

Forum Informatik

Kryptologische Erkenntnisse mit „CrypTool“





Stabile v1.4.30
Jetzt herunterladen

Über

Funktionen

Screenshots

Dokumentation

Download



Download



Download CryptTool 1.4.x



Download CryptTool 2.0 Beta



Download JCryTool Beta

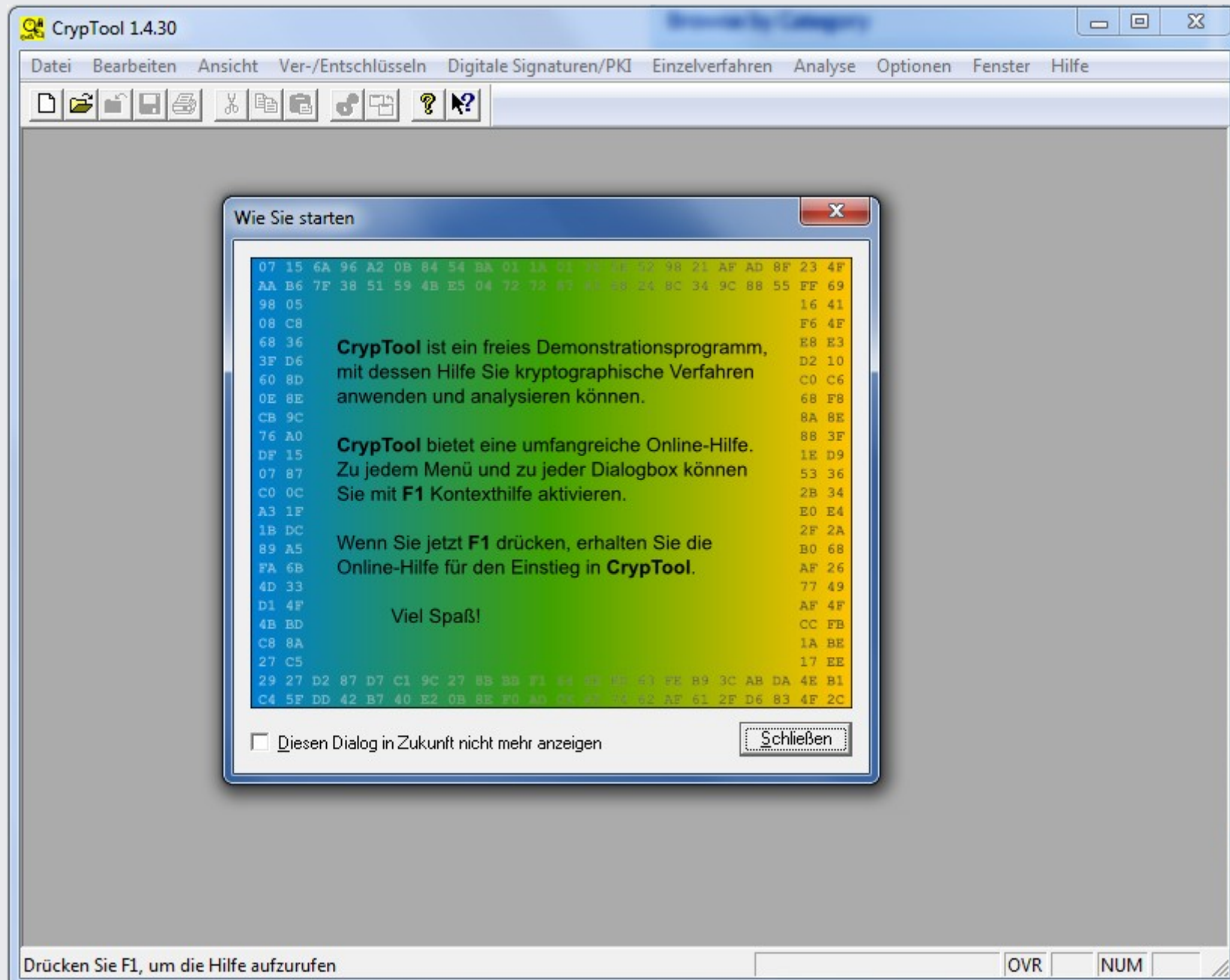
CrypTool 1.4.30

Die aktuelle, für Benutzer empfohlene Release-Version ist CrypTool 1.4.30 (erschieden am 04. August 2010).

Diese Version benötigt eine Win32-Umgebung. Das Programm enthält einige Funktionen, die Java-Anwendungen aufrufen: Dafür muss eine Java-Laufzeitumgebung ab JRE 1.6 installiert sein.

Sowohl die Release-Quellen (Tag "CrypTool_1_4_30") als auch die Quellen mit letzten Änderungen stehen im [Subversion-Repository](#) zur Verfügung. Darauf kann jedermann lesend zugreifen (Benutzername *anonymous* mit leerem Passwort).





Einsatzbereiche innerhalb des Informatikunterrichts

- Durchführen von Ver-/Entschlüsselungen:
 - Caesar
 - Substitution
 - Vigenère
 - AES (Rijndael)
 - RSA
 - AES-RSA
- Analyse
 - Substitution
 - Vigenère
- Einzelverfahren
 - Hashverfahren
 - RSA (Primzahltest, Faktorisieren, ...)
- Visualisierung von Algorithmen
 - Vigenère
 - AES
- u.v.m.



Einsatzbereiche innerhalb des Informatikunterrichts

- Durchführen von Ver-/Entschlüsselungen:
 - Caesar
 - Substitution
 - Vigenère
 - AES (Rijndael)
 - RSA
 - AES-RSA
- Analyse
 - **Substitution**
 - Vigenère
- Einzelverfahren
 - Hashverfahren
 - RSA (Primzahltest, Faktorisieren, ...)
- Visualisierung von Algorithmen
 - Vigenère
 - AES
- u.v.m.



Analyse – Substitution

The screenshot shows the CrypTool 1.4.30 interface with a substitution cipher analysis dialog box open. The main window displays a ciphertext: "Wvi Xzvhzixsruuiv (zfxs zoh vrmuzxsvi Xzvhzi. Evihxsrvyfmth- lwi Hsruqxsruuiv vvpzmma) rha vrmv". The dialog box, titled "Substitutionsanalyse: Manuelle Nachbearbeitung", provides instructions on how to use the manual editing feature. It contains a grid for mapping ciphertext letters to plaintext letters. The current mapping is as follows:

a:	i	b:	*	c:	*	d:	W	e:	*	f:	U	g:	T
h:	S	i:	R	j:	*	k:	*	l:	O	m:	N	n:	M
o:	*	p:	K	q:	*	r:	I	s:	H	t:	*	u:	*
v:	E	w:	D	x:	C	y:	*	z:	A				

Buttons for "Ergebnis der automatischen Analyse wieder herstellen" and "Ergebnis der manuellen Analyse wieder herstellen" are visible. The "Aktueller Zwischenstand" section shows the decrypted text: "DER CAESARCHIURE AUCH AaS EINuACHER CAESAR eERSCHIEyUNIS ODER SHIuTCHIuURE yEKANNT IST EINE MONOaokHAyETISCHE uORM DER eERSCHoUESSEoUNT yEI DER DAS AokHAyET UM EINE yESTIMMTE ANaHoAN aEICHEN ROTIERT WIRD DIESE ANaHo yESTIMMT DEN SCHoUESSEo DER SCHoUESSEo aUR SUySTITUTION WIRD WAEHREND DER tANaEN CHIuURIERUNT NICHT eERAENDERT ES IST DIE EINuACHSTE uORM EINER tEHEIMSCHRIUt CAESARCHIuURE HEISST SIE NACH".



Einsatzbereiche innerhalb des Informatikunterrichts

- Durchführen von Ver-/Entschlüsselungen:
 - Caesar
 - Substitution
 - Vigenère
 - AES (Rijndael)
 - RSA
 - AES-RSA
- Analyse
 - Substitution
 - Vigenère
- Einzelverfahren
 - Hashverfahren
 - RSA (Primzahltest, Faktorisieren, ...)
- Visualisierung von Algorithmen
 - Vigenère
 - AES
- u.v.m.



Visualisierung – Vigenère

Animal Animation: Vigenère-Verschlüsselung

Speed 100% Zoom 100%

Vigenère-Verschlüsselung

Die Vigenère-Verschlüsselung ist eine polyalphabetische Substitution. Das bedeutet, dass ein Buchstabe durch verschiedene Buchstaben ersetzt wird. Zunächst wird ein Schlüssel (s) festgelegt, der aus einer beliebigen Zeichenfolge der Länge n besteht. Diese Zeichenfolge wird wiederholt über den Klartext (k) geschrieben. Anschließend werden die übereinander stehenden Paare addiert und mit der Formel $c = (s + k) \bmod 26$ berechnet. Als Ergebnis erhält man das erste Chiffrezeichen (c). Jedem Buchstaben wird eine Zahl von 0 bis 25 zugeordnet: A=0, B=1, ..., Z=25. Neben der mathematischen Berechnung kann das Verfahren auch mit Hilfe des Vigenère-Quadrats veranschaulicht werden.

Schlüssel (s):

s	e	c	r	e	t	s	e	c	r	e	t
---	---	---	---	---	---	---	---	---	---	---	---

Klartext (k):

d	a	s	i	s	t	g	e	h	e	i	m
---	---	---	---	---	---	---	---	---	---	---	---

Chiffre (c):

--	--	--	--	--	--	--	--	--	--	--	--

Mit Hilfe der Formel kann die Verschlüsselung beginnen:
 $c = (s + k) \bmod 26$
 $= (\quad + \quad) \bmod 26$

Index	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
Klartext	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Shift 0	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	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a
2	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b
3	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c
4	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d
5	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e
6	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f
7	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g
8	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h
9	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i
10	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j
11	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k
12	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l
13	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m
14	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n
15	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
16	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p
17	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q
18	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r
19	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s
20	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t
21	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u
22	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v
23	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w
24	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x
25	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y

Navigation: [Previous] [Play] [Next] [Full Screen]

Kioskmodus: [Previous] [Next]

Manuelle Schrittkontrolle: 4 / 77 [Slider]

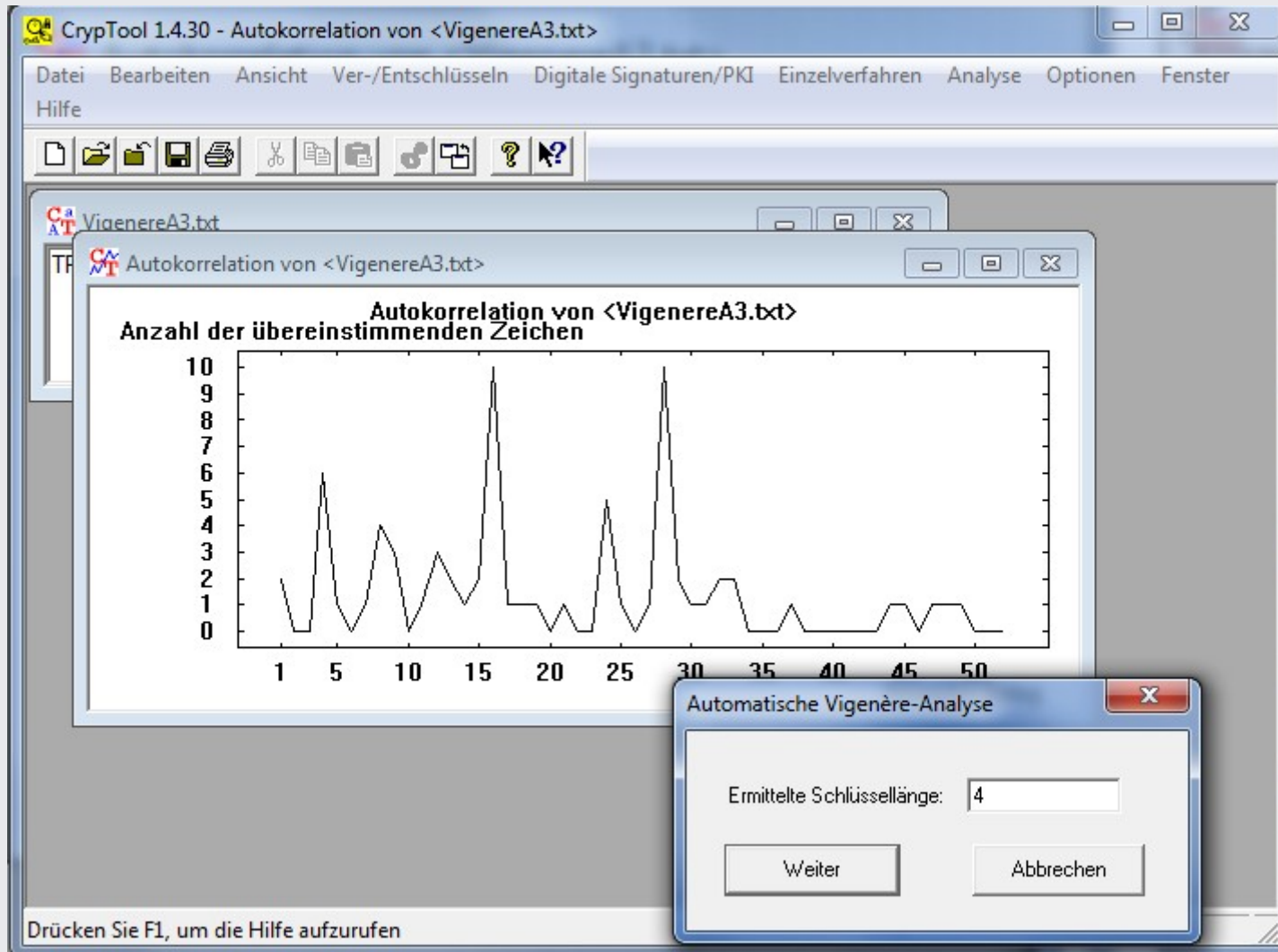


Einsatzbereiche innerhalb des Informatikunterrichts

- Durchführen von Ver-/Entschlüsselungen:
 - Caesar
 - Substitution
 - Vigenère
 - AES (Rijndael)
 - RSA
 - AES-RSA
- Analyse
 - Substitution
 - **Vigenère**
- Einzelverfahren
 - Hashverfahren
 - RSA (Primzahltest, Faktorisieren, ...)
- Visualisierung von Algorithmen
 - Vigenère
 - AES
- u.v.m.



Analyse – Vigenère

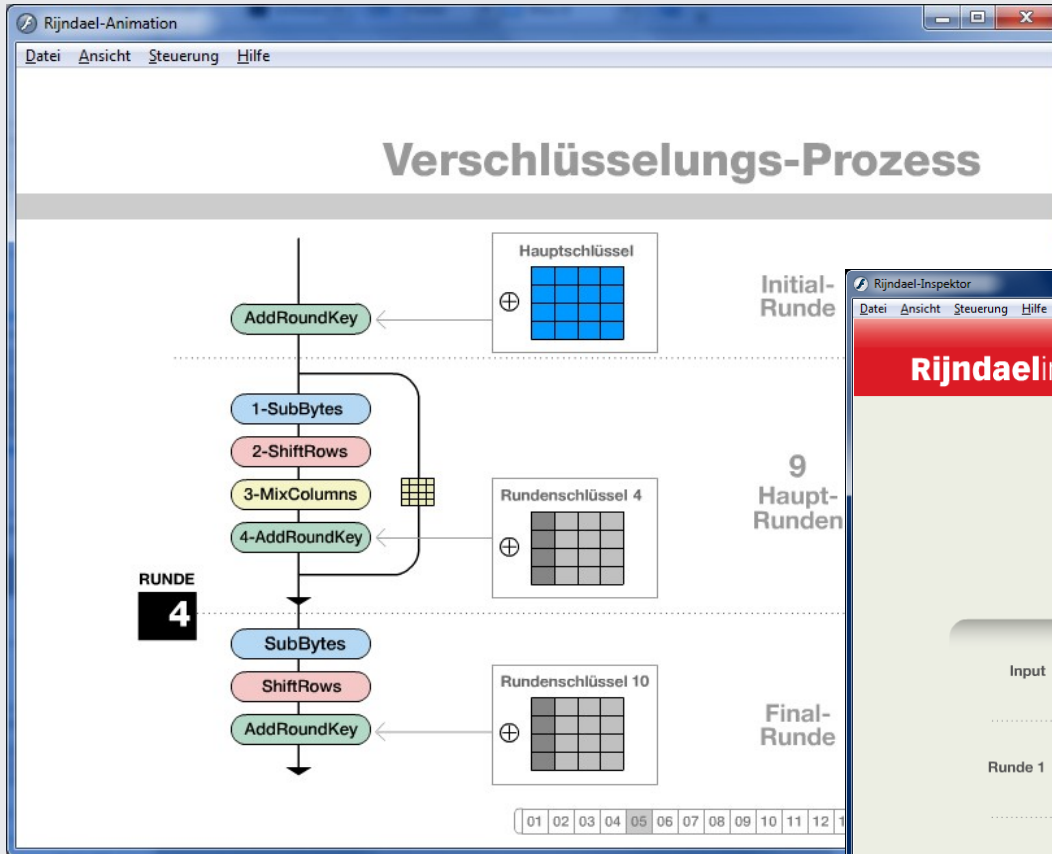


Einsatzbereiche innerhalb des Informatikunterrichts

- Durchführen von Ver-/Entschlüsselungen:
 - Caesar
 - Substitution
 - Vigenère
 - AES (Rijndael)
 - RSA
 - AES-RSA
- Analyse
 - Substitution
 - Vigenère
- Einzelverfahren
 - Hashverfahren
 - RSA (Primzahltest, Faktorisieren, ...)
- Visualisierung von Algorithmen
 - Vigenère
 - **AES**
- u.v.m.



Visualisierung – AES



Rijndaelinspektor

Testdaten laden: 1 2 2

Verschlüsseln Entschlüsseln

	Input (Klartext)	Schlüssel	Output
	32 88 31 e0 43 5a 31 37 f6 30 98 07 a8 8d a2 34	2b 28 ab 09 7e ae f7 cf 15 d2 15 4f 16 a6 88 3c	39 02 dc 19 25 dc 11 6a 84 09 85 0b 1d fb 97 32

	Start der Runde	Nach SubBytes	Nach ShiftRows	Nach MixColumns	Rundenschlüssel
Input	32 88 31 e0 43 5a 31 37 f6 30 98 07 a8 8d a2 34				2b 28 ab 09 7e ae f7 cf 15 d2 15 4f 16 a6 88 3c
Runde 1	19 a0 9a e9 3d f4 c6 f8 e3 e2 8d 48 be 2b 2a 08	d4 e0 b8 1e 27 bf b4 41 11 98 5d 52 ae f1 e5 30	d4 e0 b8 1e bf b4 41 27 5d 52 11 98 30 ae f1 e5	04 e0 48 28 66 cb f8 06 81 19 d3 26 e5 9a 7a 4c	a0 88 23 2a fa 54 a3 6c fe 2c 39 76 17 b1 39 05
Runde 2	a4 68 6b 02 9c 9f 5b 6a 7f 35 ea 50 f2 2b 43 49	49 45 7f 77 de db 39 02 d2 96 87 53 89 f1 1a 3b	49 45 7f 77 db 39 02 de 87 53 d2 96 3b 89 f1 1a	58 1b db 1b 4d 4b e7 6b ca 5a ca b0 f1 ac a8 e5	f2 7a 59 73 c2 96 35 59 95 b9 80 f6 f2 43 7a 7f
Runde 3	aa 61 82 68 8f dd d2 32 5f e3 4a 46 03 ef d2 9a	ac ef 13 45 73 c1 b5 23 cf 11 d6 5a 7b df b5 b8	ac ef 13 45 c1 b5 23 73 d6 5a cf 11 b8 7b df b5	75 20 53 bb ec 0b c0 25 09 63 cf d0 93 33 7c dc	3d 47 1e 6d 80 16 23 7a 47 fe 7e 88 f2 3e 44 3b

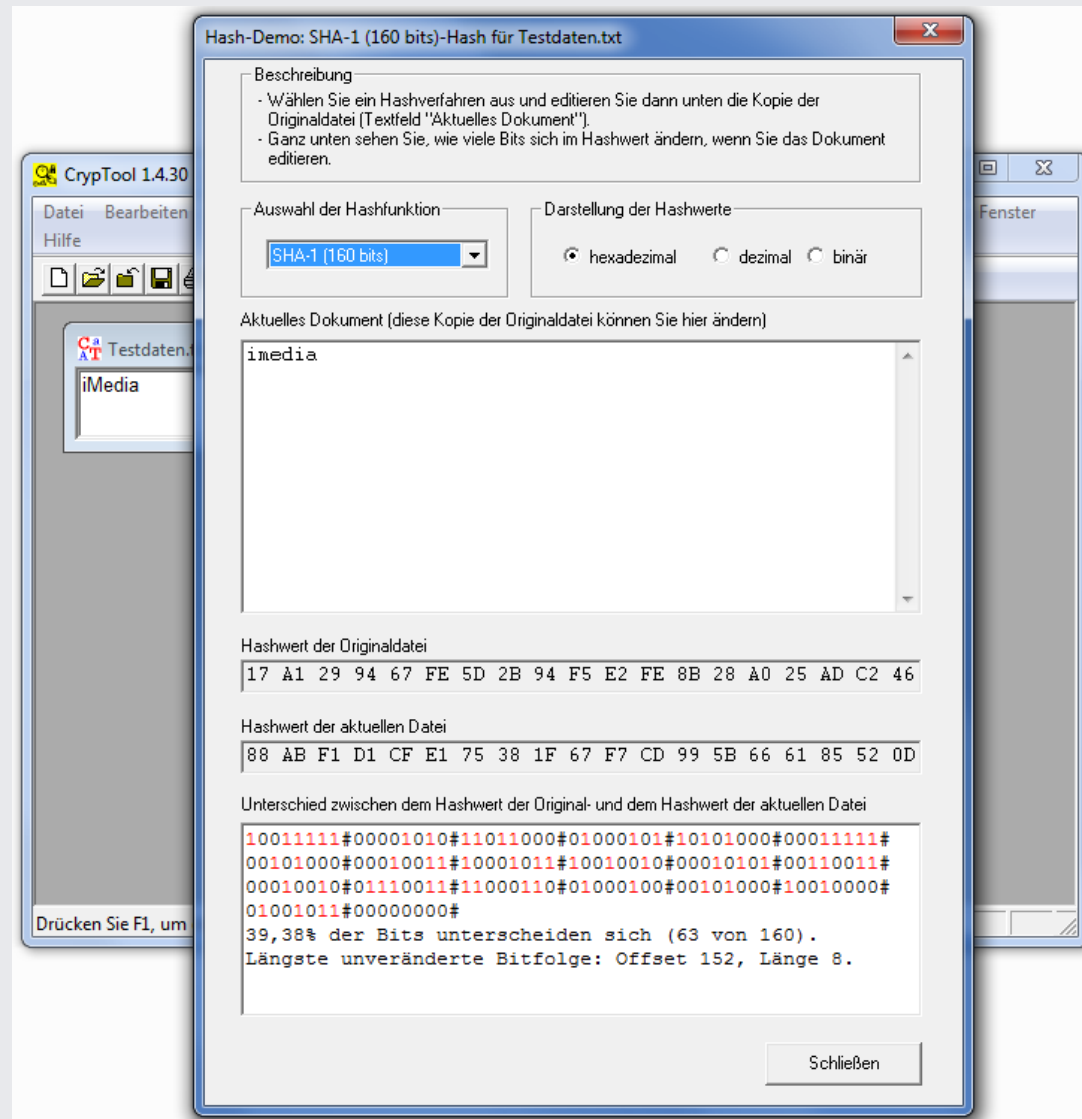


Einsatzbereiche innerhalb des Informatikunterrichts

- Durchführen von Ver-/Entschlüsselungen:
 - Caesar
 - Substitution
 - Vigenère
 - AES (Rijndael)
 - RSA
 - AES-RSA
- Analyse
 - Substitution
 - Vigenère
- Einzelverfahren
 - Hashverfahren
 - RSA (Primzahltest, Faktorisieren, ...)
- Visualisierung von Algorithmen
 - Vigenère
 - AES
- u.v.m.



Einzelverfahren – Hash (Hash-Demo)



Einsatzbereiche innerhalb des Informatikunterrichts

- Durchführen von Ver-/Entschlüsselungen:
 - Caesar
 - Substitution
 - Vigenère
 - AES (Rijndael)
 - RSA
 - AES-RSA
- Analyse
 - Substitution
 - Vigenère
- Einzelverfahren
 - Hashverfahren
 - RSA (Primzahltest, Faktorisieren, ...)
- Visualisierung von Algorithmen
 - Vigenère
 - AES
- u.v.m.

