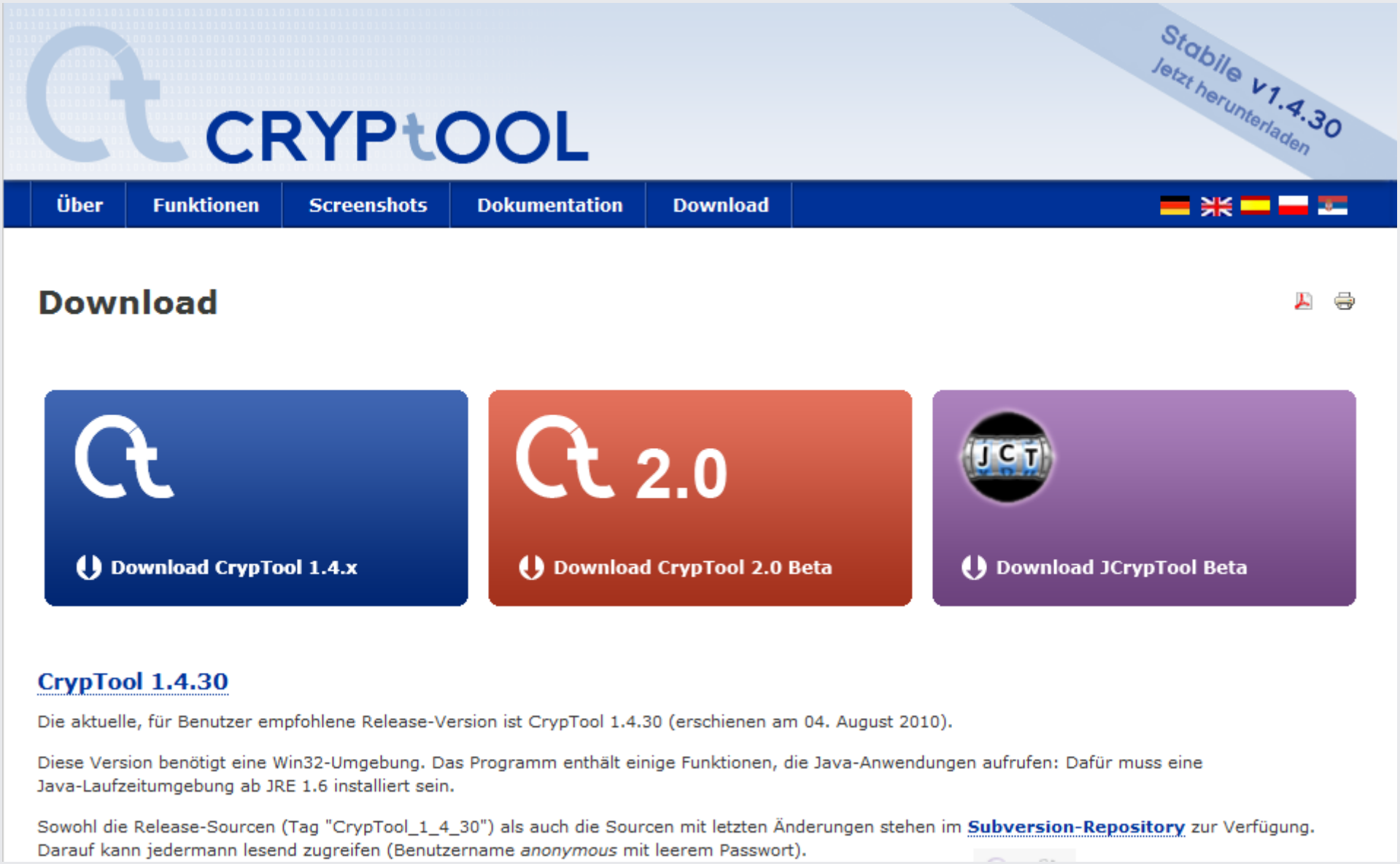
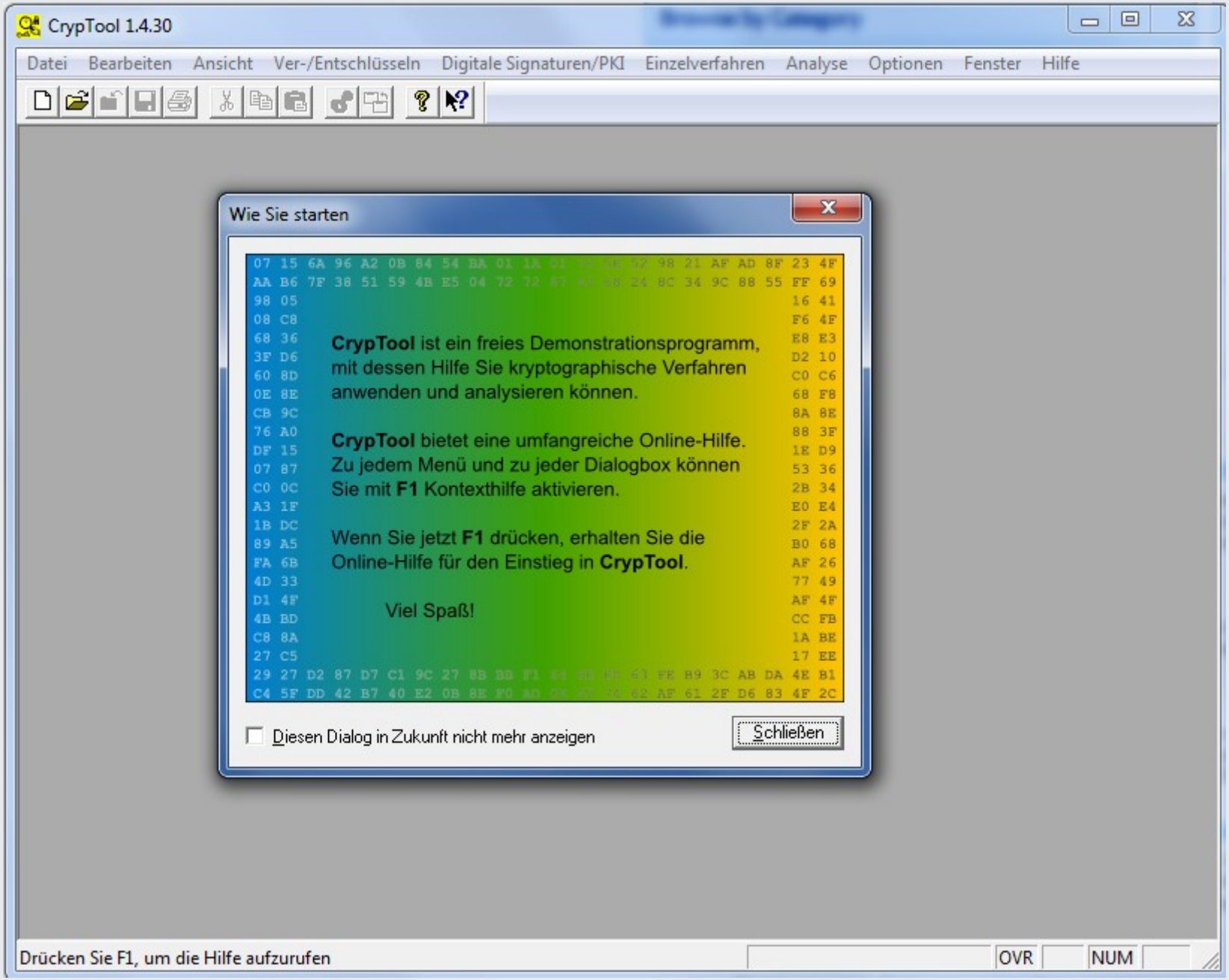
Kryptologische Erkenntnisse mit „CrypTool“

H.Jochum@gmx.de

www.cryptool.de




CrypTool 1.4.30
Datei Bearbeiten Ansicht Ver-/Entschlüsseln Digitale Signaturen/PKI Einzelverfahren Analyse Optionen Fenster Hilfe
Wie Sie starten
CrypTool ist ein freies Demonstrationsprogramm, mit dessen Hilfe Sie kryptographische Verfahren anwenden und analysieren können.
CrypTool bietet eine umfangreiche Online-Hilfe. Zu jedem Menü und zu jeder Dialogbox können Sie mit F1 Kontexthilfe aktivieren.
Wenn Sie jetzt F1 drücken, erhalten Sie die Online-Hilfe für den Einstieg in CrypTool.
Viel Spaß!
Diesen Dialog in Zukunft nicht mehr anzeigen
Schließen
Drücken Sie F1, um die Hilfe aufzurufen
OVR
NUM

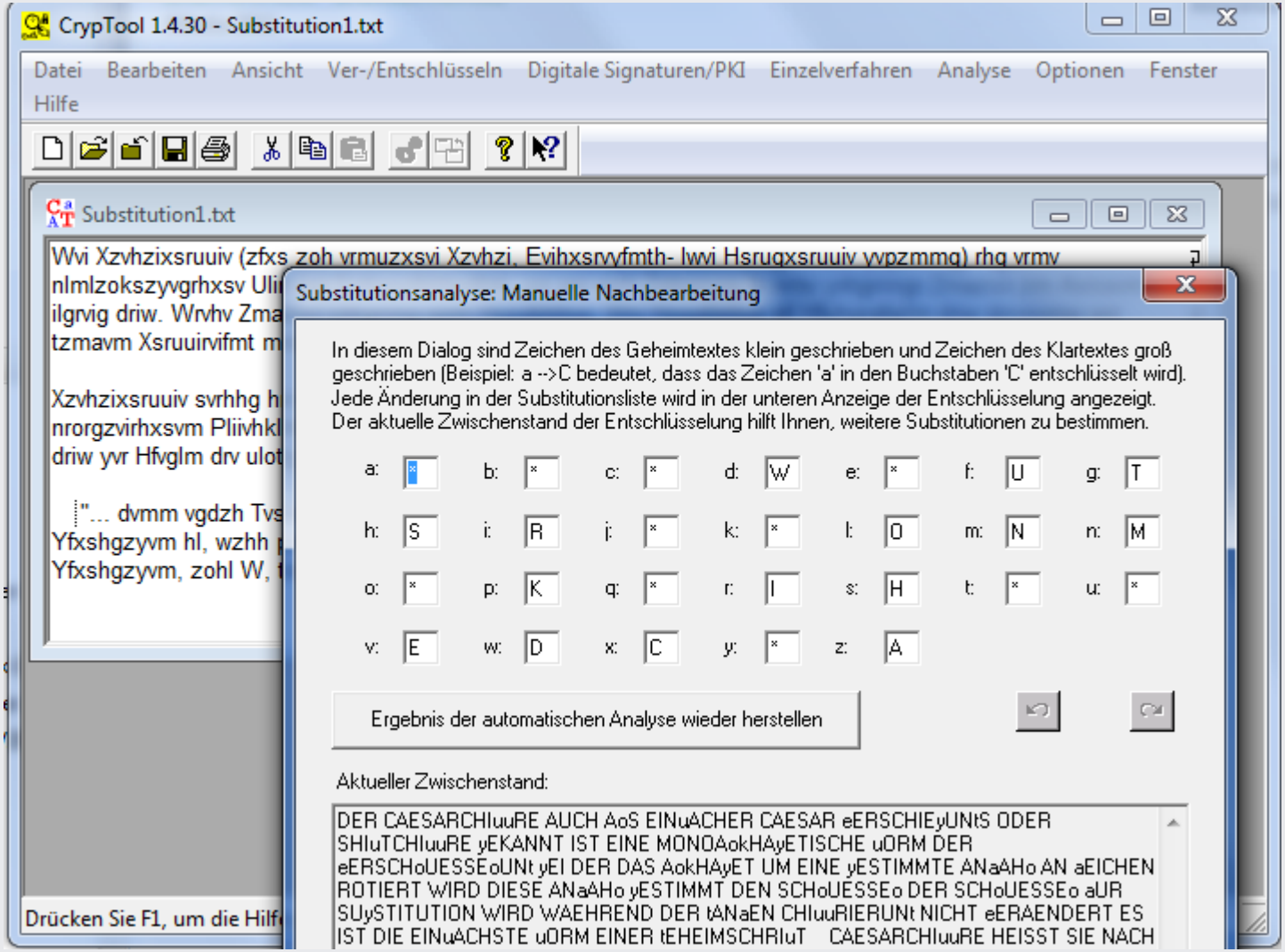
Einsatzbereiche innerhalb des Informatikunterrichts

- 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.

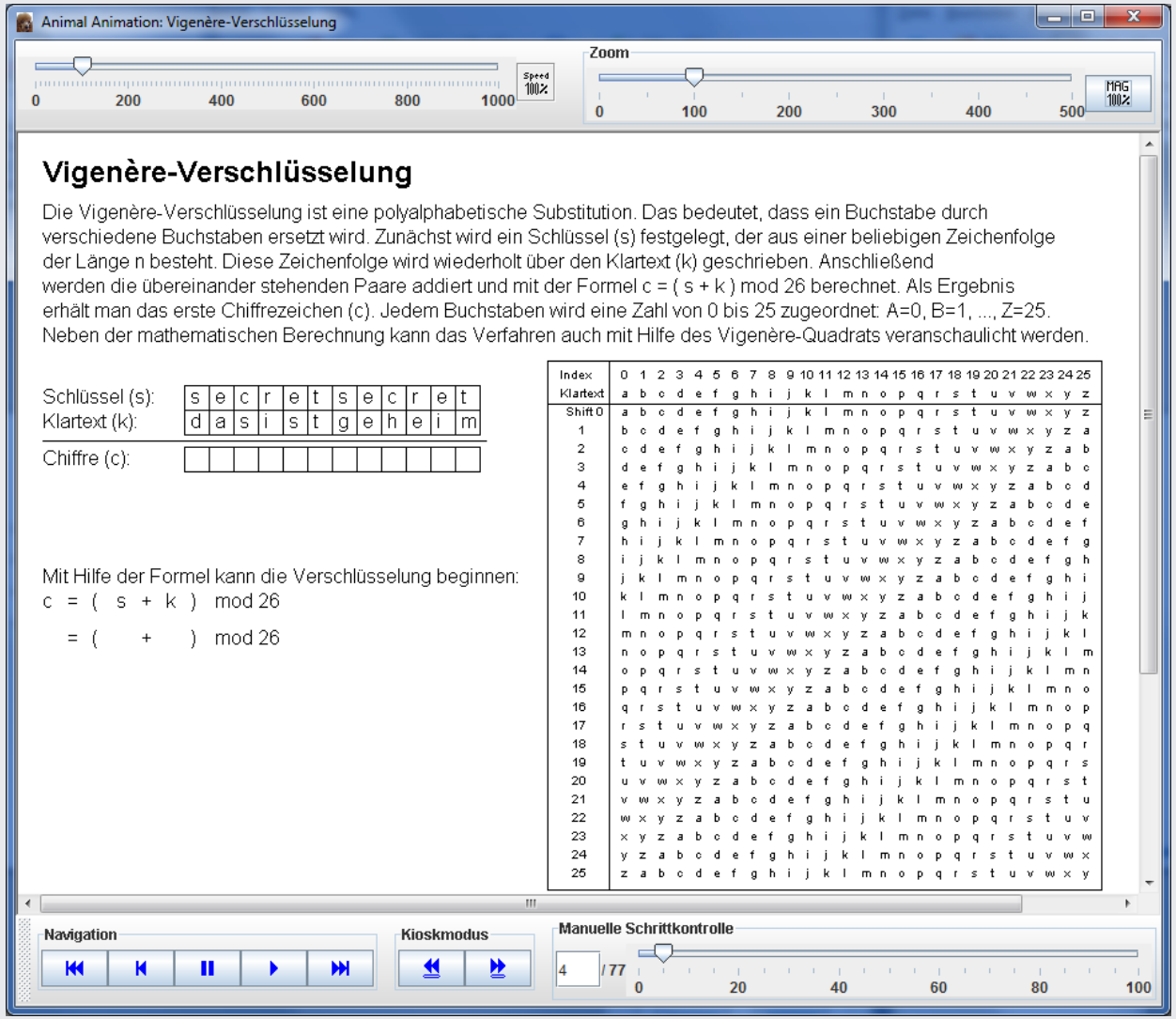
Analyse – Substitution



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.

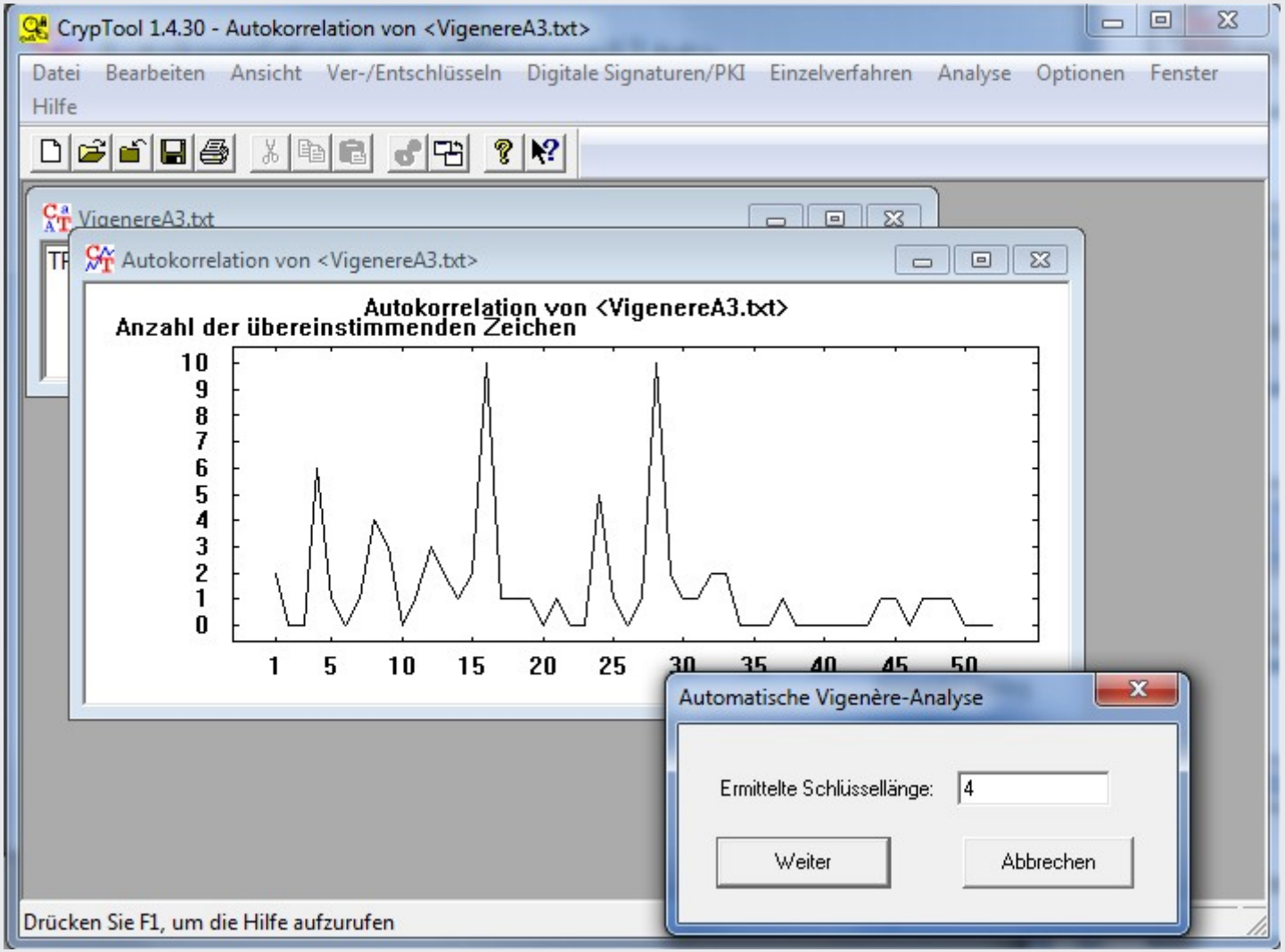
Visualisierung – Vigenère



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.

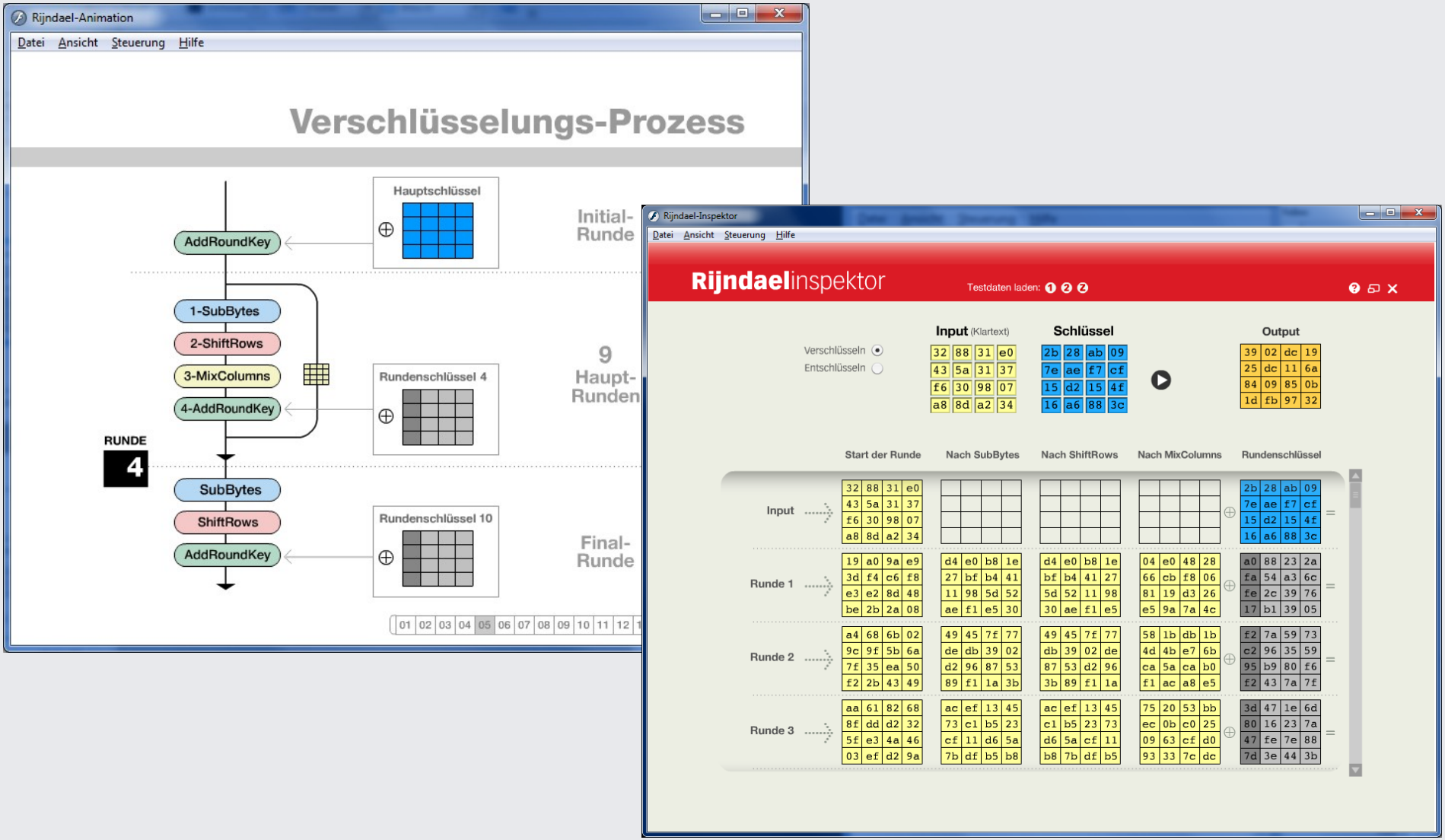
Analyse – Vigenère



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.

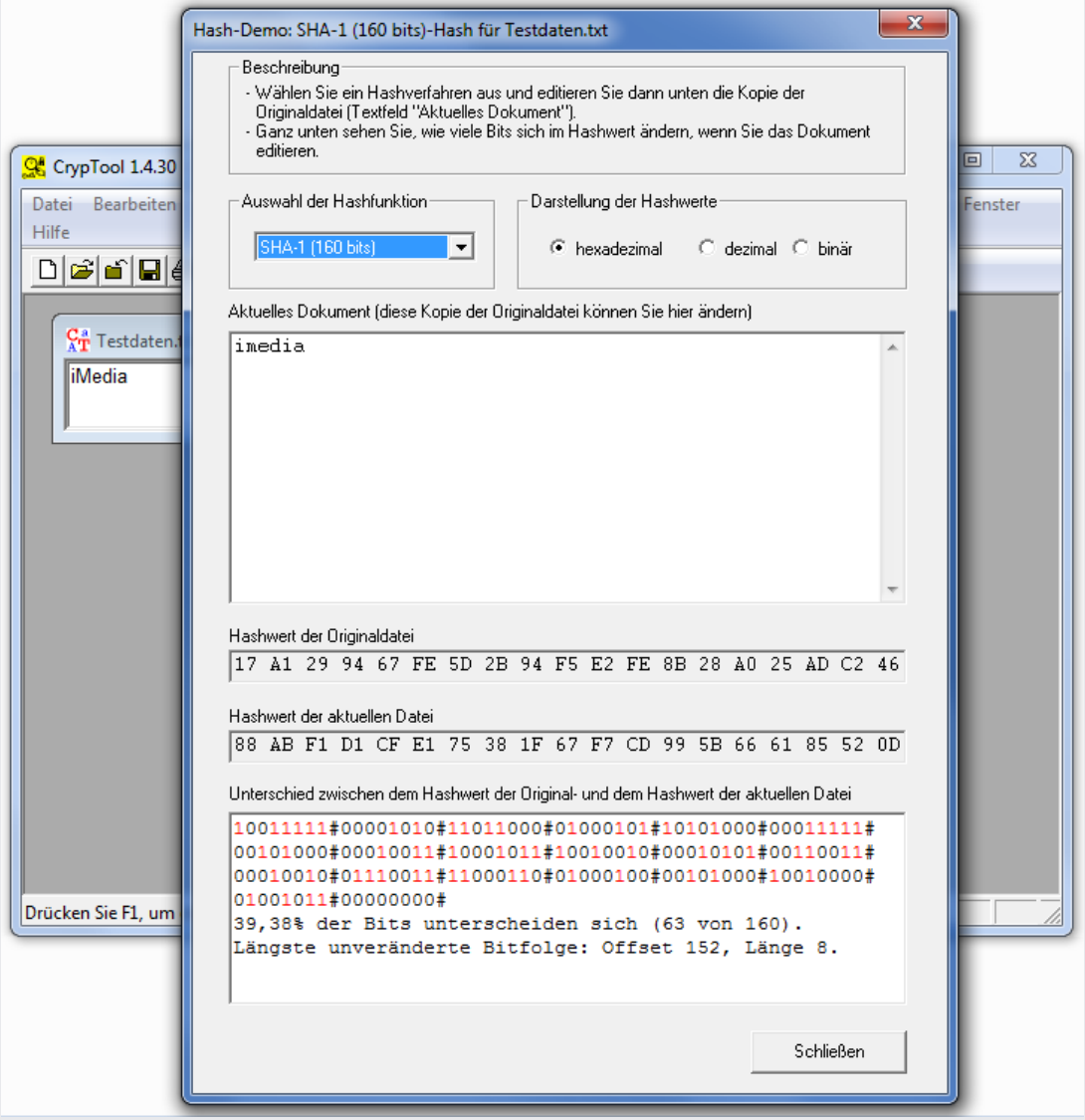
Visualisierung – AES



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.