JavaCrypTool (www.cryptool.org)

Online-Hilfe zur Bedienung der Fleißner-Schablone

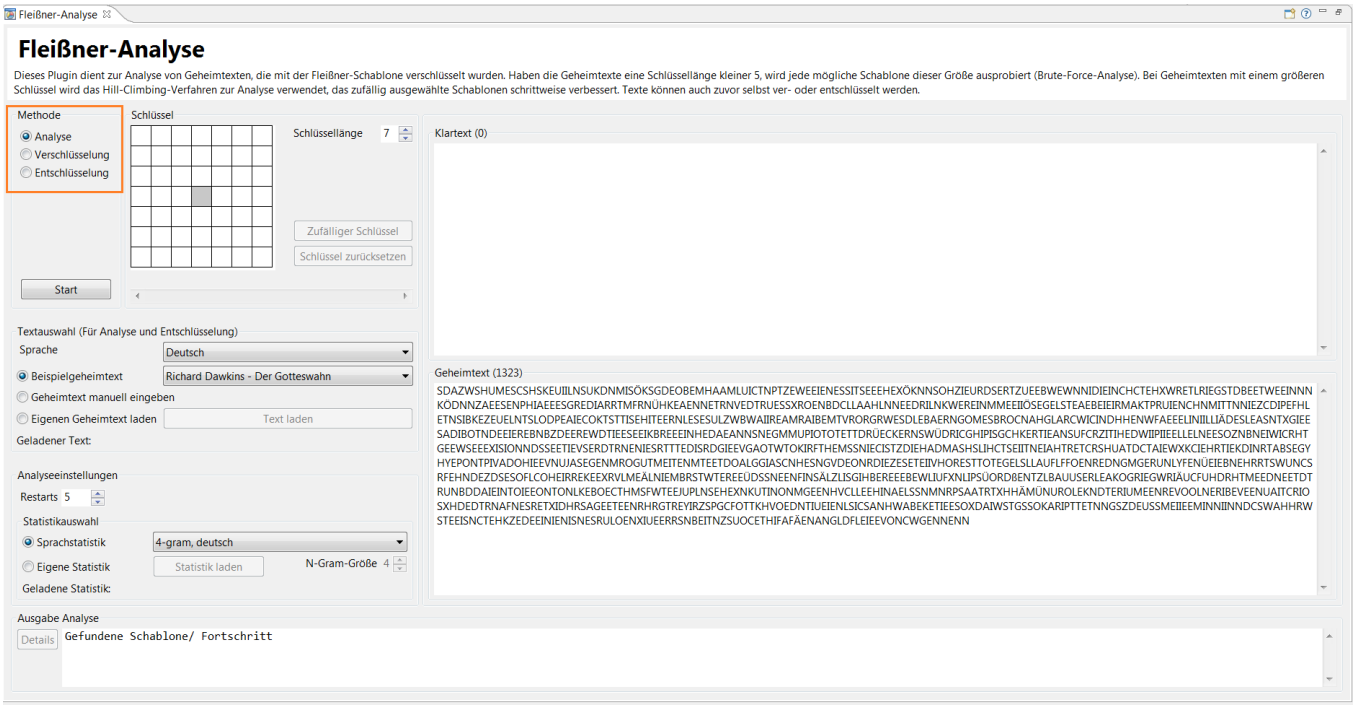
Inhaltsverzeichnis

Die Hauptfunktion dieses Plug-ins ist die Analyse eines Geheimtextes, der durch die Fleißner-Schablone verschlüsselt wurde. Als Schlüssel gilt der Inhalt der Schablone. Etwas unüblich als Schlüssellänge bezeichnet man dabei die Seitenlänge des quadratischen Feldes (Schablone).

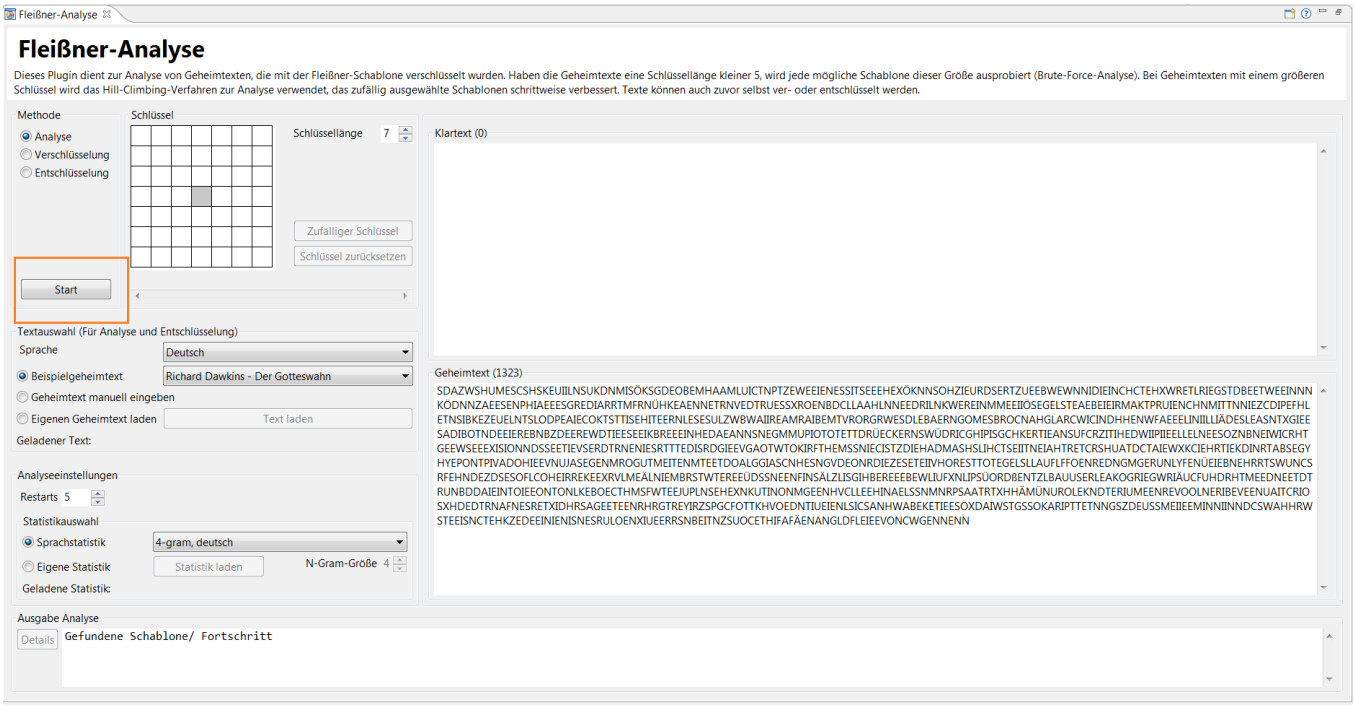
Neben der Analysefunktion stehen in diesem Plug-in auch die Funktionen Verschlüsselung und Entschlüsselung zur Verfügung.

1 Analyse

In der Ausgangseinstellung des Plug-ins (Default-Einstellung) sitzt der Radiobutton bei der Analysefunktion: Sie ist in der ersten Gruppierung „Methode“ ausgewählt. Hier kann die Methode auch auf die Verschlüsselung oder Entschlüsselung geändert werden.

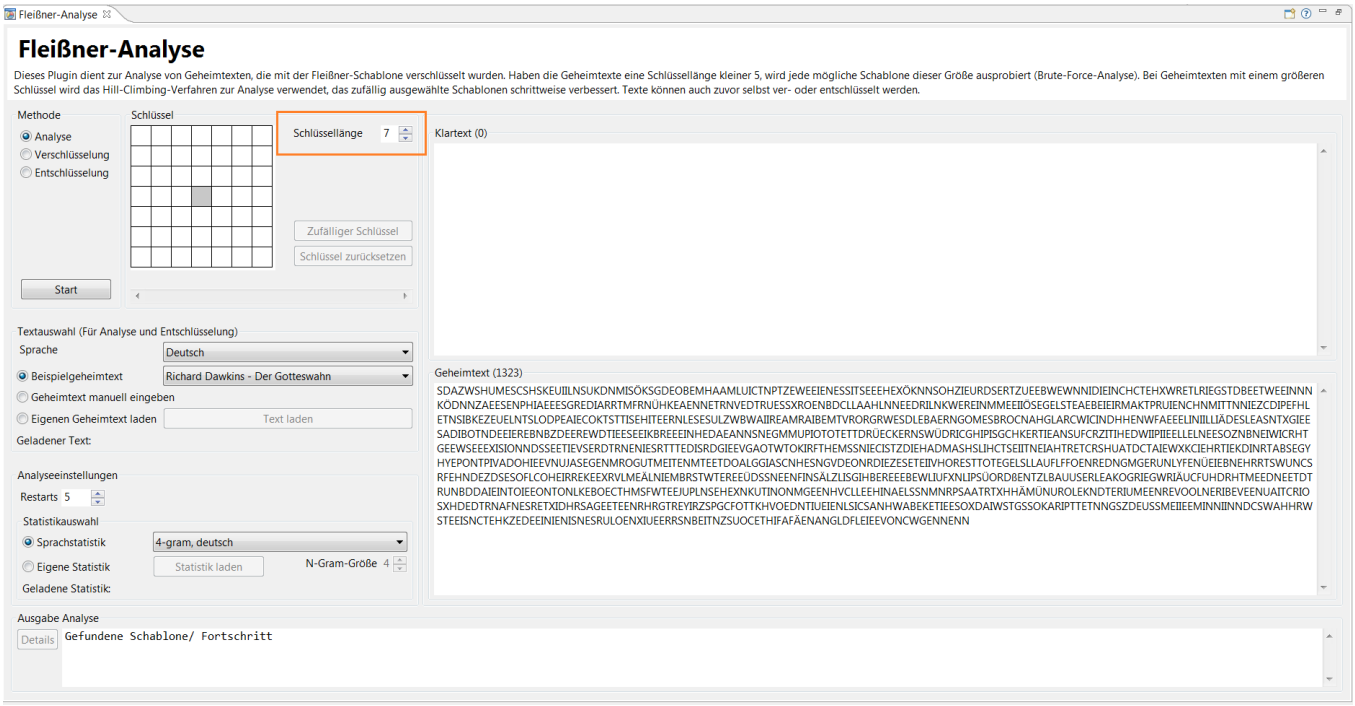


Da beim Start des Plug-ins Vorgabewerte auch für den Geheimtext gesetzt werden, kann die Analyse durch die Betätigung des „Start“-Buttons direkt ausgeführt werden.



1.1 Schlüssellänge

Da der genutzte Schlüssel für die Analyse in der Regel geheim ist und erst gefunden werden soll, ist das Schlüsselfeld selbst bei dieser Funktionsauswahl deaktiviert. Die Schlüssellänge kann aber gewählt werden und sollte mit der des, für diesen Geheimtext verwendeten, Schlüssels übereinstimmen.



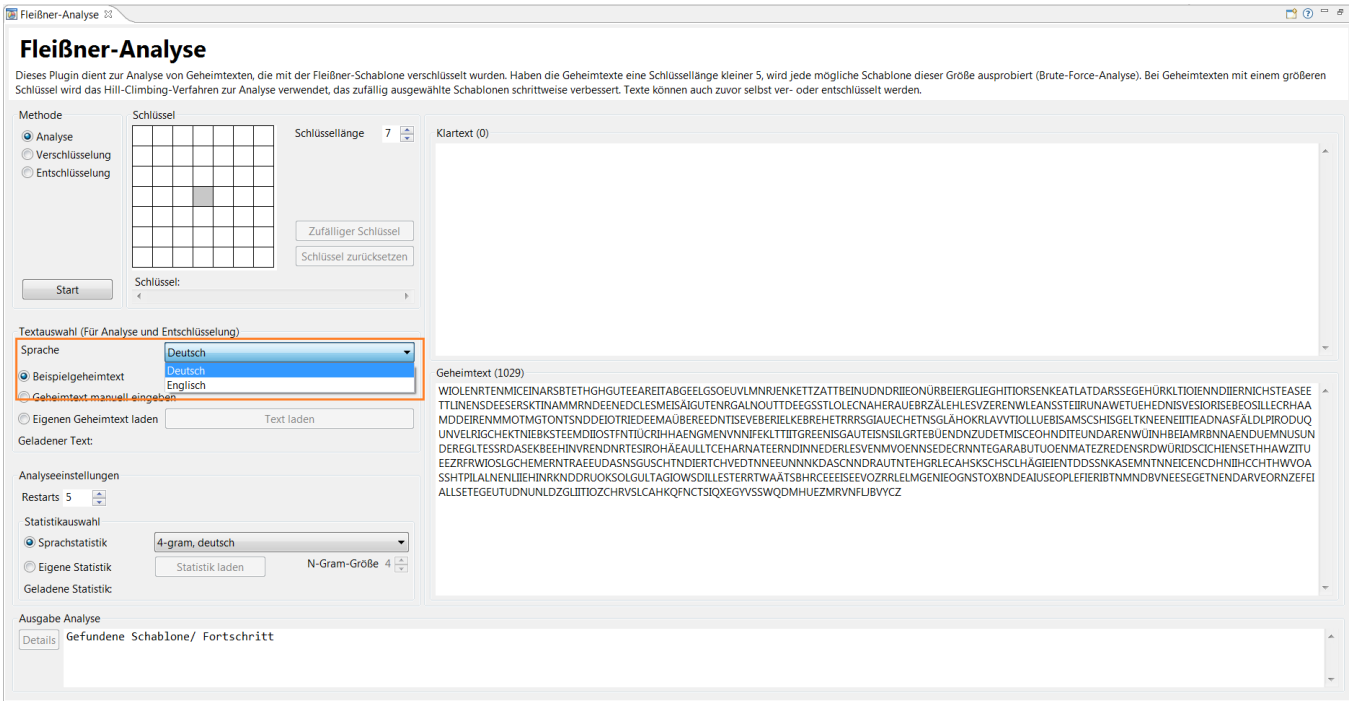
Ist bei der Textauswahl „Beispielgeheimtext“ (Voreinstellung) ausgewählt, so wird der Geheimtext der jeweiligen Schlüssellänge angepasst. Der dazu verwendete Schlüssel wird zufällig erzeugt und nach der Verschlüsselung wieder verworfen.

1.2 Textauswahl

1.2.1 Sprache

In dieser Gruppierung kann zwischen den Sprachen „Deutsch“ und „Englisch“ gewählt werden. Ist im Abschnitt Texteingabe „Beispielgeheimtext“ ausgewählt, so wird der angezeigte Text entsprechend der ausgewählten Sprache aktualisiert.

Für einen manuell eingegebenen oder geladenen Geheimtext, muss die Sprache manuell ausgewählt werden. Der zu analysierende Text muss der hier ausgewählten Sprache entsprechen, da die Analyse auf sprachspezifischen Auftrittswahrscheinlichkeiten von Buchstabenketten beruht.



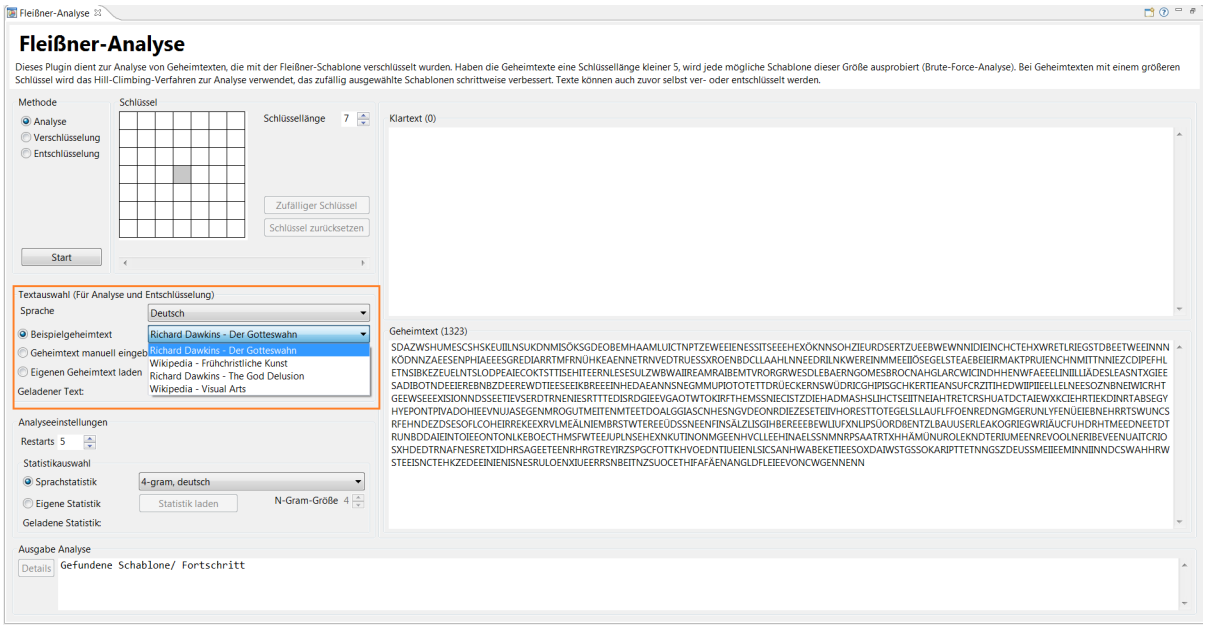
1.2.2 Texteingabe

In dieser Gruppierung kann die Art der Eingabe des Geheimtextes ausgewählt werden.

(a) **Beispielgeheimtext**

Voreingestellt ist hier die Auswahl „Beispielgeheimtext“. Hier kann zwischen zwei deutschsprachigen und zwei englischsprachigen Geheimtexten gewählt werden. [1]

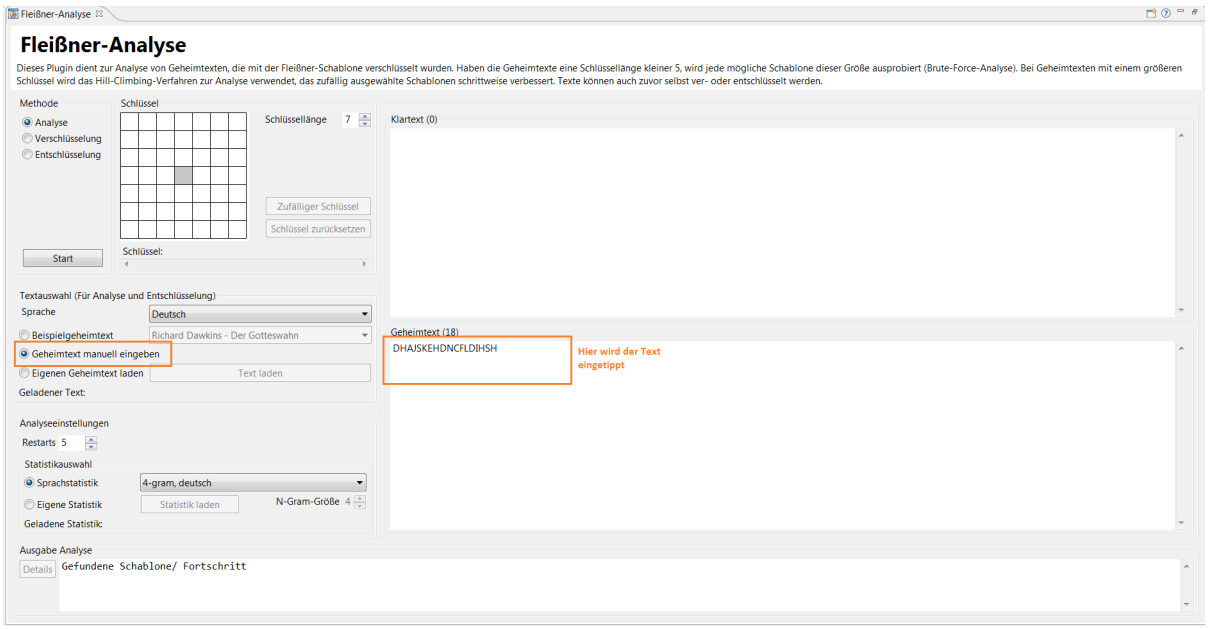
Die Texte werden je nach ausgewählter Schlüssellänge entsprechend verschlüsselt.



[1] **Quellen:**
Richard Dawkins - Der Gotteswahn
Richard Dawkins - The God Delusion
`https://de.wikipedia.org/wiki/Bildende_Kunst#Fr%C3%BChchristliche_und_byzantinische_Kunst`
`https://en.wikipedia.org/wiki/Visual_arts`

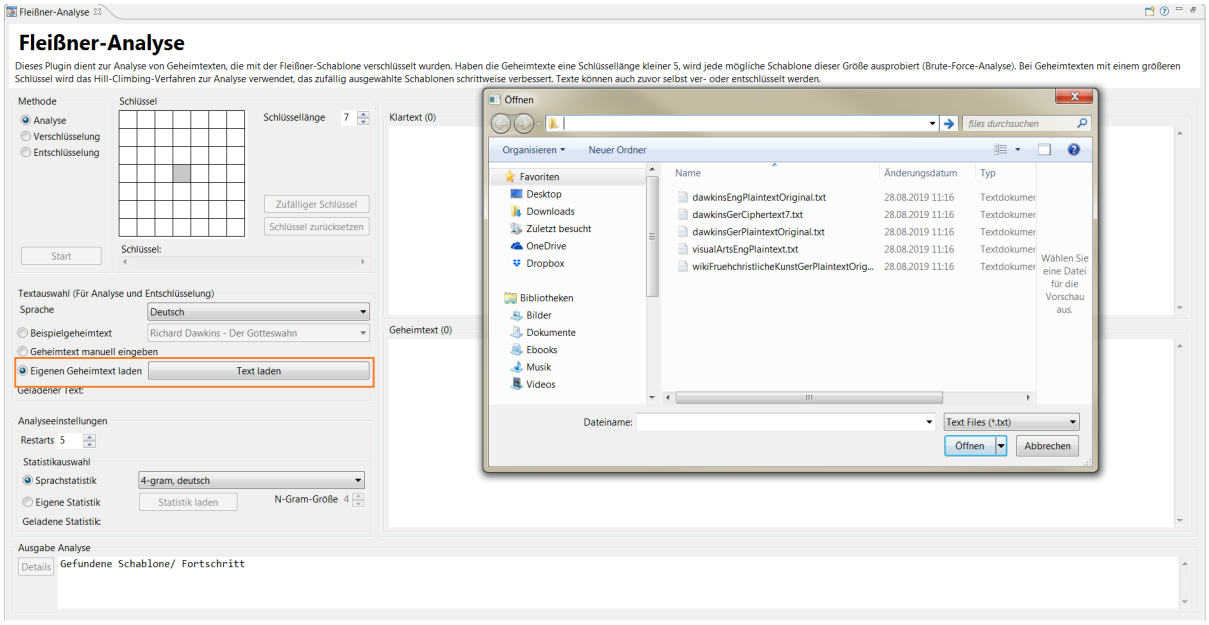
(b) Geheimtext manuell eingeben

Bei der Auswahl von „Geheimtext manuell eingeben“ wird das Feld für den Geheimtext für die manuelle Eingabe freigeschaltet und es kann ein Text eingetippt werden.



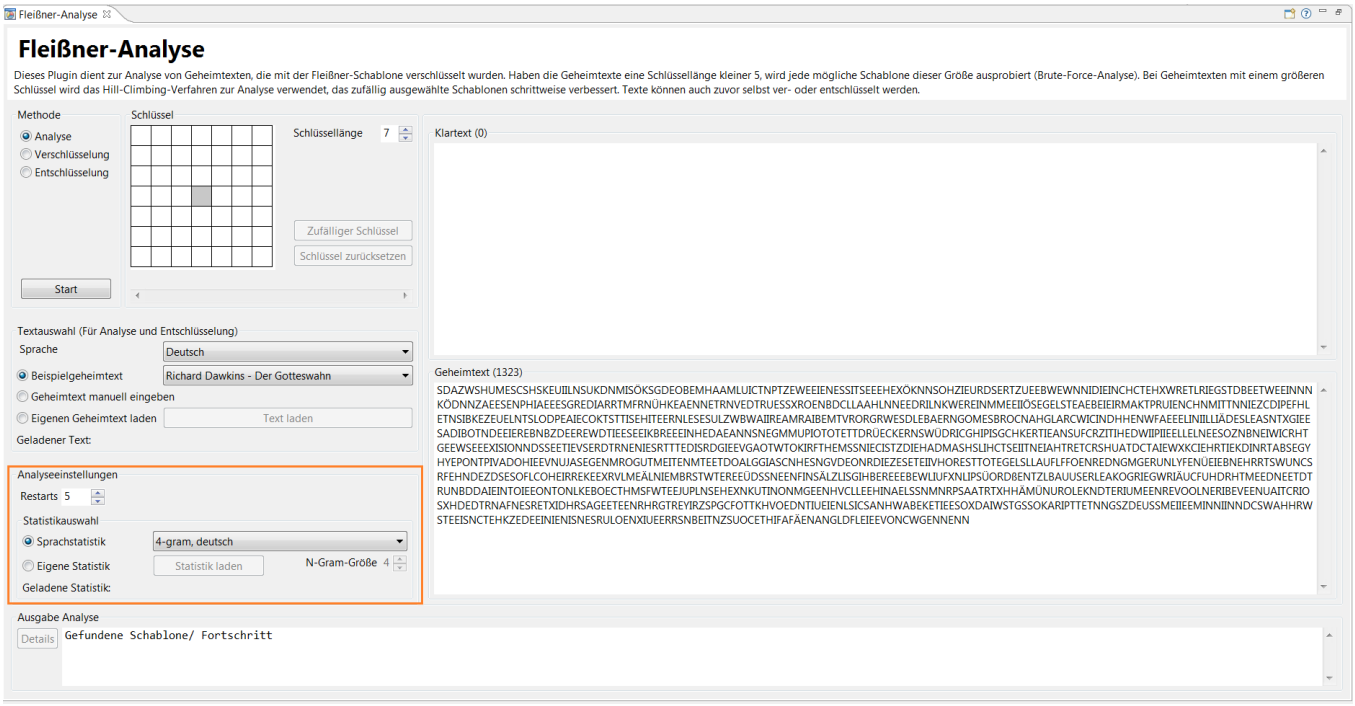
(c) Eigenen Geheimtext laden

Zum Laden eines Geheimtextes aus einer Datei dient die letzte Auswahl „Eigenen Geheimtext laden“. Bei dieser Auswahl wird der Button „Text laden“ aktiviert, über den dann eine Textdatei (*.txt) geladen werden kann. Der Text wird dann im Geheimtextfeld angezeigt.



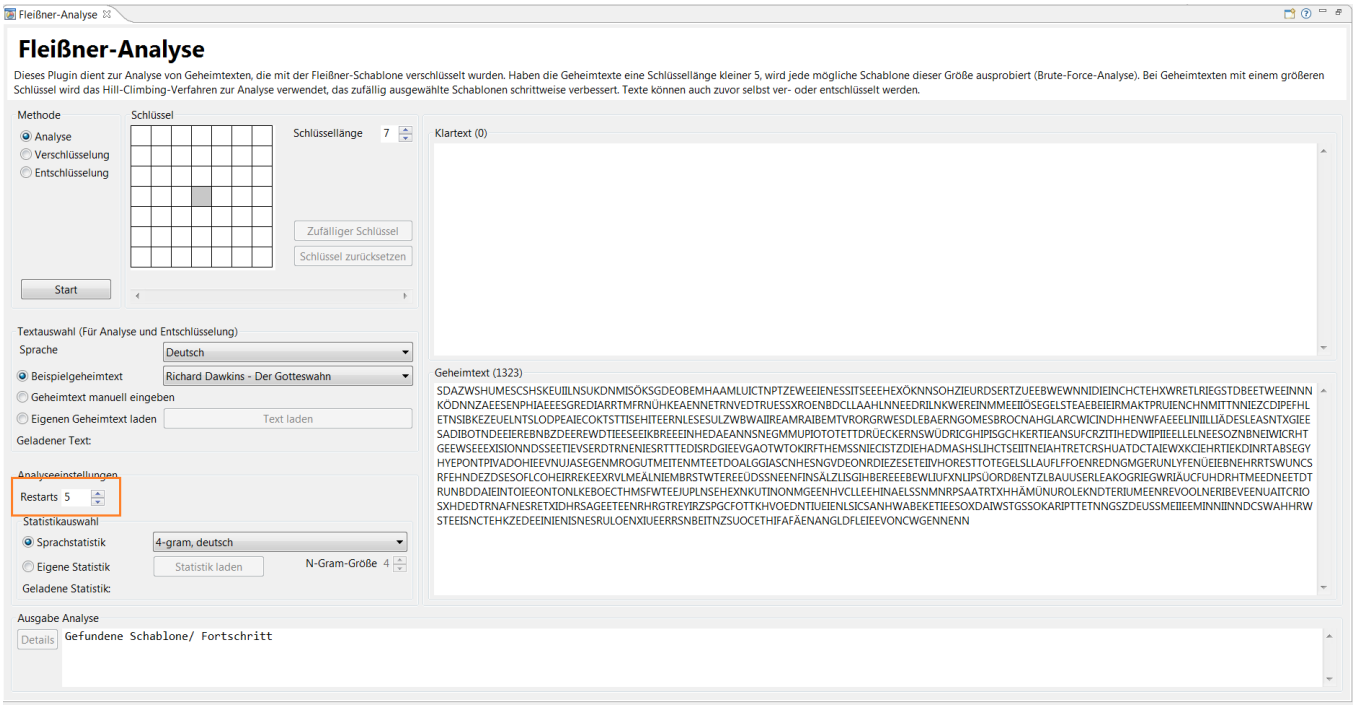
1.3 Analyseeinstellungen

Die Gruppierung „Analyseeinstellungen“ befindet sich direkt unter der Gruppierung „Textauswahl“ und ist nur für die Analysefunktion aktiviert.



1.3.1 Restarts

Die Anzahl der Restarts ist relevant für die Analyse von Geheimtexten, die mit Schlüsseln der Größe 5 oder höher verschlüsselt wurden. Bei diesen Schlüsselgrößen wird das „Hill-Climbing“-Verfahren zur Analyse verwendet. Für jeden Restart wird zufällig eine Schablone in der gewählten Schlüssellänge erstellt. Diese Schablone wird dann schrittweise verändert, bis kein besserer Klartext durch die veränderte Schablone erzeugt werden kann. Je höher die Anzahl der Restarts, desto höher ist die Wahrscheinlichkeit, dass der richtige Schlüssel durch die Analyse gefunden wird.

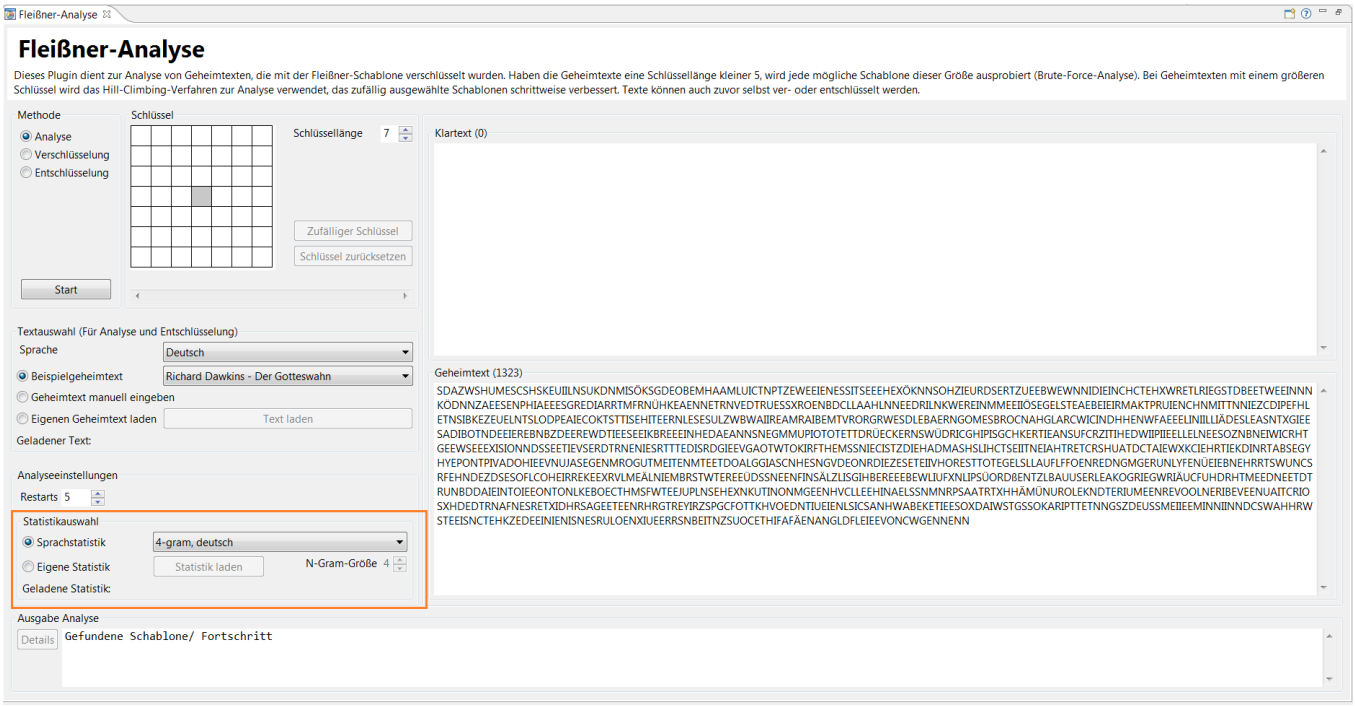


Achtung: Für große Schlüssel und eine hohe Restartanzahl ist mit einer langen Analysedauer zu rechnen. [2]

1.3.2 Sprachstatistik

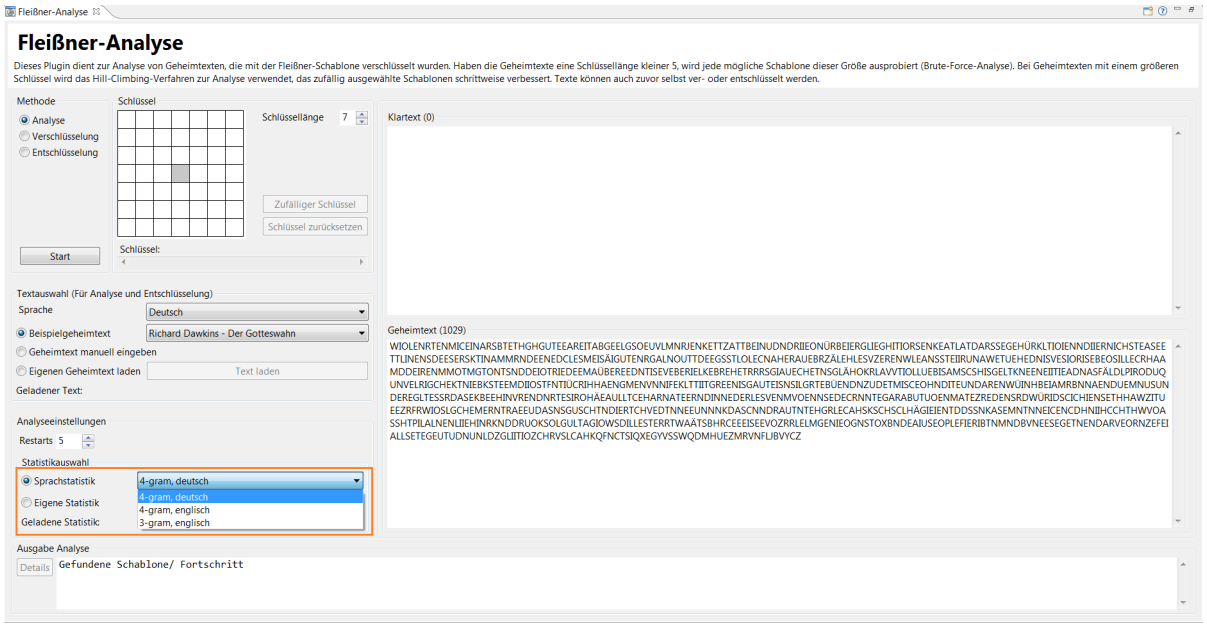
Die Sprachstatistik ist essentiell für die Analyse eines Geheimtextes. In ihr sind die Auftrittswahrscheinlichkeiten aller zusammenhängenden Zeichenketten einer bestimmten Länge n (n-Gramme) in der jeweiligen Sprache angegeben. Die Sprache des Geheimtextes muss mit der ausgewählten oder geladenen Statistik übereinstimmen, sonst sinkt die Erfolgswahrscheinlichkeit erheblich.

[2] Anhang: Evaluation der Analyse



(a) **Sprachstatistik**

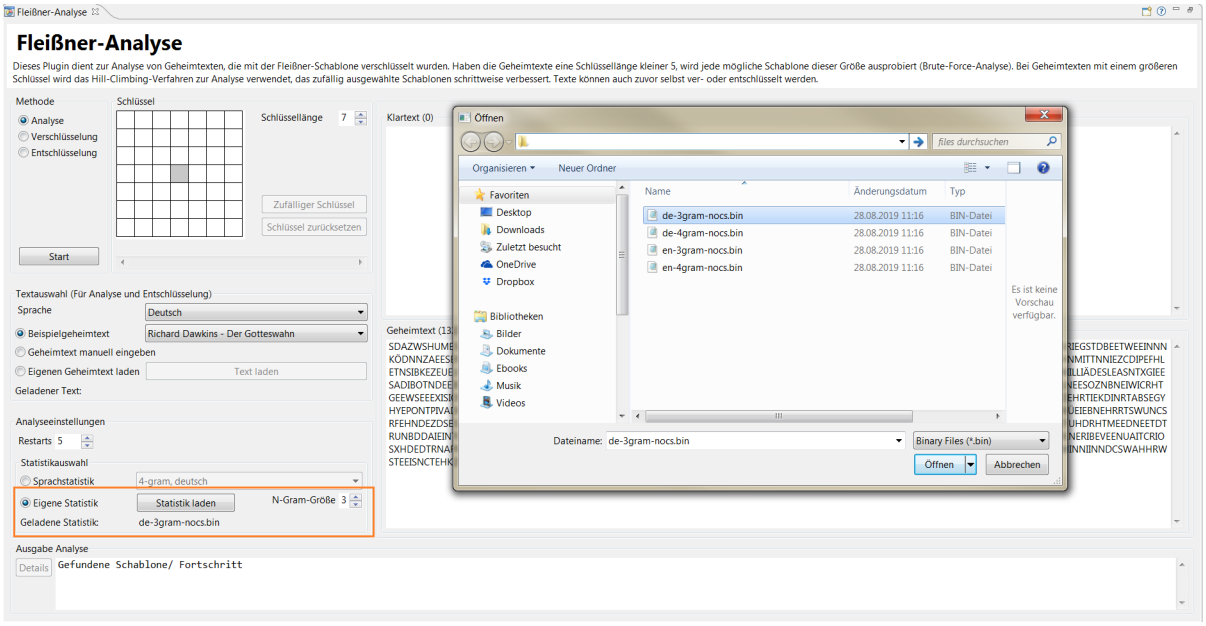
Zur Ausführung der Analyse kann eine der drei hinterlegten Statistiken genutzt werden.



(b) **Eigene Statistik**

Es kann aber auch eine eigene Sprachstatistik-Datei geladen werden. Hierzu gelten gewisse *Anforderungen* an das Format der Sprachstatistik: Im Vergleich zu anderen Sprachstatistiken, sollten sich für dieses Plug-in die tatsächlichen n-Gramme nicht in der Datei befinden. Die genutzte Sprachstatistik sollte nur die bereits logarithmisierten Werte der jeweiligen n-Gramme enthalten. Dazu wird die Sprachstatistik wie ein n-dimensionaler Würfel aufgebaut, wobei

die Position der Buchstaben im Alphabet sowie die Position jedes Buchstaben im n-Gramm gemeinsam den Index für den Wert zum jeweiligen n-Gramm angeben.



Beispiel: Zum Speichern und Abrufen des Quadgramms „Ihre“ in einer deutschen Quadgramm-Statistik geht man wie folgt vor (wobei Kleinbuchstaben wie Großbuchstaben behandelt werden):

Das deutsche Alphabet wird mit angehängten Umlauten in einer Länge von 30 in der Form „ABC...XYZÄÖÜß“ angegeben, wobei jedem Buchstaben ein Index von 0 bis 29 zugeordnet wird. Für das Quadgramm „Ihre“ wird nun jeder Buchstabenindex des Quadgramms mit einer Potenz der Alphabetlänge in Abhängigkeit der Position im Quadgram multipliziert. Diese vier Werte werden addiert und ergeben zusammen den Index des Quadgrammwerts in der Sprachstatistik. So wie gerade erläutert, wird den Buchstaben I, h, r und e jeweils der Index 8, 7, 17 und 4 zugeordnet. Man berechnet nun

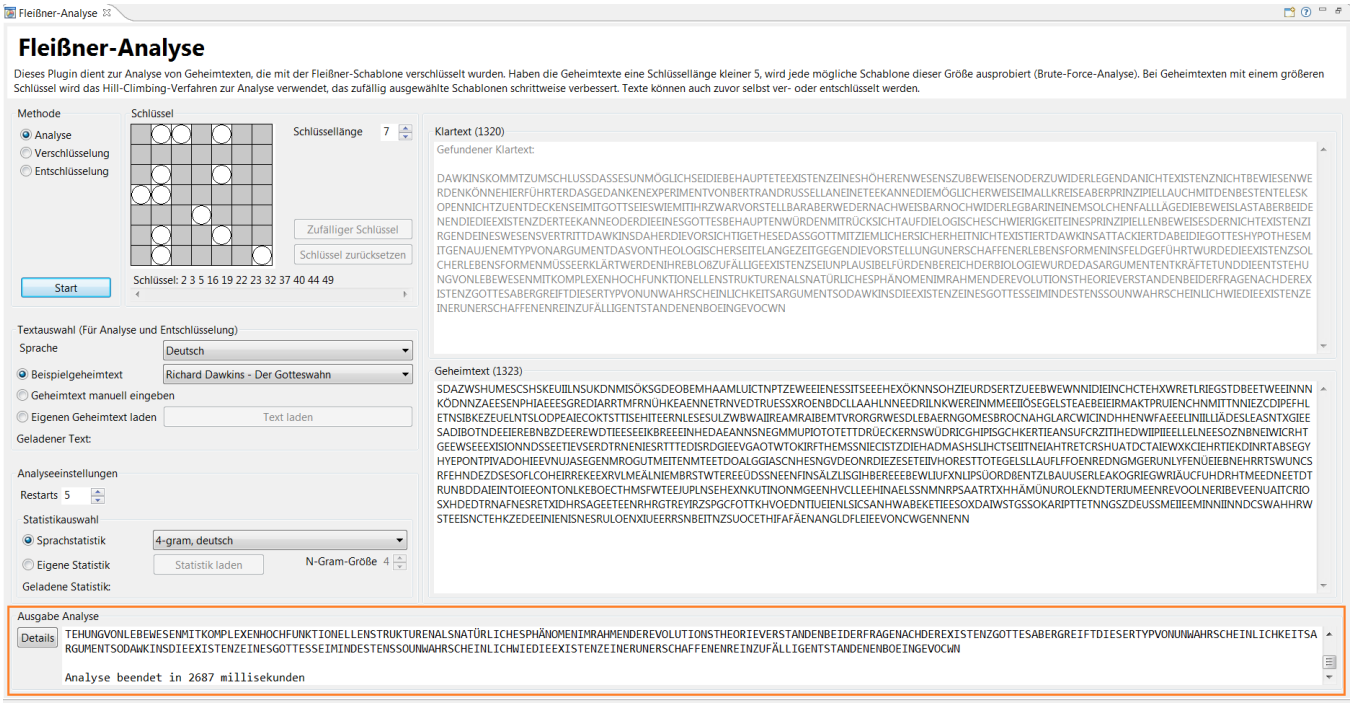
$$8 * 30^3 + 7 * 30^2 + 17 * 30^1 + 4 * 30^0 = 222.814$$

für den Index des Quadgramms „Ihre“ in einer deutschen Quadgramm-Statistik.

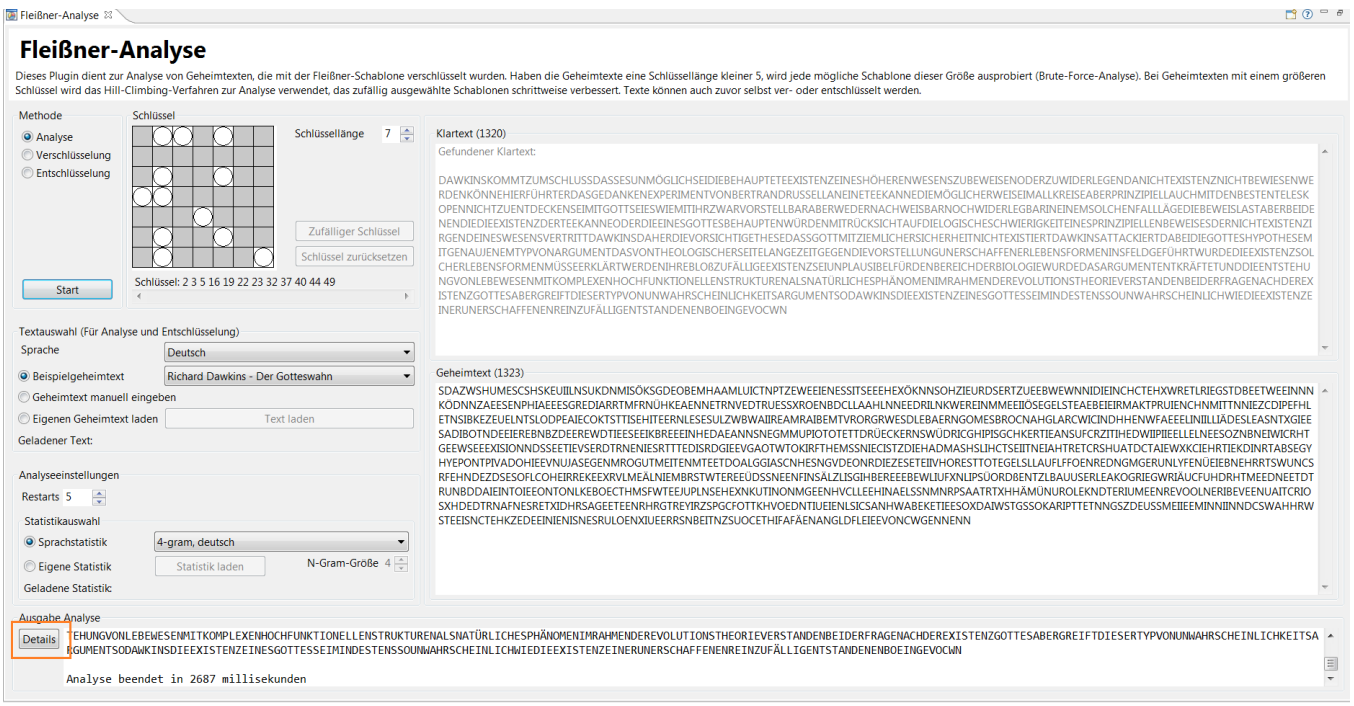
Wird eine eigene Sprachstatistik geladen, so muss hier in der Gruppierung „Statistikauswahl“ zusätzlich die Größe der n-Gramme noch manuell angegeben werden.

1.4 Ausgabe der Analyse

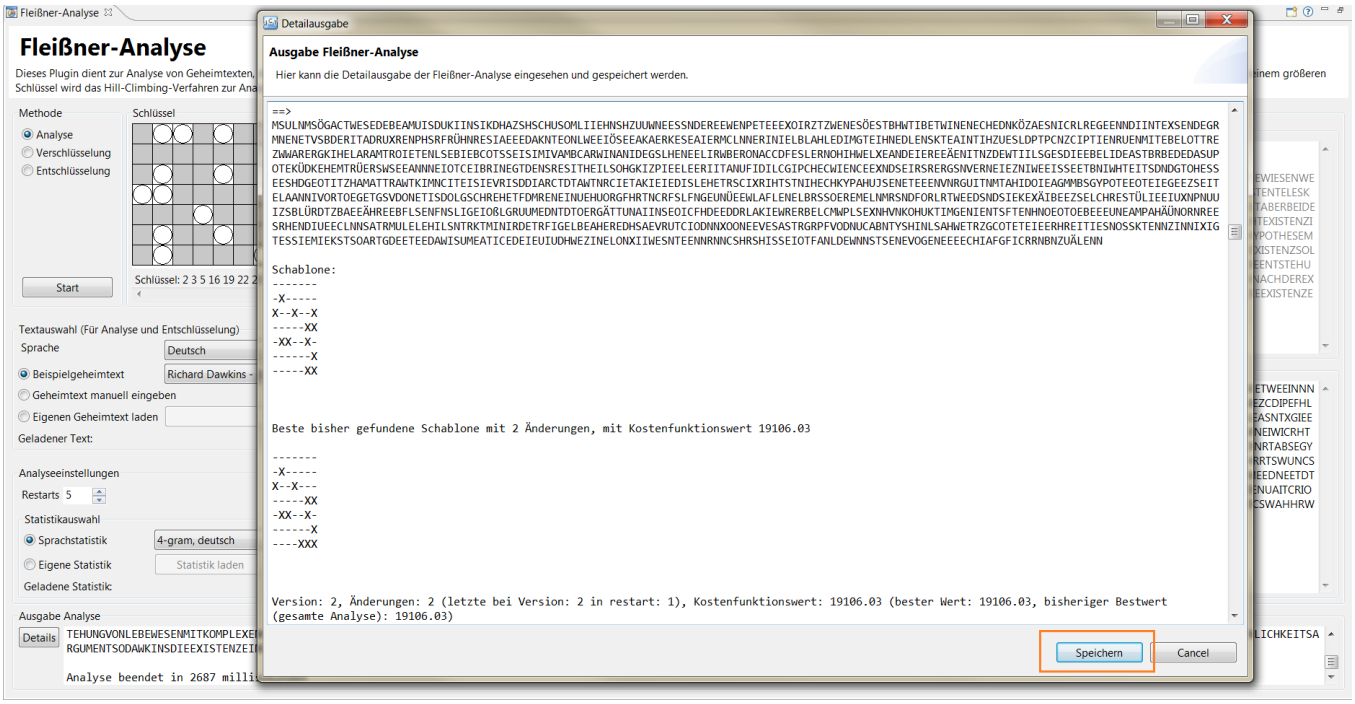
Am unteren Bildschirmrand befindet sich das Ausgabefenster zur Analyse. Hier werden zu Beginn der Analyse die ausgewählten Parameter angezeigt. Nach Abschluss der Analyse werden zusätzlich zur gefundenen Schablone der dadurch erzeugte Klartext sowie die benötigte Zeit hinzugefügt.



Für mehr Informationen befindet sich auf der linken Seite des Ausgabefelds der Button „Details“.



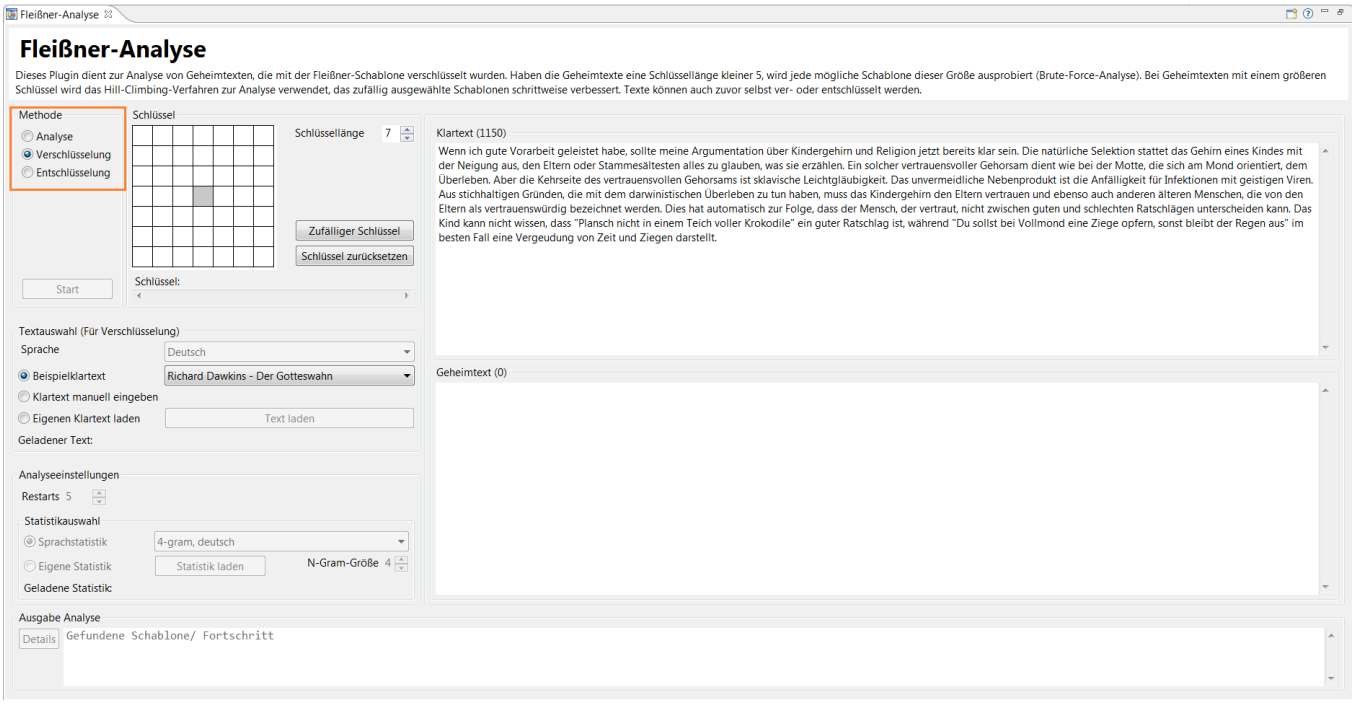
Damit öffnet sich ein neues Dialogfenster, in dem zusätzlich zu den Informationen aus dem Ausgabefenster auch Zwischenausgaben aus dem Analyseprozess angezeigt werden. Diese Ausgabe kann dann auch als Textdatei (*.txt) gespeichert werden.



Nach Abschluss der Analyse wird der gefundene Schlüssel auch im Schlüsselfeld selbst angezeigt, so dass dieser beispielsweise direkt zur Entschlüsselung und damit Validierung des Analyseergebnisses verwendet werden kann.

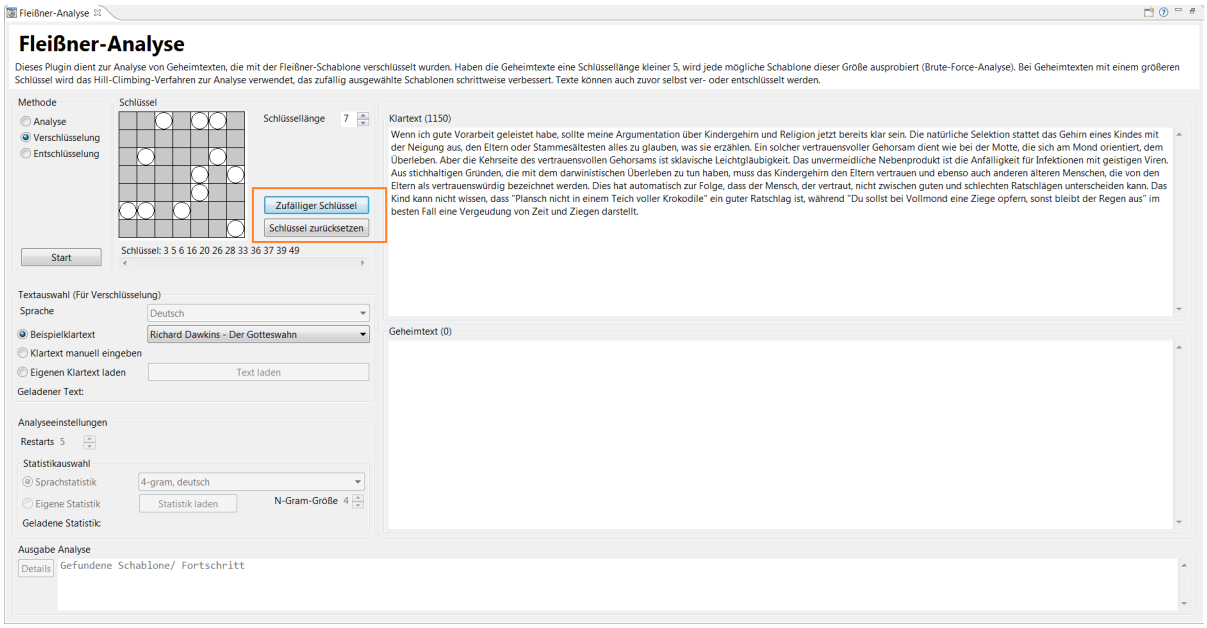
2 Verschlüsselung

In diesem Plug-in können Klartexte auch selbst verschlüsselt werden. Dazu wird in der Gruppierung „Methode“ die Funktion „Verschlüsselung“ ausgewählt. Dies aktiviert auch die Buttons zum Schlüssel-Erzeugen und -Zurücksetzen (ist Analyse ausgewählt, sind diese beiden Buttons deaktiviert).



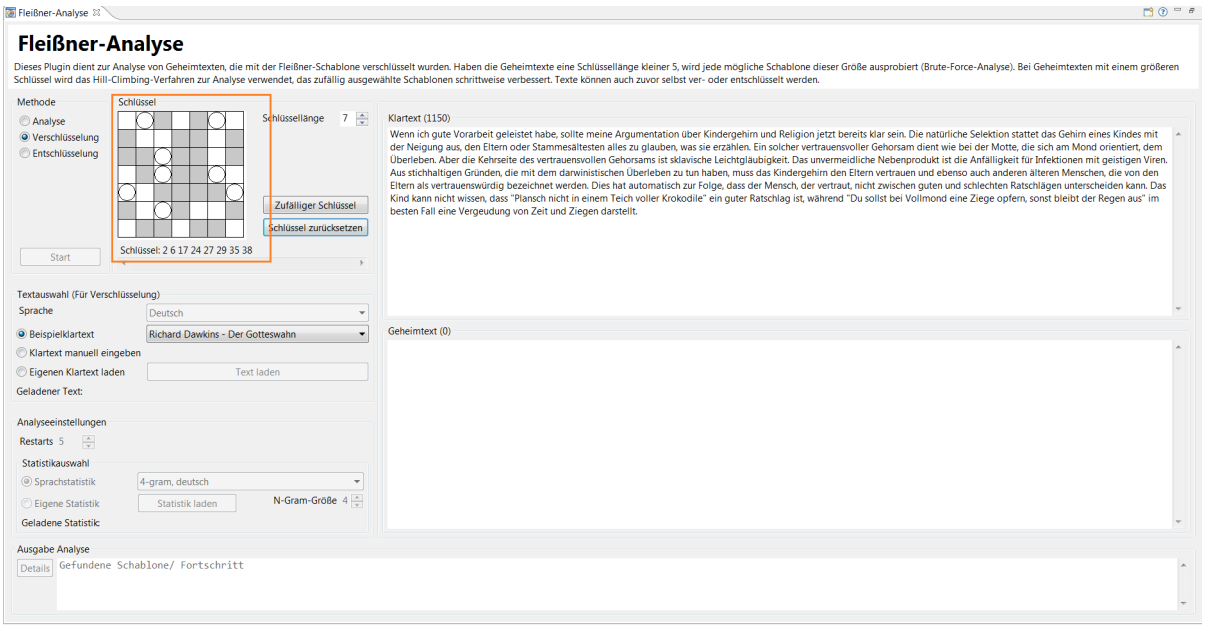
(a) Zufälliger Schlüssel

Durch die Betätigung des Buttons „Zufälliger Schlüssel“ wird ein zufälliger Schlüssel erzeugt und angezeigt.



(b) Manuelle Erstellung eines Schlüssels

Für die manuelle Erstellung eines Schlüssel wählt man die Felder aus, an denen die Schablone die Löcher zum Eintragen des Klartextes enthalten soll. Für jedes ausgewählte Feld werden zugleich in den anderen 3 Quadranten die drei zugehörigen Felder blockiert, die durch die Rotation im Verschlüsselungsprozess benötigt werden. Wird ein bereits ausgewähltes Feld noch einmal angeklickt, so wird die Auswahl dieses Feldes rückgängig gemacht.



Um die Auswahl aller Felder rückgängig zu machen, drückt man den „Schlüssel zurücksetzen“-Button.

Die ausgewählten Löcher des Schlüssels werden auch in Zahlenform unter dem Schlüsselfeld angezeigt. Die Felder sind hierzu von oben links nach unten rechts nummeriert (beginnend mit 1).

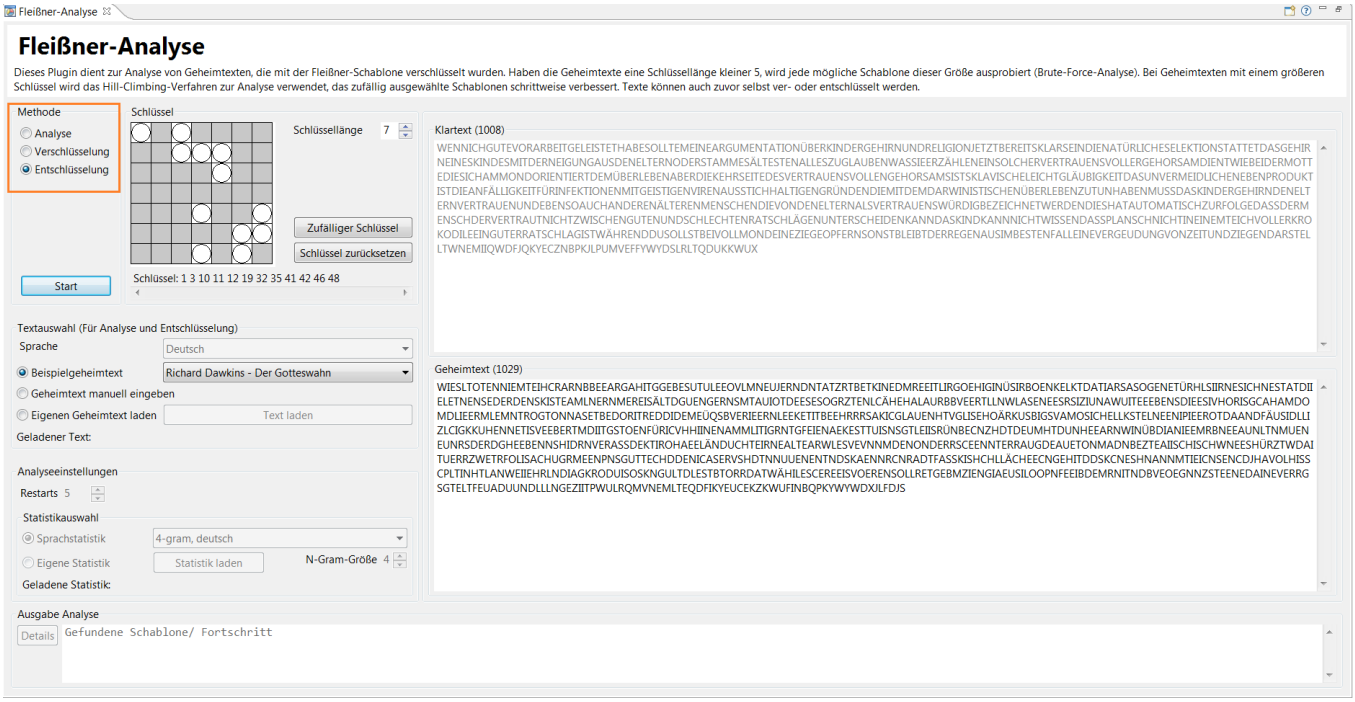
Zur Verschlüsselung ist neben dem Schlüssel auch ein Klartext erforderlich. Dieser kann wie auch in der Analysefunktion aus einer Menge von Beispieltexten gewählt, selbst eingetippt oder geladen werden. Bei der Auswahl von Beispieltexten wird die ausgewählte Funktion des Plug-ins erkannt und dementsprechend ein Klar- oder Geheimtext in das entsprechende Fenster geladen. Bei eigenen Texten muss diese Unterscheidung selbst getroffen werden. Das Plug-in erkennt bei selbst geladenen Texten nicht, ob ein Klartext oder ein Geheimtext vorliegt.

Liegt ein gültiger Schlüssel sowie ein Text im Klartextfeld vor, wird der „Start“-Button aktiviert und die Verschlüsselung kann durchgeführt werden.

Nach Änderung der Methodenwahl auf „Analyse“ oder „Entschlüsselung“ kann mit dem selbst erzeugten Geheimtext fortgefahren werden.

3 Entschlüsselung

Als letzte Funktionalität bietet das Plug-in eine Entschlüsselung an. Diese kann beispielsweise genutzt werden, um einen aus einer Analyse erhaltenen Schlüssel anzuwenden, aber auch um eigene Geheimtexte zu entschlüsseln.



Für die Entschlüsselung sowie auch schon für die Verschlüsselung wird ein gültiger Schlüssel und ein nichtleeres Geheimtextfeld benötigt. Die Bedienung der Textauswahl ist hier analog zu den beiden bereits beschriebenen Methoden.