: KLMNOPQRSTUVWXYZABCDEFGHIJ

Verschlüsseln Entschlüsseln Textoptionen Abbrechen

# CrypTool

## Permutation – Klartext-Analyse und durch Ausprobieren

The screenshot displays the CrypTool 1.4.10 interface. The main window shows a Caesar cipher decryption of a German text about Alaska. A dialog box titled "Schlüssel eingabe: Permutation / Transposition" is open, allowing the user to input a key for permutation or transposition. The dialog has two sections: "1. Permutation (einfache Spaltentransposition)" and "2. Permutation (doppelte Spaltentransposition)". Both sections have a text input field for the key and radio buttons for "Zeilenweise" (row-wise) and "Spaltenweise" (column-wise) processing, with sub-options for "einlesen" (read), "permutieren" (permute), and "auslesen" (decrypt). The "Optionen" section includes checkboxes for "Jeweils die inverse Permutation anwenden" and "Zwischendialog mit der inversen Permutation anzeigen". At the bottom are buttons for "Verschlüsseln", "Entschlüsseln", and "Abbrechen".

**Schlüssel eingabe: Permutation / Transposition**

1. Permutation (einfache Spaltentransposition)

Schlüssel (Buchstaben oder durch Kommas separierte Zahlen)  
4,2,3,1

Permutation, wenn der Schlüssel als Buchstabenfolge eingegeben wurde

Zeilenweise ☒ einlesen ☐ permutieren ☐ auslesen  
Spaltenweise ☐ einlesen ☒ permutieren ☒ auslesen

2. Permutation (doppelte Spaltentransposition)

Schlüssel (Buchstaben oder durch Kommas separierte Zahlen)  
(1)

Permutation, wenn der Schlüssel als Buchstabenfolge eingegeben wurde

Zeilenweise ☒ einlesen ☐ permutieren ☐ auslesen  
Spaltenweise ☐ einlesen ☒ permutieren ☒ auslesen

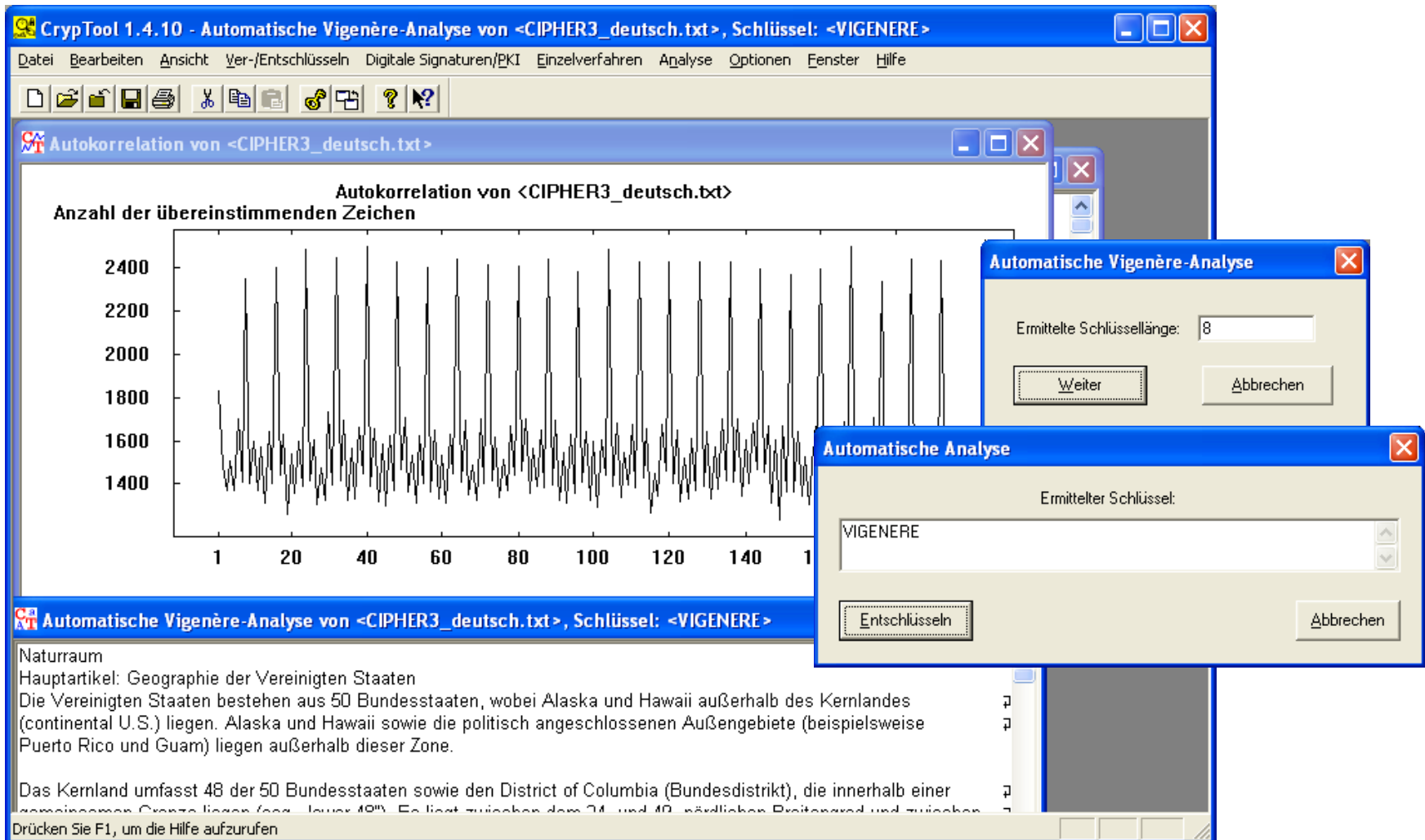
Optionen

☐ Jeweils die inverse Permutation anwenden  
☐ Zwischendialog mit der inversen Permutation anzeigen

Verschlüsseln Entschlüsseln Abbrechen

# CrypTool

## Vigenère – Automatische Analyse





# CrypTool

## Hill – Known-Plaintext Hill-Analyse mit linearer Algebra

The screenshot shows the CrypTool 1.4.10 interface with the 'Hill-Analyse (Known Plaintext)' window open. The main window displays a text file 'CIPHER4\_deutsch.txt' containing encrypted text. The 'Hill-Analyse (Known Plaintext)' window has a text area with the following content:

Naturraum  
Hauptartikel: Geographie der Vereinigten Staaten

Dimension: Analyse von 1 bis 10

Buttons: Weiter, Abbrechen

The 'Hill-Schlüsselmatrix' dialog is also open, showing the 'Hill-Schlüsselmatrix (Verschlüsseln)' option selected. It displays a 4x4 grid of alphabet characters and a corresponding 4x4 grid of numerical values.

Alphabetzeichen				Zahlenwerte			
D	X	Q	O	04	24	17	15
M	R	G	R	13	18	07	18
I	N	V	I	12	14	22	09
H	E	Q	S	08	05	17	19

Buttons: Schlüssel kopieren, Schließen

# CrypTool

## Substitution – Halbautomatische Analyse monoalphabetischer Substitution

The screenshot displays the CrypTool 1.4.10 interface with the 'Substitution' method selected. The main window shows the file 'CIPHER5\_deutsch.txt' and the key 'SUBKEYACDFGHIJLMNOPQRTVV'. A dialog box titled 'Methodenauswahl zur automatische Substitutionsanalyse' is open, showing 'Verfahren 1' selected. Another dialog box, 'Automatische Substitutionsanalyse mittels Digrammhäufigkeit', is also open, displaying the current substitution key and the analyzed text. The analyzed text is a German article about the United States. The interface includes a menu bar, a toolbar, and a status bar.

**CrypTool 1.4.10 - CIPHER5\_deutsch.txt - Substitution- SUBKEYACDFGHIJLMNOPQRTVV**

Datei Bearbeiten Ansicht Ver-/Entschlüsseln Digitale Signaturen/PKI Einzelverfahren Analyse Optionen

Methodenauswahl zur automatische Substitutionsanalyse

Bitte wählen Sie zwischen folgenden Algorithmen aus:

- ☒ Verfahren 1 basierend auf der Häufigkeitsanalyse der Digramme im Text

Der Algorithmus analysiert die Häufigkeit einzelner Digramme im verschlüsselten Text anhand einer Standardverteilung den Schlüssel zu erraten.

Verfahren 1 eignet sich am besten für die Analyse längerer Texte. Die automatische Spracherkennung ist eingebaut. Das Verfahren arbeitet auch mit Texten, die keine Leerzeichen enthalten.

Verfahren 2 basiert auf der Beobachtung, dass in jedem Text das Wort "A Fast Method for the Cryptanalysis of Substitution" vorkommt. Dieses Wort ist in der Liste der häufigsten Wörter einer Sprache enthalten. Auf einer Liste mit den häufigsten Wörtern der jeweiligen Sprache werden die Wörter des Ciphertextes mit den Wörtern der Liste verglichen. Die Zuordnung ergibt sich daraus eine (partielle) Substitution. Durch die Zuordnung der Wörter des Ciphertextes zu den Wörtern der Liste ergibt sich eine (partielle) Substitution. Durch die Zuordnung der Wörter des Ciphertextes zu den Wörtern der Liste ergibt sich eine (partielle) Substitution. Durch die Zuordnung der Wörter des Ciphertextes zu den Wörtern der Liste ergibt sich eine (partielle) Substitution.

Abbrechen

**Automatische Substitutionsanalyse mittels Digrammhäufigkeit**

Aktuelle Substitution (Schlüssel):  
ABCDEFGHIJKLMNOPQRSTUVWXYZ  
SUBKEYACDFGHIJLMNOPQRTVVXZ

Anzahl der validen Zeichen im Text:  
33728

Referenzdatei für Sprachanalyse:  
C:\Documents and Settings\ldj100\MyApps\CrypTool\reference\deutsch

Erkannte Sprache:  
Deutsch

Aktuelles Substitutionsergebnis:

Naturraum  
Hauptartikel: Geographie der Vereinigten Staaten  
Die Vereinigten Staaten bestehen aus 50 Bundesstaaten, wobei Alaska und Hawaii außerhalb des Kernlandes (continental U.S.) liegen. Puerto Rico und Guam sind ebenfalls Teil der Vereinigten Staaten, aber nicht Teil des Kernlandes.

Das Kernland umfasst 48 der 50 Bundesstaaten sowie den District of Columbia (Bundesdistrikt), die innerhalb einer Linie liegen, die von der Ostküste bis zur Westküste verläuft.

Im Jahr 1959 wurden auch die pazifische Inselgruppe Hawaii sowie das nordwestlich gelegene Alaska, das u.a. die Grenze zu Kanada: 8.895 km (davon 2.477 km zwischen Alaska und Kanada)  
Grenze zu Mexiko: 3.326 km  
Küstenlinie: 19.924 km  
Das Landschaftsbild ist sehr vielfältig: es existieren Waldgebiete und Mittelgebirge an der Ostküste, Mangrove an der Westküste.

Fläche  
Die Vereinigten Staaten sind der territorial dritt- oder viertgrößte Staat der Erde. Russland und Kanada sind deutlich größer.

Fläche der 50 Bundesstaaten (inkl. District of Columbia): 9.631.418 km²  
Landfläche: 9.158.453 km²  
Wasserfläche: 471.356 km²  
Siehe auch: Liste der Bundesstaaten nach Fläche

Substitution akzeptieren Schlüssel kopieren Manuelle Analyse Abbrechen

Drücken Sie F1, um die Hilfe anzuzeigen.

# Einführung in die Kryptologie mit CryptTool

Übung Teil III – Moderne Verfahren

**Workshop  
INFOS 2009**



[www.cryptool.com](http://www.cryptool.com)  
[www.cryptool.de](http://www.cryptool.de)  
[www.cryptool.org](http://www.cryptool.org)  
[www.cryptool.pl](http://www.cryptool.pl)

## Aufgabe 2:

### Dokument-Signaturen

1. Erzeugen Sie sich Ihren eigenen RSA-Schlüssel.
2. Öffnen Sie das Dokument „original.txt“ (Unterordner „Examples“) und signieren Sie es  
(Menü „Digitale Signaturen/PKI“ \ „Dokument signieren“).
3. Erzeugen und prüfen Sie die Signatur nun „Schritt-für-Schritt“  
(Menü „Digitale Signaturen/PKI“ \ „Signaturdemo“).  
Erklären Sie:
  - Warum ist vor der Signatur-Erstellung eine PIN-Eingabe notwendig?
  - Wie kann man die Echtheit einer Signatur prüfen?
  - Was geschieht mit dem Hashwert des zu signierenden Dokuments?
4. Öffnen Sie das Dokument „original.txt“ und rufen Sie die Hash-Demo auf  
(Menü „Einzelfahren“ \ „Hashverfahren“ \ „Hash-Demo“).  
Beobachten Sie, was mit dem Hashwert passiert, wenn man den Text verändert.

# CrypTool

## Elektronische Identität erzeugen

**Erzeugung eines asymmetrischen Schlüsselpaares**

**Verfahren**

- ☒ RSA  
Bitlänge des RSA-Moduls: 1024
- ☐ DSA  
Bitlänge der DSA-Primzahl: 1024
- ☐ Elliptische Kurven  
Bezeichner (Bitlänge und Kurvenparameter): prime239v1

**Benutzerdaten**

Das erzeugte Schlüsselpaar wird in einer verschlüsselten Datei (PSE) abgelegt. Durch Ihren PIN-Code wird das Schlüsselpaar geschützt:

Name: Mustermann  
Vorname: Max  
Schlüsselkennung (Optional): MM  
PIN-Code: [Masked]  
PIN-Verifikation: [Masked]

Hier werden die Domain-Parameter der spezifizierten Elliptischen Kurve angezeigt:

Parameter	Wert des Parameters	Bitlänge

**SECUDE Crypto Runtime - Random Number Generator**

Random Number Generation

Move your mouse and press different keys on your keyboard until enough random material is collected.

OK

**Öffentliche Parameter**

Öffentliche Parameter von [Mustermann][Max][RSA-1024][1189972311][MM] anzeigen.

Variable	Wert
Modul	17821438830281509246161407632274278549583316431333315657994...
Expon...	65537

Zahlensystem der Parameterdarstellung:

☐ Oktal ☒ Dezimal ☐ Hexadezimal

Übernehmen Zurück

**CrypTool**

Die von ihnen gewählten Parameter und das erzeugte Schlüsselpaar wurden erfolgreich abgespeichert.  
Der zugewiesene Schlüsselbezeichner ist:  
'[Mustermann][Max][RSA-1024][1189972311][MM]'

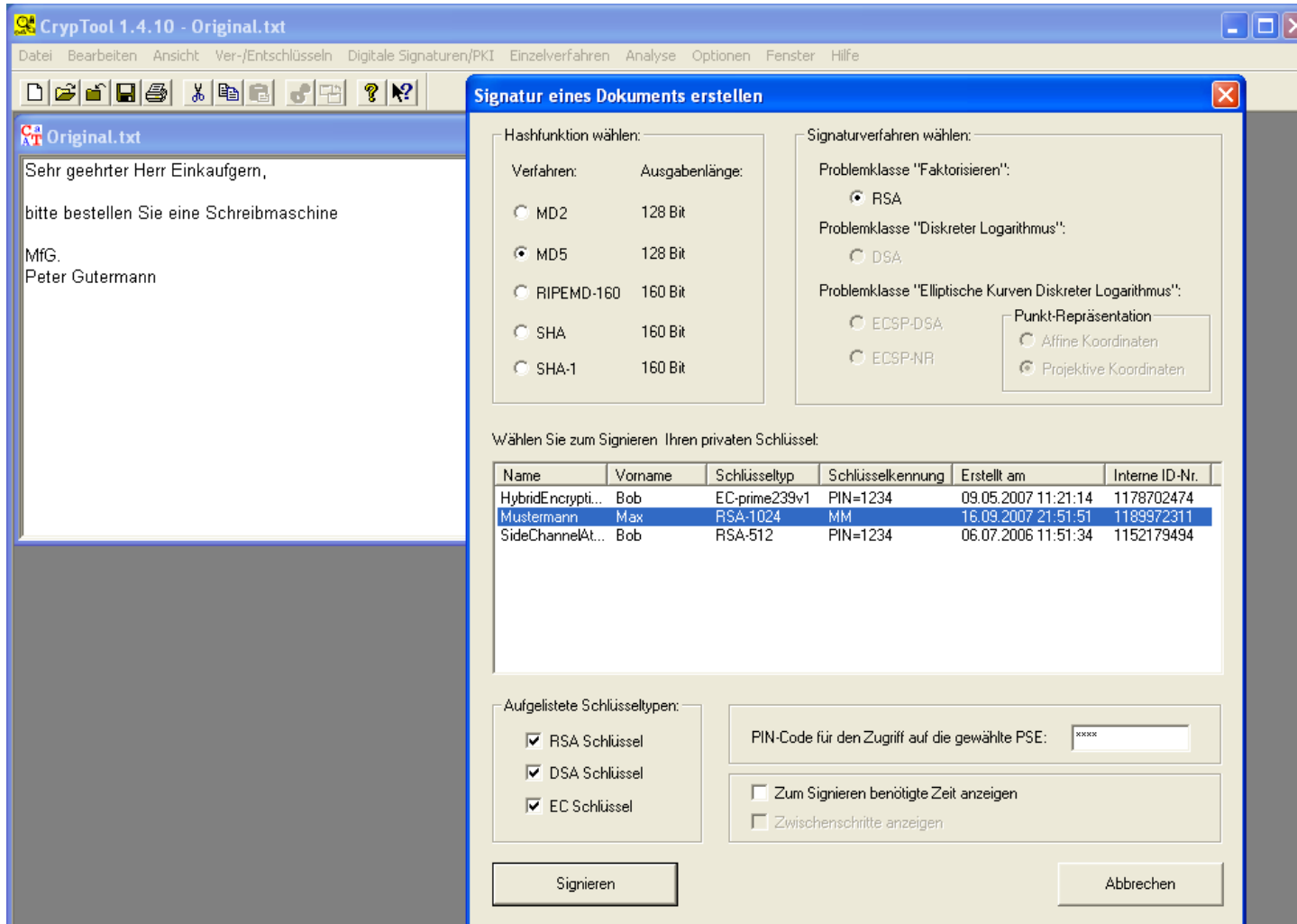
Zum Erzeugen des Schlüsselpaares benötigte Zeit: 7,952 Sekunden.

OK

„Zufall“ erforderlich

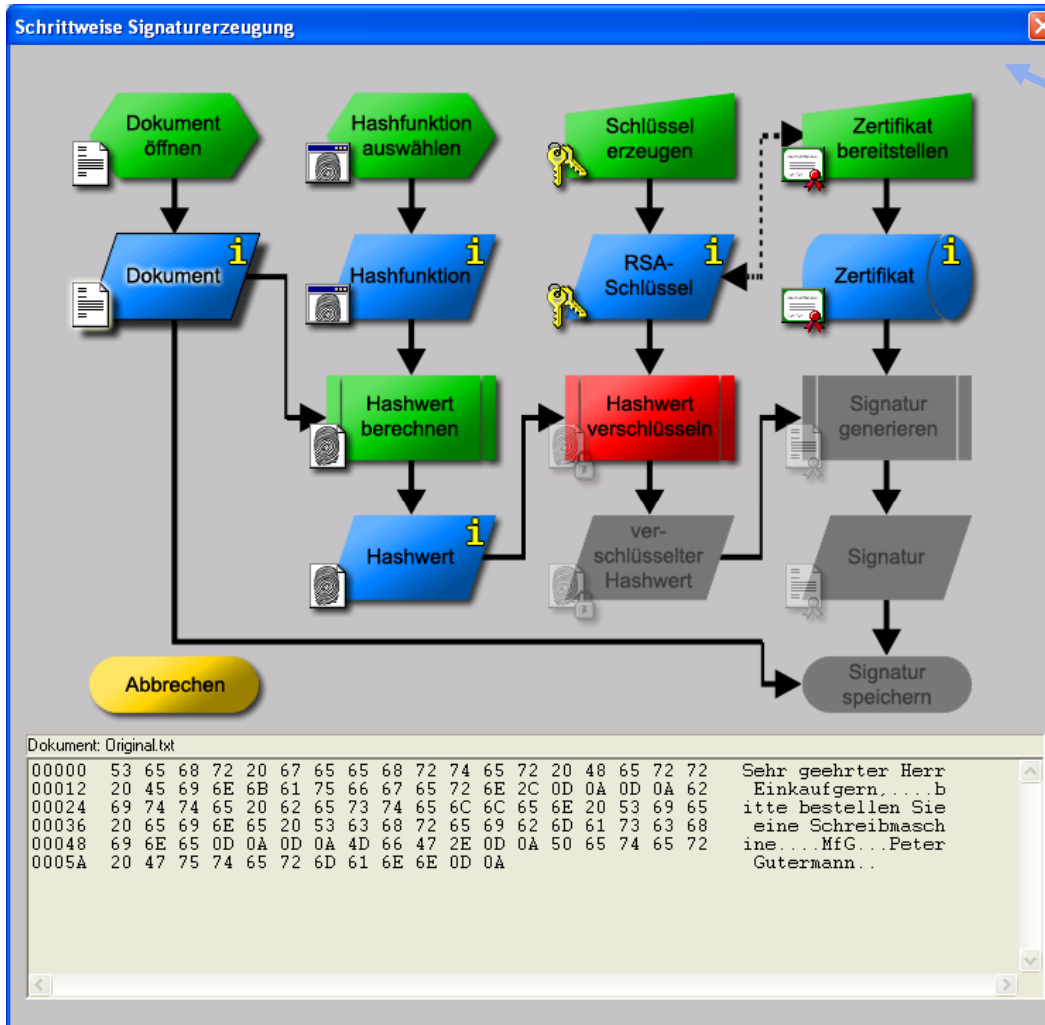
# CrypTool

## Schutz der Integrität und Urheber-Nachweis durch elektronische Signatur (1)



# CrypTool

## Schutz der Integrität und Urheber-Nachweis durch elektronische Signatur (2)



Signatur-Demo:  
Signaturerzeugung  
Schritt-für-Schritt



## Signatur extrahieren und Signatur-Prüfung (1)

[illegible]

# CrypTool

## Signatur extrahieren und Signatur-Prüfung (2)

**CrypTool 1.4.10 - RSA (MD5)-Signatur von <Original.txt>**

Datei Bearbeiten Ansicht Ver-/Entschlüsseln Digitale Signaturen/PKI Einzelverfahren

Original.txt

Sehr geehrter Herr Einkaufsgern,  
bitte bestellen Sie eine Schreibmaschine  
MfG.  
Peter Gutermann

**RSA (MD5)-Signatur von <Original.txt>**

00000000 53 69 67 6E 61 74 75 72 3A 20 20 20 20 20 20 20  
00000015 22 91 F2 3E B2 AA 13 7A 50 D3 33 43 FD AE 7C  
0000002A 3A 6F 32 5D 31 0B 5E CA 4C 70 A3 54 DB 64 FD  
0000003F 75 A6 FF 27 C8 A7 62 C8 91 83 2A 87 F9 17 0A  
00000054 E5 DB 44 59 F0 63 DB CE 80 88 68 5C 77 71 DE  
00000069 E3 7E 41 9F 00 CB AF B4 2A A0 A2 19 EC 6C CD  
0000007E 4B F5 48 E7 CD 9A A2 64 B9 E3 AF 78 E5 F8 D7  
00000093 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20  
000000A8 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20  
000000BD 3A 20 20 31 30 32 34 20 20 20 20 20 20 20  
000000D2 20 20 20 20 20 20 20 20 20 20 20 20 20 20  
000000E7 65 6E 3A 20 20 20 20 20 20 20 20 20 20 20  
000000FC 20 20 20 20 20 20 20 20 20 20 20 20 20 20  
00000111 61 73 68 66 75 6E 6B 74 69 6F 6E 3A 20 20 20  
00000126 20 20 20 20 20 20 20 20 20 20 20 20 20 20  
0000013B 20 20 20 20 20 20 20 20 20 20 20 20 20 20  
00000150 5B 4D 75 73 74 65 72 6D 61 6E 6E 5D 5B 4D 61  
00000165 2D 31 30 32 34 5D 5B 31 31 38 39 39 37 32 33  
0000017A 5D 20 20 20 20 20 20 20 20 20 20 20 20 20  
0000018F 20 4E 61 63 68 72 69 63 68 74 3A 20 20 20  
000001A4 20 67 65 65 68 72 74 65 72 20 48 65 72 72 20  
000001B9 66 67 65 72 6E 2C 0D 0A 0D 0A 62 69 74 74 65  
000001CE 6C 6C 65 6E 20 53 69 65 20 65 69 6E 65 20 53  
000001E3 6D 61 73 63 68 69 6E 65 0D 0A 0D 0A 4D 66 47  
000001F8 65 72 20 47 75 74 65 72 6D 61 6E 6E 0D 0A

**Verifizieren einer Signatur**

Wählen Sie aus der folgenden Liste den Signaturersteller:

Name	Vorname	Schlüsseltyp	Schlüsselkennung	Erstellt am	Interne ID-Nr.
HybridEncrypti...	Bob	EC-prime239v1	PIN=1234	09.05.2007 11:21:14	1178702474
Mustermann	Max	RSA-1024	MM	16.09.2007 21:51:51	1189972311
SideChannelAt...	Bob	RSA-512	PIN=1234	06.07.2006 11:51:34	1152179494

Angabe Daten

Signatur-Verfahren: RSA Hashfunktion: SHA-1

Aufgelistete Schlüsseltypen:

- ☒ RSA-Schlüssel
- ☒ DSA-Schlüssel
- ☒ EC-Schlüssel

Verifikation mit Verfahren:

☐ ECSP-DSA ☐ ECSP-NR

Verifikation mit Hashfunktion:

☒ SHA-1 ☐ RIPEMD-160

Repräsentation der EC-Punkte in:

☐ Affine Koord. ☒ Projektive Koord.

☒ Zum Verifizieren benötigte Zeit anzeigen

☒ Zwischenschritte anzeigen

Suche Schlüssel

Signatur verifizieren

Abbrechen

Signatur-Prüfung:  
Schritt-für-Schritt

## Signatur extrahieren und Signatur-Prüfung (3)

### CrypTool 1.4.10 - RSA (MD5)-Signatur von <Original.txt>

Datei Bearbeiten Ansicht Ver-/Entschlüsseln Digitale Signaturen/PKI Einzelverfahren

**Original.txt**

Sehr geehrter Herr Eir...

bitte bestellen Sie ein...

MfG.

Peter Gutermann

**SHA-1-Hashwert von <Original.txt>**

8A 6E FD 12 AE C2 E7 4D QA F9 1F 01 BD 1E 72 C3 F0 29 9A 32

Hashwert als HEX-Datei

Schließen

**RSA (MD5)-Signatur von <Original.txt>**

00000000	53	69	67	6E	61	74	75	72	3A	20	20	20	20	20	20	20
000000015	22	91	F2	3E	B2	AA	13	7A	50	D3	33	43	FD	AE	7C	58
00000002A	3A	6F	32	5D	31	0B	5E	CA	4C	70	A3	54	DB	64	FD	81
00000003F	75	A6	FF	27	C8	A7	62	C8	91	83	2A	87	F9	17	0A	0B
000000054	E5	DB	44	59	F0	63	DB	CE	80	88	68	5C	77	71	DE	FE
000000069	E3	7E	41	9F	00	CB	AF	B4	2A	A0	A2	19	EC	6C	CD	80
00000007E	4B	F5	48	E7	CD	9A	A2	64	B9	E3	AF	78	E5	F8	D7	16
000000093	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20
0000000A8	20	20	20	20	20	20	20	20	53	69	67	6E	61	74	75	72
0000000BD	3A	20	20	31	30	32	34	20	20	20	20	20	20	20	20	20
0000000D2	20	20	20	20	20	20	20	20	20	20	20	20	20	20	56	69
0000000E7	65	6E	3A	20	20	20	20	20	52	53	41	20	20	20	20	20
0000000FC	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20
000000111	61	73	68	66	75	6E	6B	74	69	6F	6E	3A	20	20	20	4D
000000126	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20
00000013B	20	20	20	20	20	53	63	68	6C	FC	73	73	65	6C	3A	20
000000150	5B	4D	75	73	74	65	72	6D	61	6E	6E	5D	5B	4D	61	78
000000165	2D	31	30	32	34	5D	5B	31	31	38	39	39	37	32	33	31
00000017A	5D	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20
00000018F	20	4E	61	63	68	72	69	63	68	74	3A	20	20	20	20	20
0000001A4	20	67	65	65	68	72	74	65	72	20	48	65	72	72	20	49
0000001B9	66	67	65	72	6E	2C	0D	0A	0D	0A	62	69	74	74	65	20
0000001CE	6C	6C	65	6E	20	53	69	65	20	65	69	6E	65	20	53	63
0000001E3	6D	61	73	63	68	69	6E	65	0D	0A	0D	0A	4D	66	47	2B
0000001F8	65	72	20	47	75	74	65	72	6D	61	6E	6E	0D	0A		

### RSA-Demo

☐ RSA mit privatem und öffentlichem Schlüssel -- oder nur mit öffentlichem Schlüssel  
☐ Wählen Sie Primzahlen p und q. Die Zahl N = pq ist der öffentliche RSA-Modul und  $\phi(N) = (p-1)(q-1)$  ist die Eulersche Zahl. Der öffentliche Schlüssel e ist teilerfremd zu  $\phi(N)$ . Daraus wird der geheime Schlüssel  $d = e^{-1} \pmod{\phi(N)}$  berechnet.  
☒ Zur Verschlüsselung von Daten oder zur Verifikation einer Signatur genügt es, dass Sie die öffentlichen RSA-Parameter angeben: den RSA-Modul N und den öffentlichen Schlüssel e.

**Faktorisierungsangriff**  
 Sie können mit Hilfe der Faktorisierung versuchen, den öffentlichen RSA-Modul N in seine Primfaktoren p und q zu faktorisieren.
 RSA-Modul faktorisieren...

**RSA-Parameter**  
 RSA-Modul N:  (öffentlich)  
 $\phi(N) = (p-1)(q-1)$ :  (geheim)  
 Öffentlicher Schlüssel e:   
 Geheimer Schlüssel d:  Parameter aktualisieren

**RSA-Verschlüsselung mit e / Entschlüsselung mit d**  
 Eingabe als: ☐ Text

# CrypTool

## Hash-Demo

The screenshot displays the CrypTool 1.4.10 interface. The main window, titled "Original.txt", contains the following text:

Sehr geehrter Herr Einkaufsgrn,  
bitte bestellen Sie eine Schreibmaschine  
MfG.  
Peter Gutermann

A blue callout box with the text "Kleine Änderungen im Dokument führen zu großen Änderungen im Hashwert." has an arrow pointing to the change in the document text.

The "Hash-Demo: SHA-1 (160 Bit)-Hash für Original.txt" dialog box is open on the right. It shows the "Auswahl der Hashfunktion" set to "SHA-1 (160 Bit)" and "Darstellung der Hashwerte" set to "hexadezimal". The "Aktuelles Dokument" field contains the modified text:

Sehr geehrter Herr Einkaufsgrn,  
bitte bestellen Sie keine Schreibmaschine  
MfG.  
Peter Gutermann

The dialog box displays the following hash values:

Hashwert der Originaldatei  
8A 6E FD 12 AE C2 E7 4D 0A F9 1F 01 BD 1E 72 C3 F0 29

Hashwert der aktuellen Datei  
12 26 E5 6A BC 0E 97 C4 16 90 B6 B1 33 00 61 E7 2D 2E

The difference between the two hashes is shown in binary:

```
10011000#01001000#00011000#01111000#00010010#11001100#  
01110000#10001001#00011100#01101001#10101001#10110000#  
10001110#00011110#00010011#00100100#11011101#00000111#  
00111111#11101011#
```

Below the binary difference, it states: "44.4% der Bits unterscheiden sich (71 von 160). Längste unveränderte Bitfolge: Offset 13, Länge 6."

The "Dialog beenden" button is at the bottom right of the dialog box.

## Aufgabe 3 (Fallbeispiel):

RSA-Verschlüsselung mit zu kurzer Schlüssellänge „knacken“

1. 128 Bit RSA-Schlüssel generieren
2. Öffentlicher / geheimer Schlüssel
  - Verschlüsseln: Öffentlicher Schlüssel (des Empfängers) wird benötigt
  - Entschlüsseln: Privater Schlüssel (des Empfängers) wird benötigt
3. RSA knacken

# CrypTool

## RSA-Schlüssel (128-Bit) generieren

**Primzahlen generieren**

Primzahlen spielen in der modernen Kryptographie eine wichtige Rolle. Hier erzeugen Sie sich zwei zufällige Primzahlen p und q aus dem Wertebereich [Untergrenze, Obergrenze].

Algorithmen zur Generierung

- ☒ Miller-Rabin-Test
- ☐ Solovay-Strassen-Test
- ☐ Fermat-Test

Wertebereich der beiden Primzahlen

- ☐ unabhängig voneinander eingeben
- ☒ beide gleich (nur einen eingeben)

Primzahl p

Untergrenze:

Obergrenze:

Ergebnis:

Primzahl q

Untergrenze:

Obergrenze:

Ergebnis:

**RSA-Demo**

RSA mit privatem und öffentlichem Schlüssel -- oder nur mit öffentlichem Schlüssel

- ☒ Wählen Sie 2 Primzahlen p und q. Die Zahl  $N = pq$  ist der öffentliche RSA-Modul und  $\phi(N) = (p-1)(q-1)$  ist die Eulersche Zahl. Der öffentliche Schlüssel e ist teilerfremd zu  $\phi(N)$ . Daraus wird der geheime Schlüssel  $d = e^{-1} \pmod{\phi(N)}$  berechnet.
- ☐ Zur Verschlüsselung von Daten oder zur Verifikation einer Signatur genügt es, dass Sie die öffentlichen RSA-Parameter angeben: den RSA-Modul N und den öffentlichen Schlüssel e.

Primzahleingabe

Primzahl p:

Primzahl q:

RSA-Parameter

RSA-Modul N:  (öffentlich)

$\phi(N) = (p-1)(q-1)$ :  (geheim)

Öffentlicher Schlüssel e:

Geheimer Schlüssel d:

RSA-Verschlüsselung mit e / Entschlüsselung mit d

Eingabe als ☒ Text ☐ Zahlen 

Eingabe der zu ver- oder entschlüsselnden Nachricht als Text oder als HexDump.

## RSA-Verschlüsselung mit dem öffentlichen Schlüssel

**RSA-Demo**

---

**- RSA mit privatem und öffentlichem Schlüssel -- oder nur mit öffentlichem Schlüssel**

- Wählen Sie 2 Primzahlen p und q. Die Zahl N = pq ist der öffentliche RSA-Modul und  $\phi(N) = (p-1)(q-1)$  ist die Eulersche Zahl. Der öffentliche Schlüssel e ist teilerfremd zu  $\phi(N)$ . Daraus wird der geheime Schlüssel  $d = e^{-1} \pmod{\phi(N)}$  berechnet.
- Zur Verschlüsselung von Daten oder zur Verifikation einer Signatur genügt es, dass Sie die öffentlichen RSA-Parameter angeben: den RSA-Modul N und den öffentlichen Schlüssel e.

---

**- Faktorisierungsangriff**

Sie können mit Hilfe der Faktorisierung versuchen, den öffentlichen RSA-Modul N in seine Primfaktoren p und q zu faktorisieren.

RSA-Modul faktorisieren...

---

**- RSA-Parameter**

RSA-Modul N	<input type="text" value="18445365965984830309239740090702827987"/>	(öffentlich)
$\phi(N) = (p-1)(q-1)$	<input type="text"/>	(geheim)
Öffentlicher Schlüssel e	<input type="text" value="65537"/>	
Geheimer Schlüssel d	<input type="text"/>	

---

**- RSA-Verschlüsselung mit e / Entschlüsselung mit d**

Eingabe als ☒ Text ☐ Zahlen

Eingabetext

Der Eingabetext wird in Blöcke der Länge 15 aufgeteilt (das Symbol '#' dient als Trennzeichen).

Zahlendarstellung der Eingabe zur Basis 16.

Verschlüsselung in den Chiffretext  $c[i] = m[i]^e \pmod{N}$ .

## RSA-Entschlüsselung mit dem privaten Schlüssel

**RSA-Demo**

---

- RSA mit privatem und öffentlichem Schlüssel -- oder nur mit öffentlichem Schlüssel

- ☒ Wählen Sie 2 Primzahlen p und q. Die Zahl  $N = pq$  ist der öffentliche RSA-Modul und  $\phi(N) = (p-1)(q-1)$  ist die Eulersche Zahl. Der öffentliche Schlüssel e ist teilerfremd zu  $\phi(N)$ . Daraus wird der geheime Schlüssel  $d = e^{-1} \pmod{\phi(N)}$  berechnet.
- ☐ Zur Verschlüsselung von Daten oder zur Verifikation einer Signatur genügt es, dass Sie die öffentlichen RSA-Parameter angeben: den RSA-Modul N und den öffentlichen Schlüssel e.

---

Primzahleingabe

Primzahl p	2444050160748480917	Primzahlen generieren...
Primzahl q	7547048854486688711	

---

RSA-Parameter

RSA-Modul N	18445365965984830309239740090702827987	(öffentlich)
$\phi(N) = (p-1)(q-1)$	18445365965984830299248641075467658360	(geheim)
Öffentlicher Schlüssel e	65537	
Geheimer Schlüssel d	15244157602814232624291684797451131113	Parameter aktualisieren

---

- RSA-Verschlüsselung mit e / Entschlüsselung mit d

Eingabe als ☐ Text ☒ Zahlen Optionen für Alphabet und Zahlensystem...

Chiffretext in Zahlendarstellung zur Basis 16 .

D8FDEAAAF1080DFF27464811E267F74F # 6DDC528B25EEBFD4895B21D0EA80670

Entschlüsselung in den Klartext  $m[i] = c[i]^d \pmod{N}$

05448495320495320412053484F5254 # 0204D45535341474520202020202020

Ausgabertext aus der Entschlüsselung (in Blöcken der Länge 15; das Symbol '#' dient nur als Trennzeichen).

THIS IS A SHORT # MESSAGE

Klartext

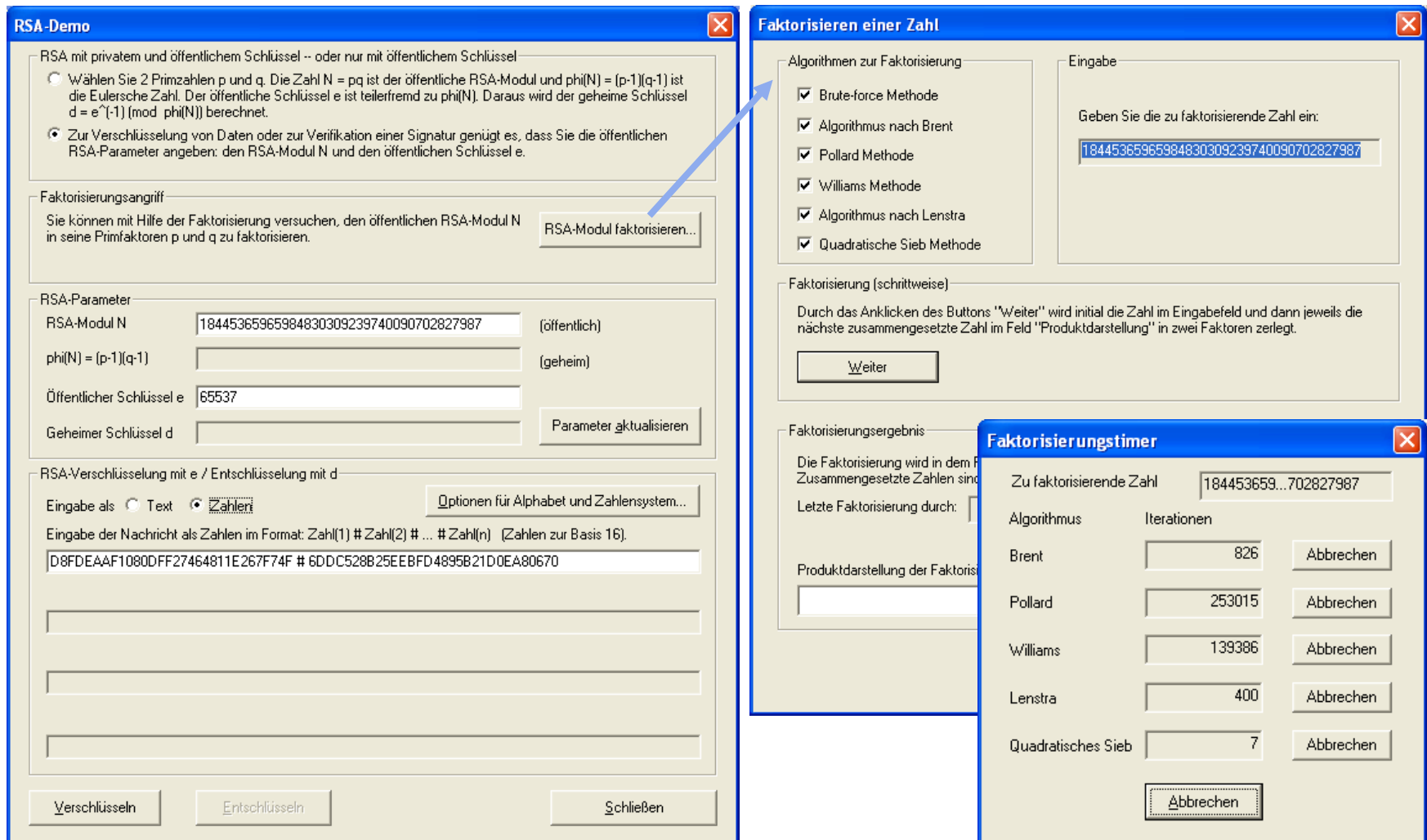
THIS IS A SHORT MESSAGE

Verschlüsseln
Entschlüsseln
Schließen



# CrypTool

## RSA „knacken“ durch die Faktorisierung von N (1/2)



**RSA-Demo**

RSA mit privatem und öffentlichem Schlüssel -- oder nur mit öffentlichem Schlüssel

- ☐ Wählen Sie 2 Primzahlen p und q. Die Zahl  $N = pq$  ist der öffentliche RSA-Modul und  $\phi(N) = (p-1)(q-1)$  ist die Eulersche Zahl. Der öffentliche Schlüssel e ist teilerfremd zu  $\phi(N)$ . Daraus wird der geheime Schlüssel  $d = e^{-1} \pmod{\phi(N)}$  berechnet.
- ☒ Zur Verschlüsselung von Daten oder zur Verifikation einer Signatur genügt es, dass Sie die öffentlichen RSA-Parameter angeben: den RSA-Modul N und den öffentlichen Schlüssel e.

**Faktorisierungsangriff**

Sie können mit Hilfe der Faktorisierung versuchen, den öffentlichen RSA-Modul N in seine Primfaktoren p und q zu faktorisieren. RSA-Modul faktorisieren...

**RSA-Parameter**

RSA-Modul N:  (öffentlich)

$\phi(N) = (p-1)(q-1)$ :  (geheim)

Öffentlicher Schlüssel e:

Geheimer Schlüssel d:

Parameter aktualisieren

**RSA-Verschlüsselung mit e / Entschlüsselung mit d**

Eingabe als: ☐ Text ☒ **Zahlen** Optionen für Alphabet und Zahlensystem...

Eingabe der Nachricht als Zahlen im Format: Zahl(1) # Zahl(2) # ... # Zahl(n) (Zahlen zur Basis 16).

Verschlüsseln Entschlüsseln Schließen

**Faktorisieren einer Zahl**

**Algorithmen zur Faktorisierung**

- ☒ Brute-force Methode
- ☒ Algorithmus nach Brent
- ☒ Pollard Methode
- ☒ Williams Methode
- ☒ Algorithmus nach Lenstra
- ☒ Quadratische Sieb Methode

**Eingabe**

Geben Sie die zu faktorisierende Zahl ein:

**Faktorisierung (schrittweise)**

Durch das Anklicken des Buttons "Weiter" wird initial die Zahl im Eingabefeld und dann jeweils die nächste zusammengesetzte Zahl im Feld "Produktdarstellung" in zwei Faktoren zerlegt.

Weiter

**Faktorisierungsergebnis**

Die Faktorisierung wird in dem Produkt dargestellt. Zusammengesetzte Zahlen sind in Klammern dargestellt.

Letzte Faktorisierung durch:

Produktdarstellung der Faktorisierung:

**Faktorisierungstimer**

Algorithmus	Iterationen	
Brent	826	<span>Abbrechen</span>
Pollard	253015	<span>Abbrechen</span>
Williams	139386	<span>Abbrechen</span>
Lenstra	400	<span>Abbrechen</span>
Quadratisches Sieb	7	<span>Abbrechen</span>

Abbrechen

# CrypTool

## RSA „knacken“ durch die Faktorisierung von N (2/2)

**Faktorisieren einer Zahl**

Algorithmen zur Faktorisierung

- ☒ Brute-force Methode
- ☒ Algorithmus nach Brent
- ☒ Pollard Methode
- ☒ Williams Methode
- ☒ Algorithmus nach Lenstra
- ☒ Quadratische Sieb Methode

Eingabe

Geben Sie die zu faktorisierende Zahl ein:

18445365965984830309239740090702827987

Faktorisierung (schrittweise)

Durch das Anklicken des Buttons "Weiter" wird initial die Zahl in das Eingabefeld und dann jeweils die nächste zusammengesetzte Zahl eingegeben.

Weiter

Faktorisierungsergebnis

Die Faktorisierung wird in dem Feld dargestellt. Zusammengesetzte Zahlen sind blau hervorgehoben.

Letzte Faktorisierung durch: Quadratisches Sieb

Insgesamt benötigte Zeit: 5.767 Sekunden.

Produktdarstellung der Faktorisierung:

2444050160748480917 \* 7547048854486688711

Details

Schließen

**CrypTool**

Der RSA-Modul N wurde erfolgreich in die Primzahlen p und q faktorisiert! Sie können jetzt die RSA-Operation auch mit dem geheimen Schlüssel d durchführen: Benutzen Sie hierfür den Knopf Entschlüsseln.

OK

**RSA-Demo**

RSA mit privatem und öffentlichem Schlüssel -- oder nur mit öffentlichem Schlüssel

- ☒ Wählen Sie 2 Primzahlen p und q. Die Zahl  $N = pq$  ist der öffentliche RSA-Modul und  $\phi(N) = (p-1)(q-1)$  ist die Eulersche Zahl. Der öffentliche Schlüssel e ist teilerfremd zu  $\phi(N)$ . Daraus wird der geheime Schlüssel  $d = e^{-1} \pmod{\phi(N)}$  berechnet.
- ☐ Zur Verschlüsselung von Daten oder zur Verifikation einer Signatur genügt es, dass Sie die öffentlichen RSA-Parameter angeben: den RSA-Modul N und den öffentlichen Schlüssel e.

Primzahleingabe

Primzahl p: 2444050160748480917

Primzahl q: 7547048854486688711

Primzahlen generieren...

RSA-Parameter

Modul N: 18445365965984830309239740090702827987 (öffentlich)

$\phi(N) = (p-1)(q-1)$ : 18445365965984830299248641075467658360 (geheim)

Öffentlicher Schlüssel e: 65537

Privater Schlüssel d: 15244157602814232624291684797451131113

Parameter aktualisieren

Modus: Verschlüsselung mit e / Entschlüsselung mit d

Eingabe als: ☐ Text ☒ Zahlen

Optionen für Alphabet und Zahlensystem...

Chiffretext in Zahlendarstellung zur Basis 16:

D8FDEAAAF108DFF27464811E267F74F # 6DDC528B25EEBFD4895B21D0EA80670

Entschlüsselung in den Klartext  $m[i] = c[i]^d \pmod{N}$ :

05448495320412053484F5254 # 0204D45535341474520202020202020

Ausgabertext aus der Entschlüsselung (in Blöcken der Länge 15; das Symbol '#' dient nur als Trennzeichen):

THIS IS A SHORT # MESSAGE

Klartext:

THIS IS A SHORT MESSAGE

Verschlüsseln

Entschlüsseln

Schließen

Durch Faktorisierung  
gefundene Primzahlen

# CrypTool – Neue Versionen, Weiterentwicklung

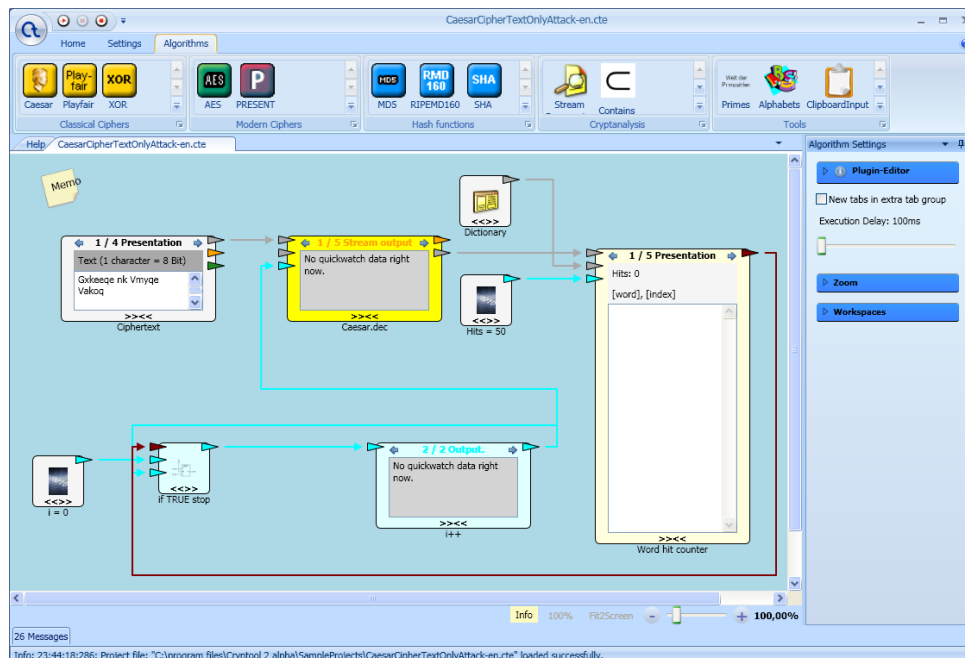
Pure-Plugin-Architekturen mit Java / Eclipse und mit C# / VS2008

JCT: Portierung und Neudesign von CrypTool in Java / SWT / Eclipse 3.4 / RCP

- siehe: <http://jcryptool.sourceforge.net>
- Meilenstein 5 für Benutzer und Entwickler verfügbar seit 20.9.2009

CT2: Portierung und Neudesign von CrypTool mit C# / WPF / VS2008 / .NET 3.5 SP1

- Direkter Nachfolger des aktuellen Releases: Erlaubt visuelle Programmierung, ...
- Betas für Benutzer und Entwickler verfügbar seit Juli 2008; aktuell CrypTool 2.0.3517b



CrypTool 2 (CT2)



JCrypTool (JCT)