

Beispiele:

Alle in einem großen Fonts:

1) Zu Caesar

Klartext laden von: Caesar-Plaintext(deutsch).txt [564 B]

Er stammt von:

<http://www.harrypotter-xperts.de/gurkensalat?book=1&sid=f1568227cc1d5e5cb990aec08afa207a>

Hagrid hat für Dumbledore etwas Wichtiges bei Gringotts zu erledigen: "It's about the You-Know-What in vault seven hundred and thirteen." - "Es geht um den Du-weißt-schon-was in Verlies siebenhundertundneunzehn." (S. 83)

Dies ist eine der Gurken schlechthin im ersten Band, denn "seven hundred and thirteen" ist nun mal nie und nimmer 719, sondern 713.

Wie kommt's? Lesefehler kann's nicht sein, denn die Zahl steht im englischen Original voll ausgeschrieben da, nicht als "713", so dass man die 3 versehentlich als 9 lesen könnte. Vielleicht hat Fritz für seine Übersetzung die Zahl zuerst als "713" in den Computer getippt, die Lektorin wollte die Zahl dann aber doch ausschreiben und hat versehentlich eine 9 draus gemacht? Mysteriös ...

- Verschlüsseln mit Caesar mit dem Passwort „C“, offset 0 ➔ Shift = 2.
- Sie können alle Zeichen verschlüsseln oder erst alles in Großbuchstaben umwandeln (siehe die Parameter in dem Textoptionen-Dialog oder Umformatieren oder über den Menüeintrag „Ansicht -> Textdokument formatieren“)

2) Zu Vigenère

Klartext laden von: Vigenere-Plaintext(lateinisch).txt [280 B]

Er stammt von:

http://www.ccbuchner.de/musterseiten/detail/m5980_3.pdf

Gallia est omnis divisa in partes tres,
 quarum unam incolunt Belgae,
 aliam Aquitani tertiam,
 qui ipsorum lingua Celtae,
 nostra Galli appellantur.
 Hi omnes lingua institutis legibus inter se differunt.
 Gallos ab Aquitanis Garunna flumen,
 a Belgis Matrona et Sequana dividit.

*Stammt aus Caesars Buch "De Bello Gallico", 1,1: "Gallia est omnis divisa in partes tres...":
 Caesar wurde das Aufgabengebiet Gallien im Verlauf des Jahres 59 v. Chr. zugesprochen; über seine
 zehn Jahre dauernde Kriegsführung legt er hier Rechenschaft ab.*

- Verschlüsselung: Vigenere mit einem lateinischen Wort für „Angriff“ = PEDATUS
- Analyse: Vigenere-Analyse:
 - a) mit dem deutschen Referenztext findet man das fast richtige Passwort: PLDATUS
 - b) mit dem lateinischen Referenztext C:\program files\CrypTool\reference\genesis-la.txt findet CrypTool : das richtige Passwort.
- Alternativ hätte der Angreifer per Social Engineering erraten können, dass der Verschlüsseler ein Wort aus seiner Strategie wählt und m Netzz.B. die ff. 6 Worte für „Angriff“ finden können:
 invasio, impetus, aggressio, incursio, petitio, pedatus, oppugnatio (Sturmangriff).

- In den Textoptionen kann man es so einstellen, dass Groß- und Kleinbuchstaben und Nichtalphabetzeichen beibehalten bleiben (erhöht die Lesbarkeit)

Textoptionen

Formatierungsoptionen

☐ Nicht im Alphabet enthaltene Zeichen unverändert beibehalten

Groß-/Kleinschreibung

☐ Wenn möglich bei der Ver-/Entschlüsselung Informationen zur Groß-/Kleinschreibung beibehalten

☒ Groß-/Kleinschreibung beachten

Alphabet für Texte definieren

☒ Großbuchstaben ☐ Sonderzeichen

☐ Leerzeichen ☒ Kleinbuchstaben

☐ Ziffern ☐ Umlaute

Zu verwendendes Alphabet (52 Zeichen):

ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz

Referenzdatei für statistische Anwendungen

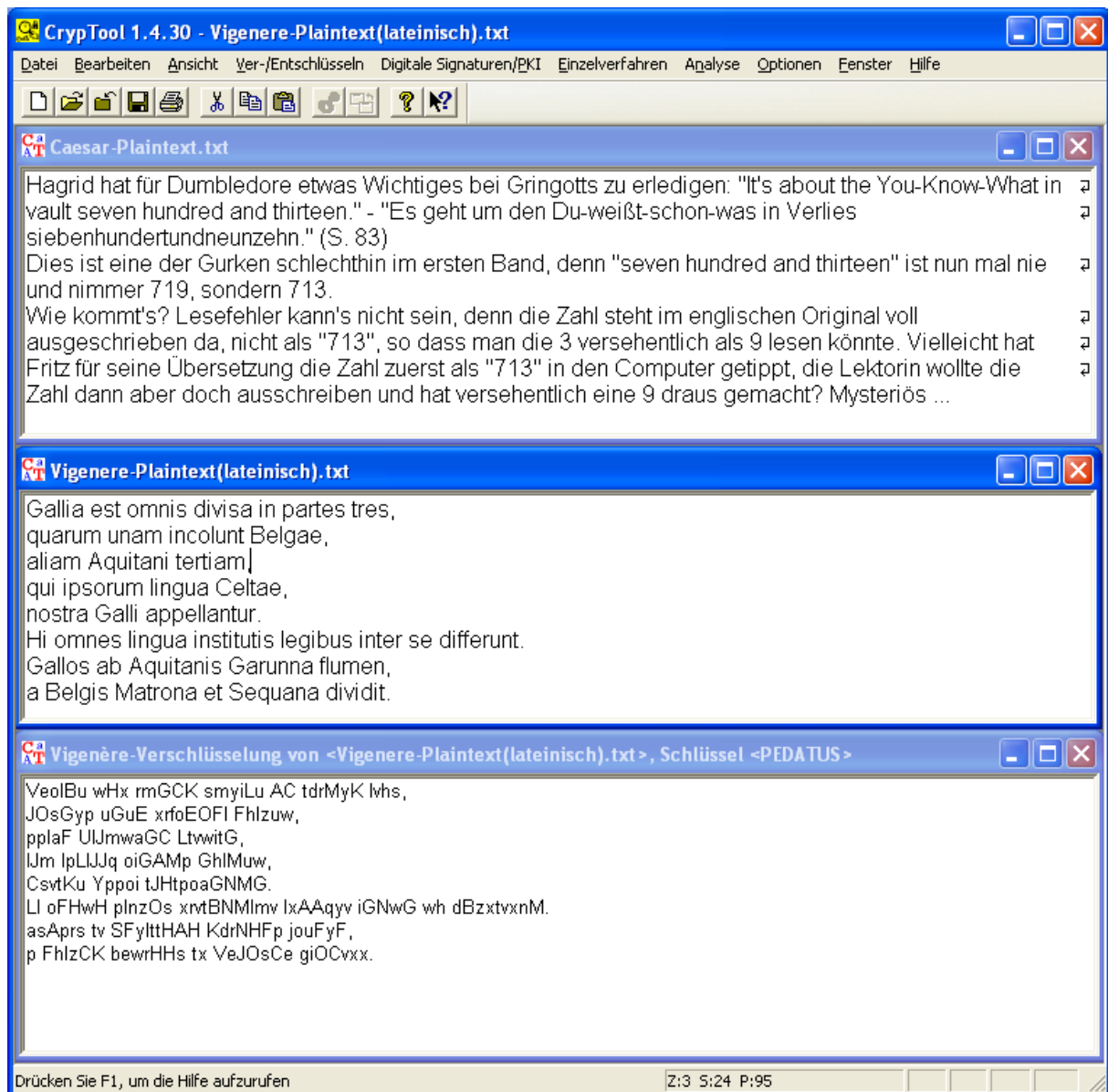
C:\program files\CrypTool\reference\deutsch.txt Suchen ...

Playfair

☒ Doppelbuchstaben trennen Trennzeichen X

Übernehmen Standard wiederherstellen Abbrechen

Screenshot zu den Klartexten und Chiffraten von den Beispielen mit Caesar und Vigenère:



3) Zu Vernam

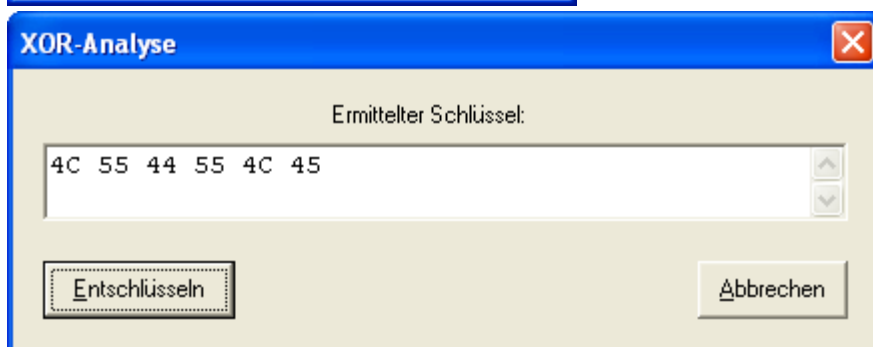
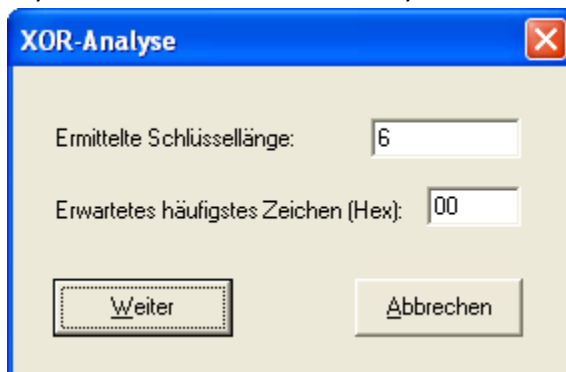
Als Klartext dient die Binärdatei: Vernam-Plain-Binary.PNG [564 B]

Normalerweise braucht man für Vernam, damit es ein sicheres Verfahren ist, einen zufälligen Schlüsselstrom, der mindestens so lang ist wie der Klartext.

Hier soll gezeigt werden, was passiert, wenn man einen zu kurzen Schlüssel verwendet.

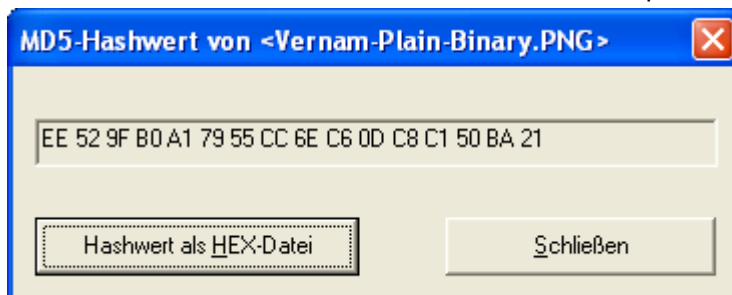
Die Schlüsselstrom-Datei „Vernam-Key1.txt“ enthält das Wort „DUMBLEDORE“,
die Schlüsselstrom-Datei „Vernam-Key2.txt“ enthält das Wort „DUMBL“.

- Die Null kommt in dieser Bilddatei mit Abstand am häufigsten vor (sichtbar machen per Histogramm!), so dass auch hier eine Vigenère-artige Analyse Erfolg haben kann.
- Key1: DUMBLEDORE → XOR-Analyse findet nicht den richtigen Key:



Key2: DUMBL → XOR-Analyse findet Key der Länge 5: 44 55 4D 42 4C

- Prüfen auf Korrektheit der entschlüsselten Binärdatei per Hashverfahren:



→ Die Analyse von Binärdateien ist hier einfach automatisierbar (mit Autokorrelation) !

➔ Für die Analyse muss man wissen, dass XOR und Vernam denselben Verschlüsselungsalgorithmus verwenden

(Unterschied ist nur die Schlüssel-Eingabe: XOR Hexwerte per Maske,

Vernam per Datei mit zusätzlicher Prüfung auf die Länge und Warnung, wenn zu kurz)

4) Zu RSA

Durchführen eines Angriffs auf eine RSA-verschlüsselte Datei.

Siehe aktuelle Cryptool-Präsentation,
Folie 50-55 "Attack on RSA encryption with short RSA modulus".

The collage consists of six slides, each showing a different step in the attack process:

- Slide 46: Anwendungsbeispiele (2)** - Shows a diagram of the RSA encryption process. A document is encrypted using a public key, and the resulting ciphertext is shown. The slide notes that the document is now protected and can only be decrypted by the intended recipient.
- Slide 47: Anwendungsbeispiele (3)** - Shows the RSA modulus N and the public exponent e . The slide lists the values of N and e and states that the task is to find the private key d . It also mentions that the modulus N is short, which makes it vulnerable to factoring.
- Slide 48: Anwendungsbeispiele (3)** - Shows the RSA modulus N and the public exponent e . The slide lists the values of N and e and states that the task is to find the private key d . It also mentions that the modulus N is short, which makes it vulnerable to factoring.
- Slide 49: Anwendungsbeispiele (3)** - Shows the RSA modulus N and the public exponent e . The slide lists the values of N and e and states that the task is to find the private key d . It also mentions that the modulus N is short, which makes it vulnerable to factoring.
- Slide 50: Anwendungsbeispiele (3)** - Shows the RSA modulus N and the public exponent e . The slide lists the values of N and e and states that the task is to find the private key d . It also mentions that the modulus N is short, which makes it vulnerable to factoring.
- Slide 51: Anwendungsbeispiele (3)** - Shows the RSA modulus N and the public exponent e . The slide lists the values of N and e and states that the task is to find the private key d . It also mentions that the modulus N is short, which makes it vulnerable to factoring.