Online-Hilfe zur Fleißner-Schablone

Inhaltsverzeichnis

1 Analyse **2**

1.1 Schlüssellänge 3

1.2 Textauswahl 4

1.3 Analyseeinstellungen 6

1.3.1 Sprache 6

1.3.2 Restarts 7

1.3.3 Sprachstatistik 8

1.4 Ausgabe der Analyse 10

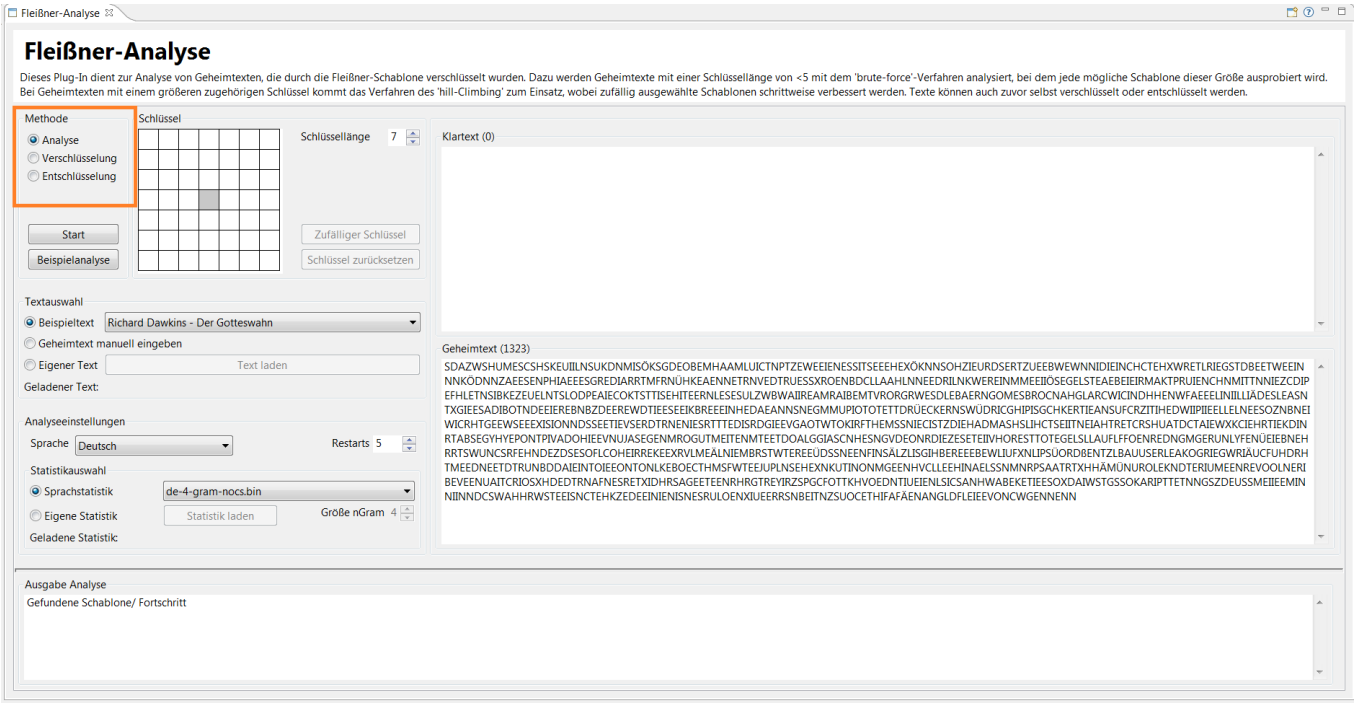
2 Verschlüsselung **11**

3 Entschlüsselung **13**

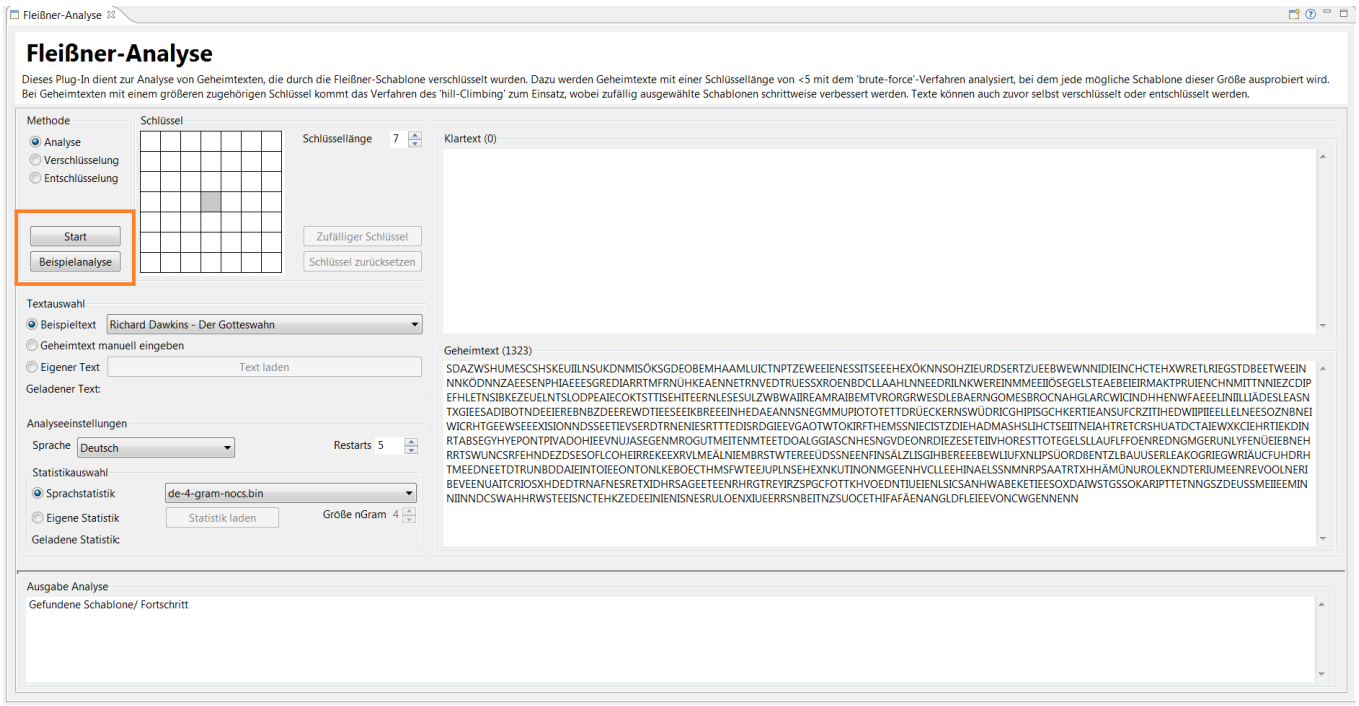
Die Hauptfunktion dieses Plug-Ins ist die Analyse eines Geheimtextes, der durch die Fleißner-Schablone verschlüsselt wurde, unter Angabe der jeweiligen Schlüssellänge. Die Schlüssellänge ist dabei die Seitenlänge des quadratischen Feldes. Neben der Analysefunktion stehen auch die Funktionen Verschlüsselung und Entschlüsselung zur Verfügung.

1 Analyse

Die Analysefunktion ist die Ausgangseinstellung des Plug-Ins und ist im ersten Feld für „Methode“ ausgewählt. Hier kann die Methode auch auf die Verschlüsselung oder Entschlüsselung geändert werden.

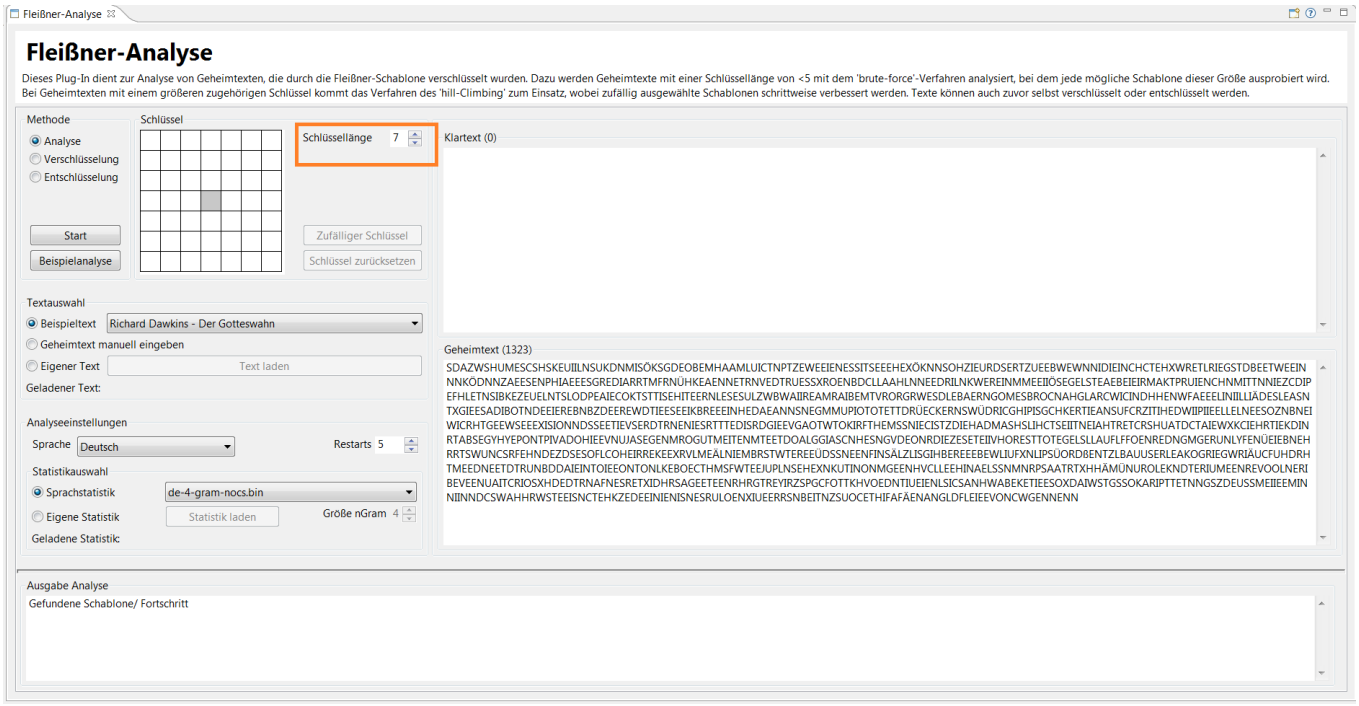


Da für den Start des Plug-Ins Vorgabewerte gesetzt werden, kann die Analyse durch die Betätigung des „Start“-Buttons direkt ausgeführt werden. Der darunterliegende „Beispielanalyse“-Button führt eine Analyse mit genau diesen vorgegebenen Parametern zu jedem Zeitpunkt durch und setzt alle Werte auf den Ausgangszustand zurück.



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.

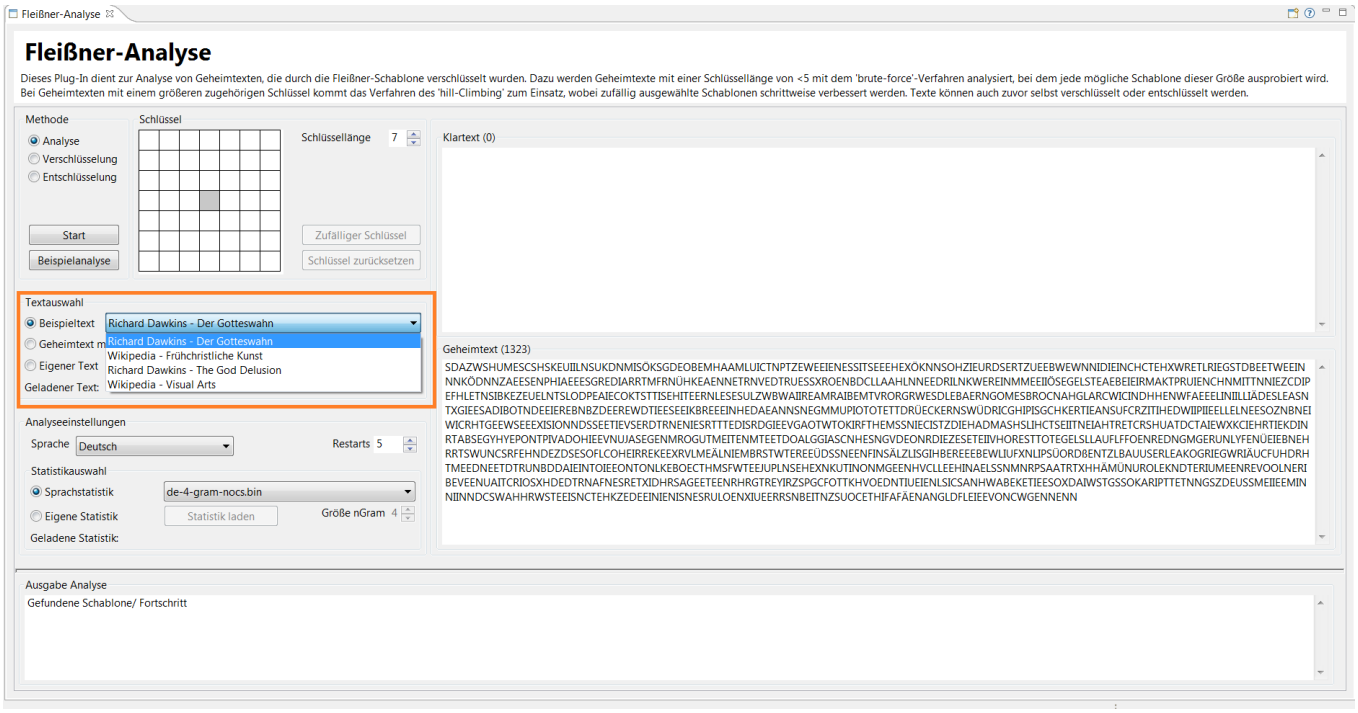


Ist bei der Textauswahl „Beispieltext“ (Voreinstellung) ausgewählt, so wird der Geheimtext der

jeweiligen Schlüssellänge angepasst. Der dazu verwendete Schlüssel wird zufällig erzeugt und nach der Verschlüsselung wieder verworfen.

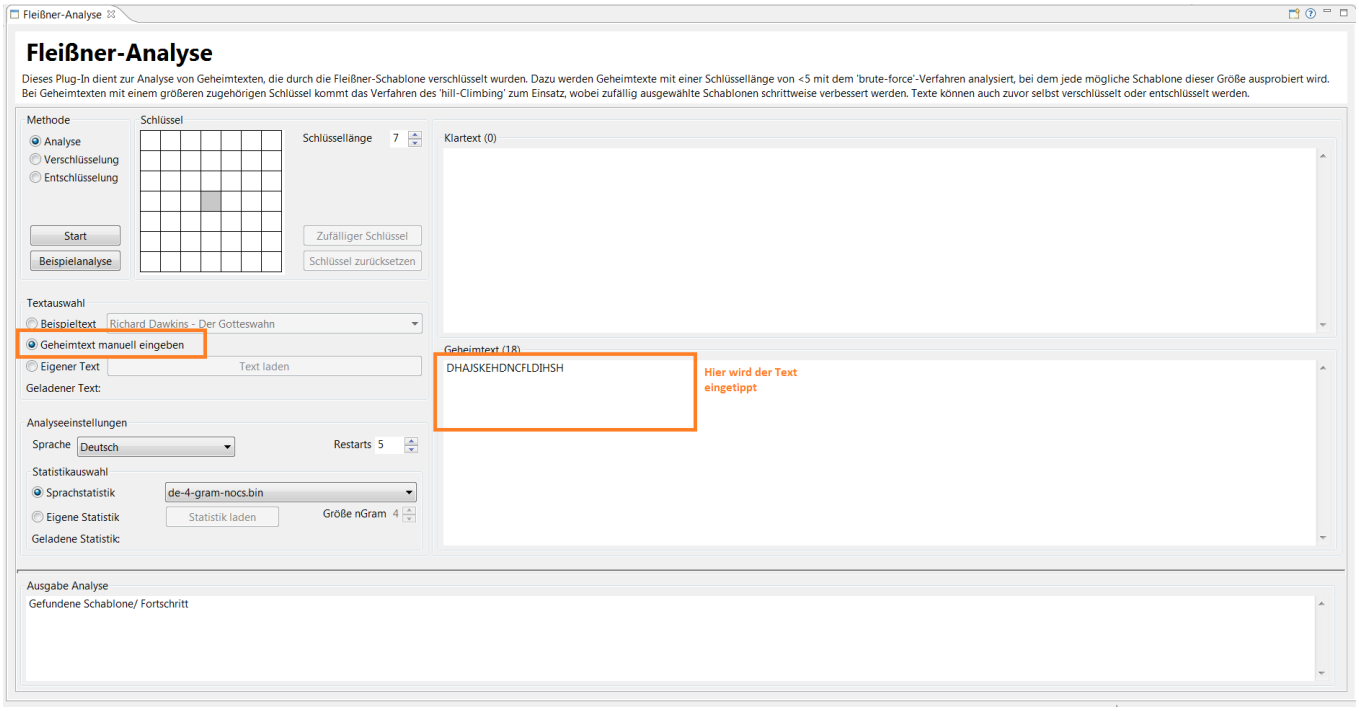
1.2 Textauswahl

In diesem Auswahlmenü kann die Eingabe des Geheimtextes ausgewählt werden. Voreingestellt ist hier die Auswahl „Beispieltext“. Hier kann zwischen zwei deutschsprachigen und zwei englischsprachigen Geheimtexten gewählt werden[1]. Die Texte werden je nach ausgewählter Schlüssellänge entsprechend verschlüsselt.

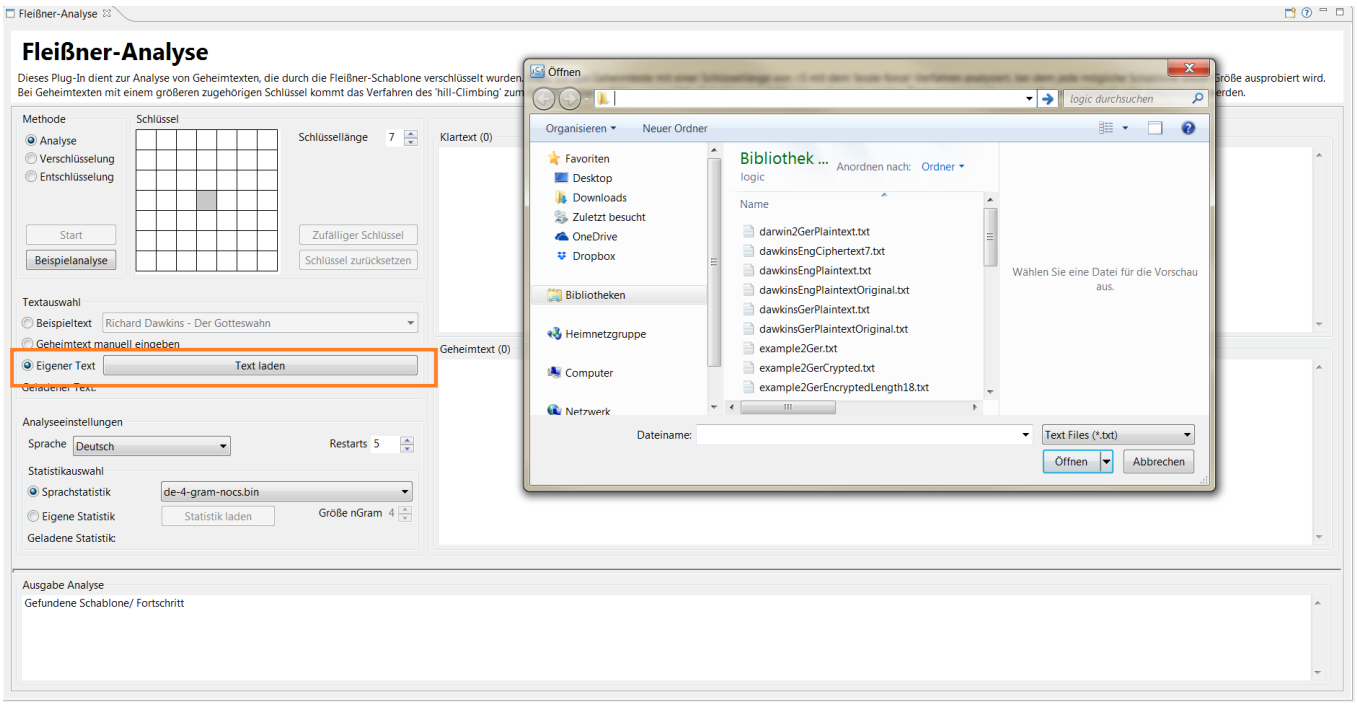


[1]**Quellen:**
Richard Dawkins - Der Gotteswahn
Richard Dawkins - The God Delusion
`https://de.wikipedia.org/wiki/Bildende_Kunst#Fr%C3%BChchristliche_und_byzantinische_Kunst`
`https://en.wikipedia.org/wiki/Visual_arts`

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

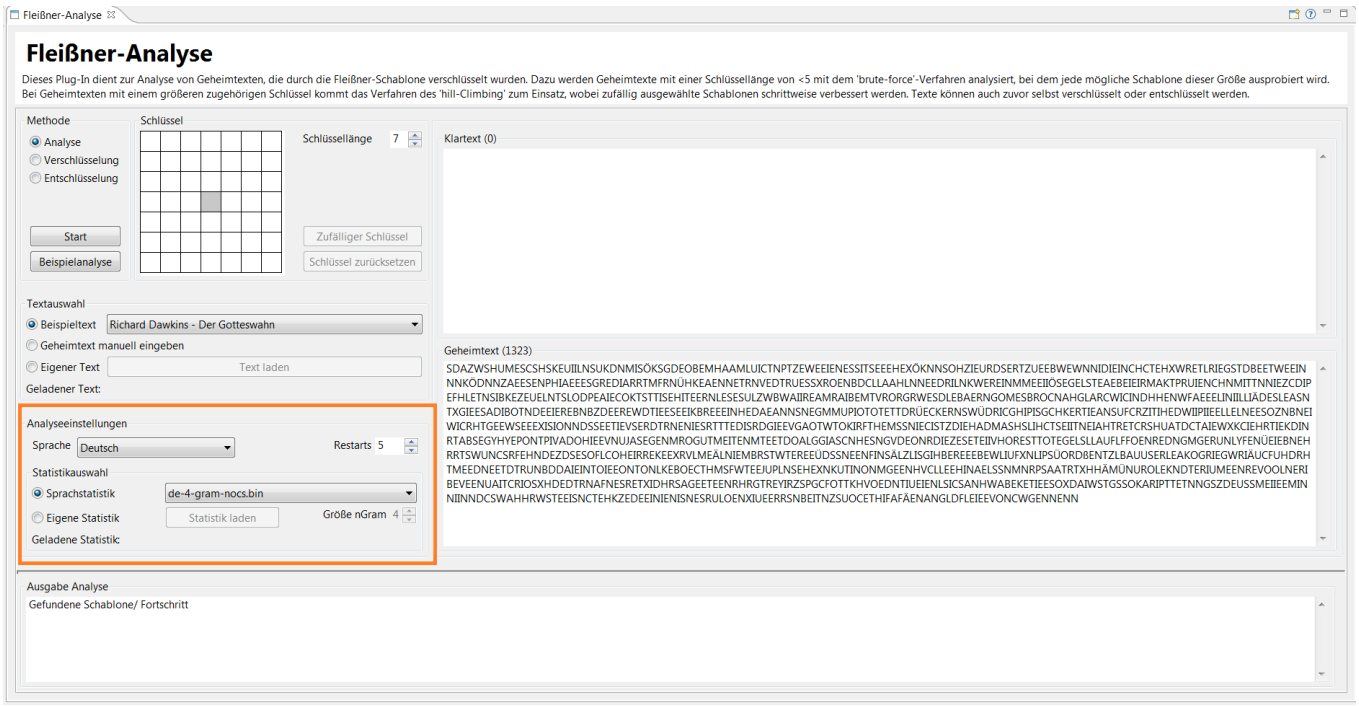


Zum Laden eines eigenen Geheimtextes dient die letzte Auswahl „Eigener Text“. Bei dieser Auswahl wird der Button „Text laden“ aktiviert, über den dann ein Text (*.txt) von einem eigenen Gerät geladen werden kann. Der Text wird dann im Geheimtextfeld angezeigt.



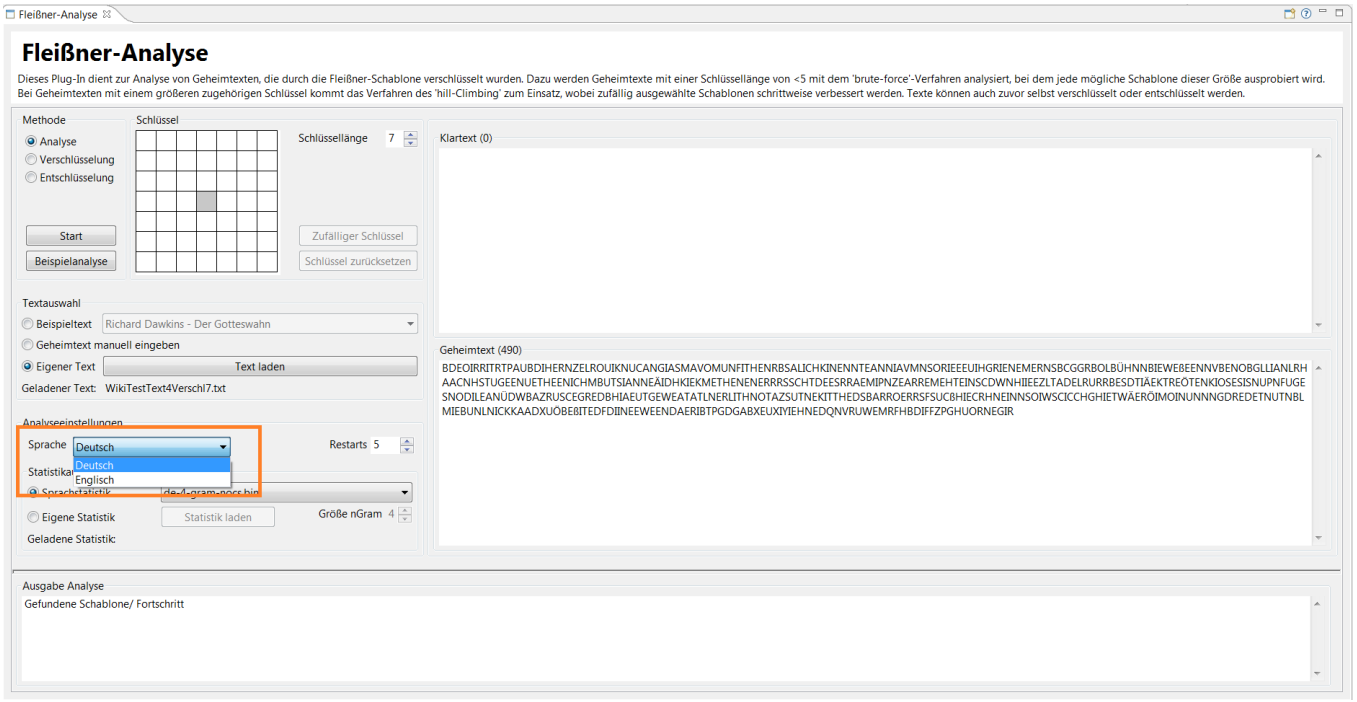
1.3 Analyseeinstellungen

Der Abschnitt „Analyseeinstellungen“ befindet sich direkt unter dem Abschnitt Textauswahl ist nur für die Analysefunktion aktiviert.



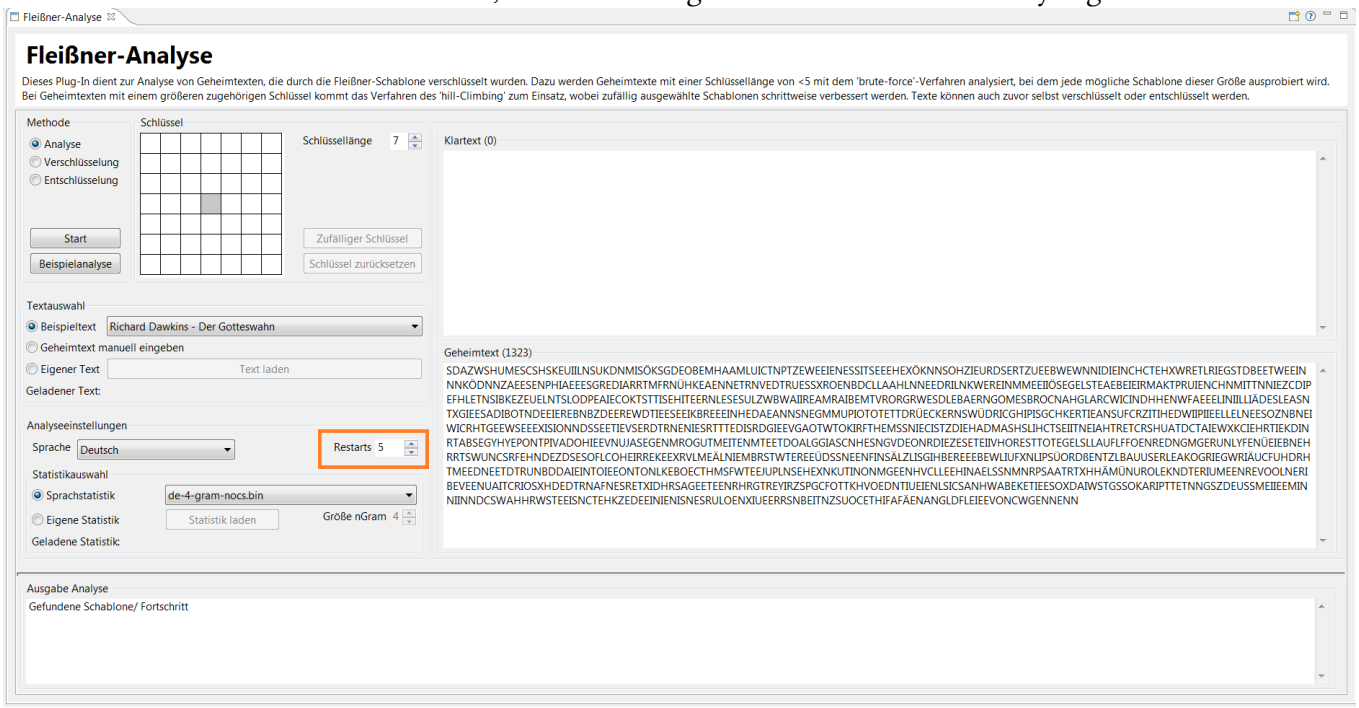
1.3.1 Sprache

Hier kann zwischen den Sprachen „deutsch“ und „englisch“ gewählt werden. Ist im Abschnitt Textauswahl „Beispieltext“ ausgewählt, so wird der angezeigte Text entsprechend der ausgewählten Sprache aktualisiert. Der zu analysierende Text muss der hier ausgewählten Sprache entsprechen. Dies gilt für jede Form der Texteingabe.



1.3.2 Restarts

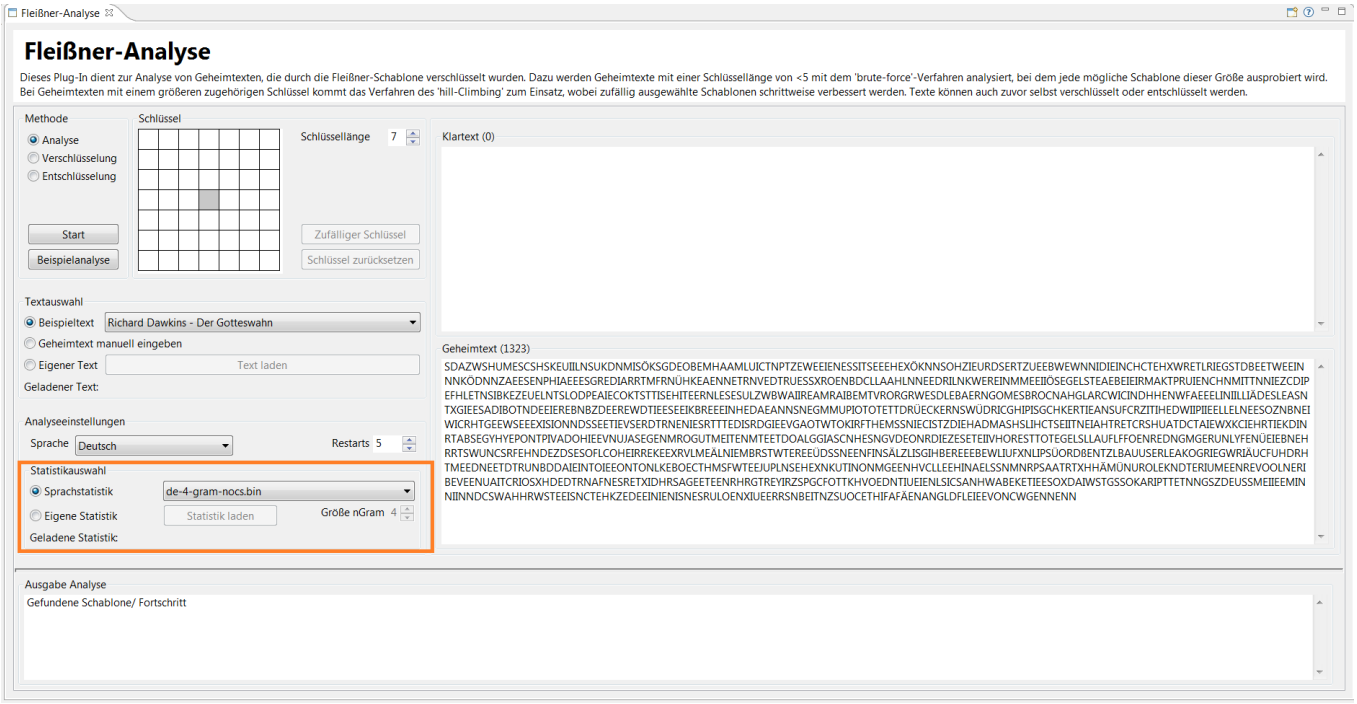
Die Anzahl der Restarts ist relevant für die Analyse von Geheimtexten, die mit Schlüsseln der Größe 5 oder höher verschlüsselt wurden. Bei einer Schlüssellänge dieser Größen wird das „Hill-Climbing"-Verfahren zur Analyse verwendet. Für jeden Restart wird zufällig eine Schablone in der gewählten Schlüssellänge 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].

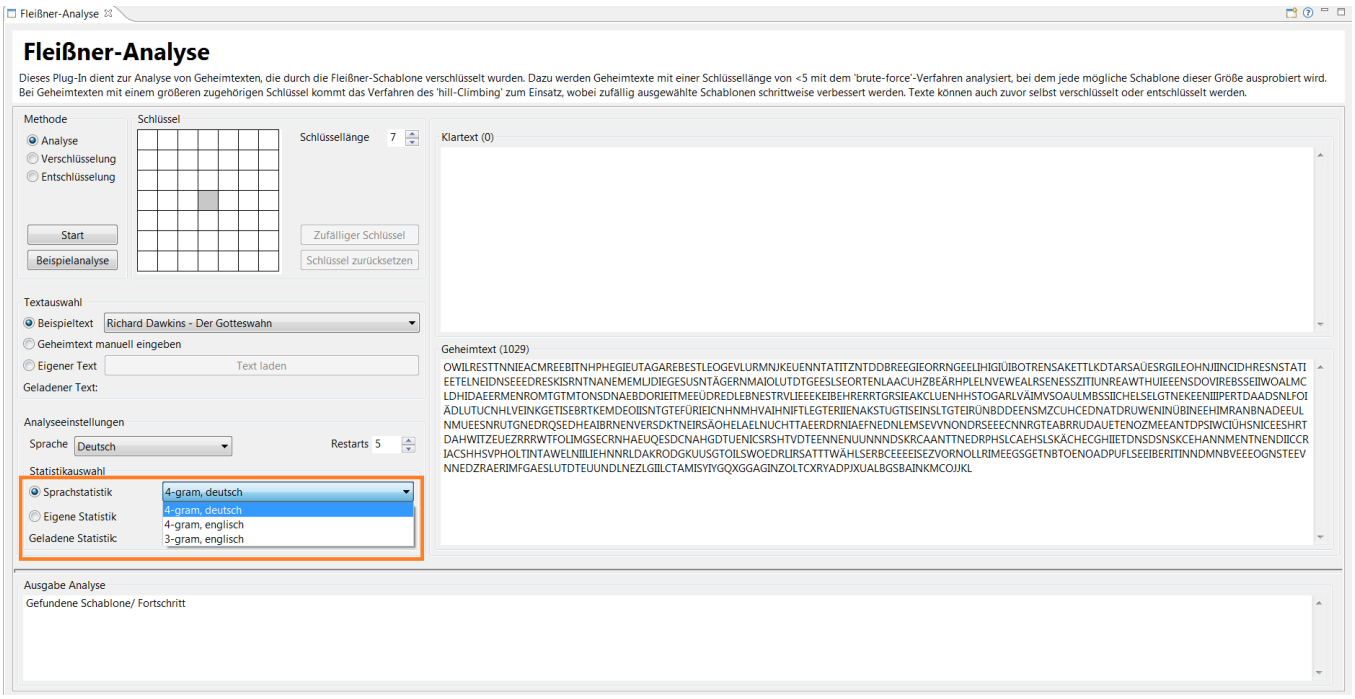
1.3.3 Sprachstatistik

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



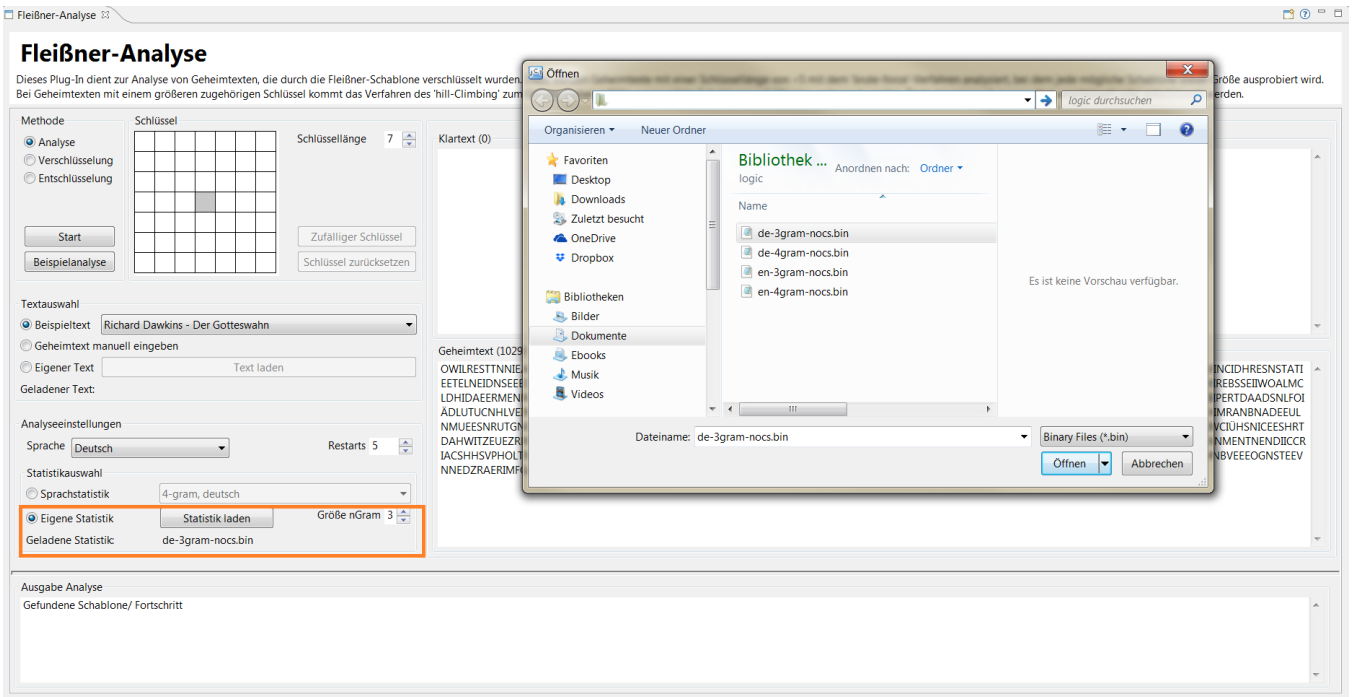
Zur Ausführung der Analyse kann eine der drei hinterlegten Statistiken genutzt werden.

[2] Anhang: Evaluation der Analyse



Es kann aber auch eine eigene Sprachstatistik geladen werden. Hierzu gelten gewisse *Anforderungen* an das Format der Sprachstatistik:

Im Vergleich zu anderen Sprachstatistiken, sollten die tatsächlichen n-Gramme sich für dieses Plug-In 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-Gram gemeinsam den Index für den Wert zum jeweiligen n-Gram angeben.



Beispiel: Zum Speichern und Abrufen des Quadgrams „Ihre“ in einer deutschen Quadgram-Statistik geht man wie folgt vor:

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 Quadgram „Ihre“ wird nun jeder Buchstabenindex des Quadgrams mit einer Potenz der Alphabetlänge in Abhängigkeit der Position im Quadgram multipliziert. Diese vier Werte werden addiert und ergeben zusammen den Index des Quadgramwerts 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

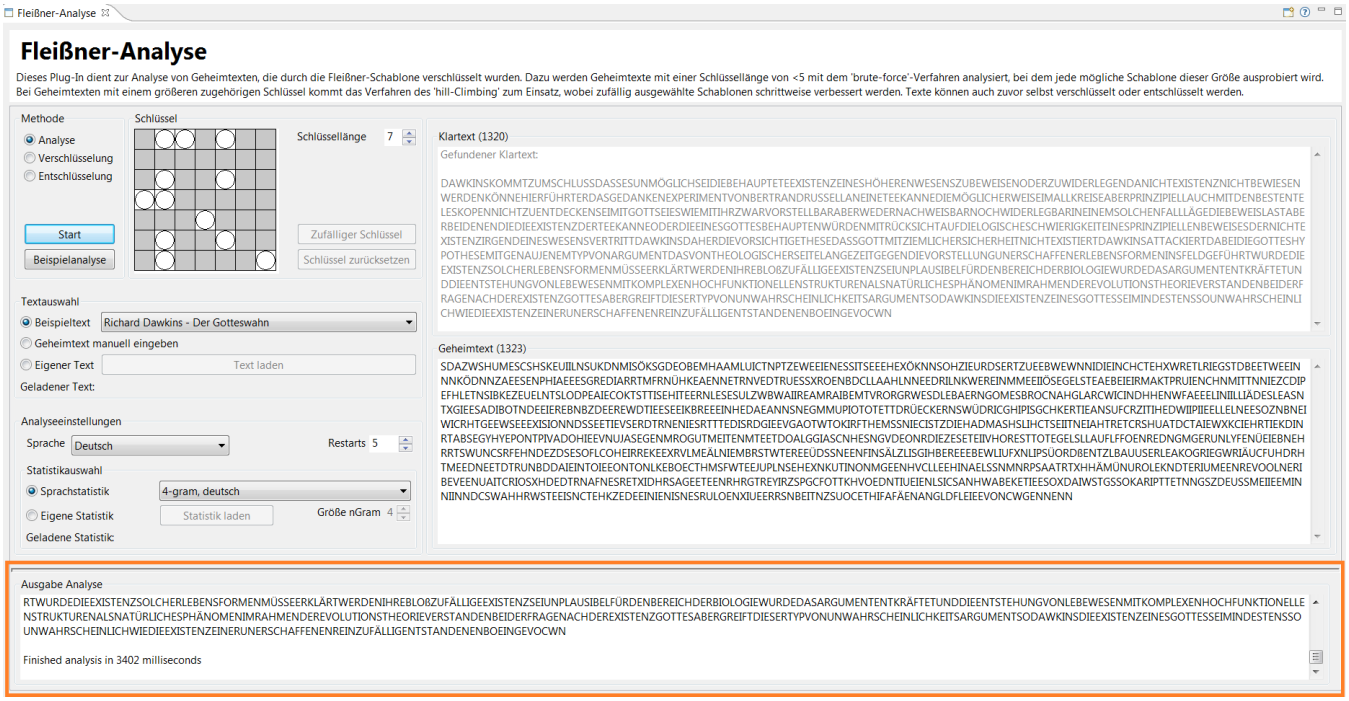
$$8 * 30^3 + 7 * 30^2 + 17 * 30^1 + 4 * 30^0 = 222.814$$

für den Index des Quadgrams „Ihre“ in einer deutschen Quadgram-Statistik.

Wird eine eigene Sprachstatistik geladen, so muss die Größe des n-Grams noch manuell angegeben werden.

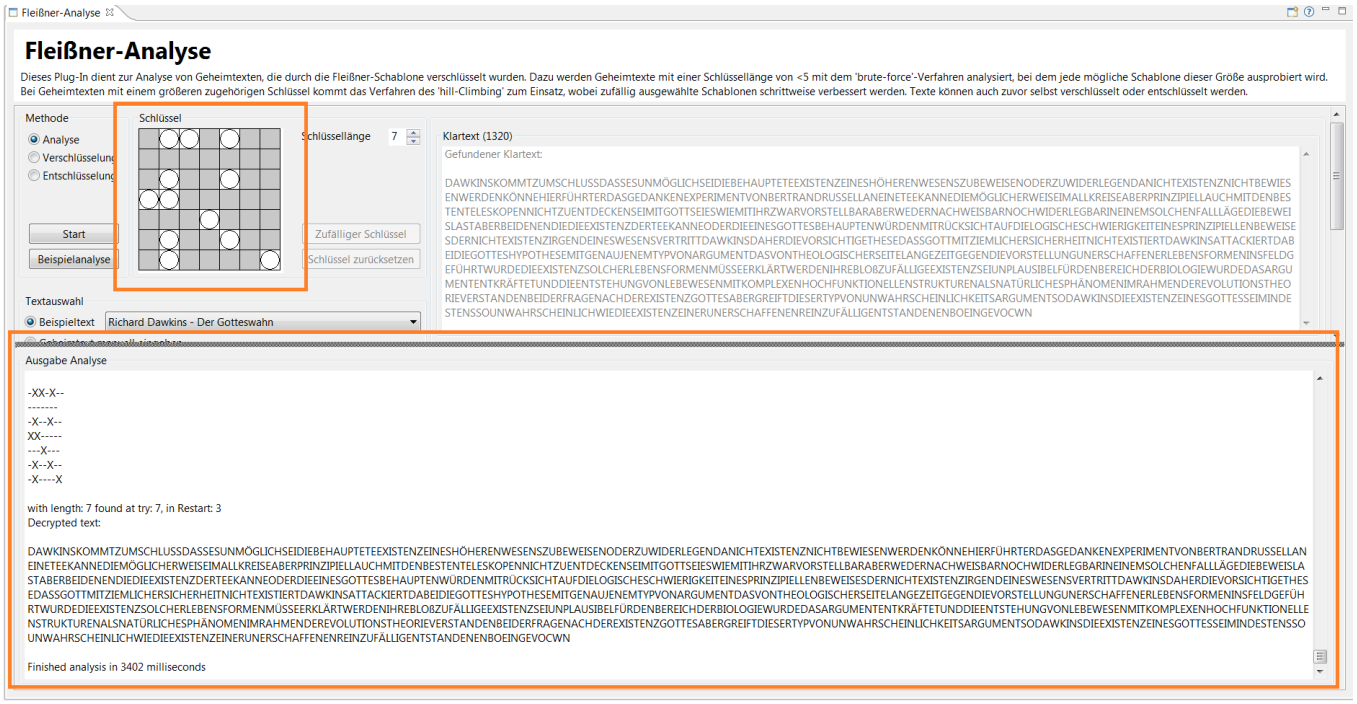
1.4 Ausgabe der Analyse

Am unteren Bildschirmrand befindet sich das Ausgabefenster zur Analyse. Hier werden während der Analyse die aktuellen Fortschritte angezeigt sowie nach Abschluss der Analyse der gefundene Schlüssel und der dazugehörige Klartext.



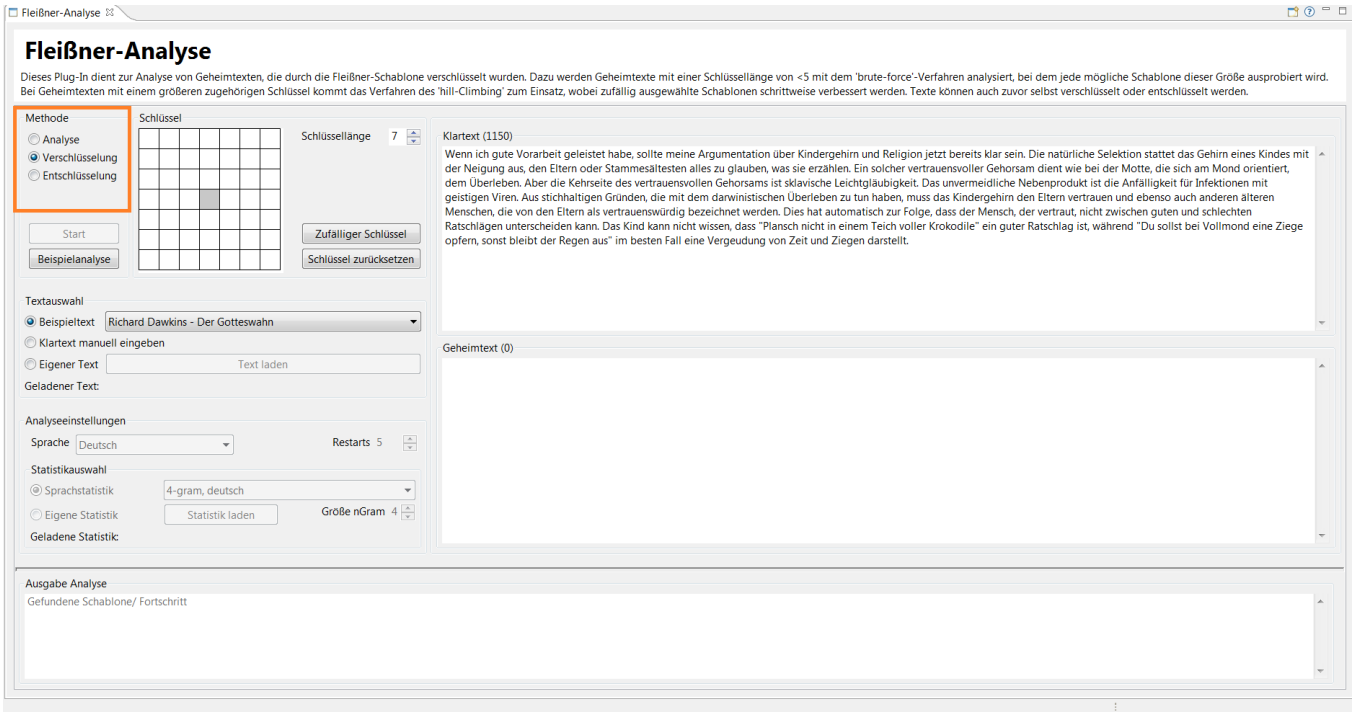
Dieses Fenster kann bei Bedarf auch nach oben vergrößert werden, um mehr Informationen auf einen Blick zu erhalten. Nach Abschluss der Analyse wird der gefundene Schlüssel auch im Schlüsselfeld

selbst angezeigt, so dass dieser beispielsweise direkt zur Entschlüsselung und damit Validierung des Analyseergebnisses verwendet werden kann.

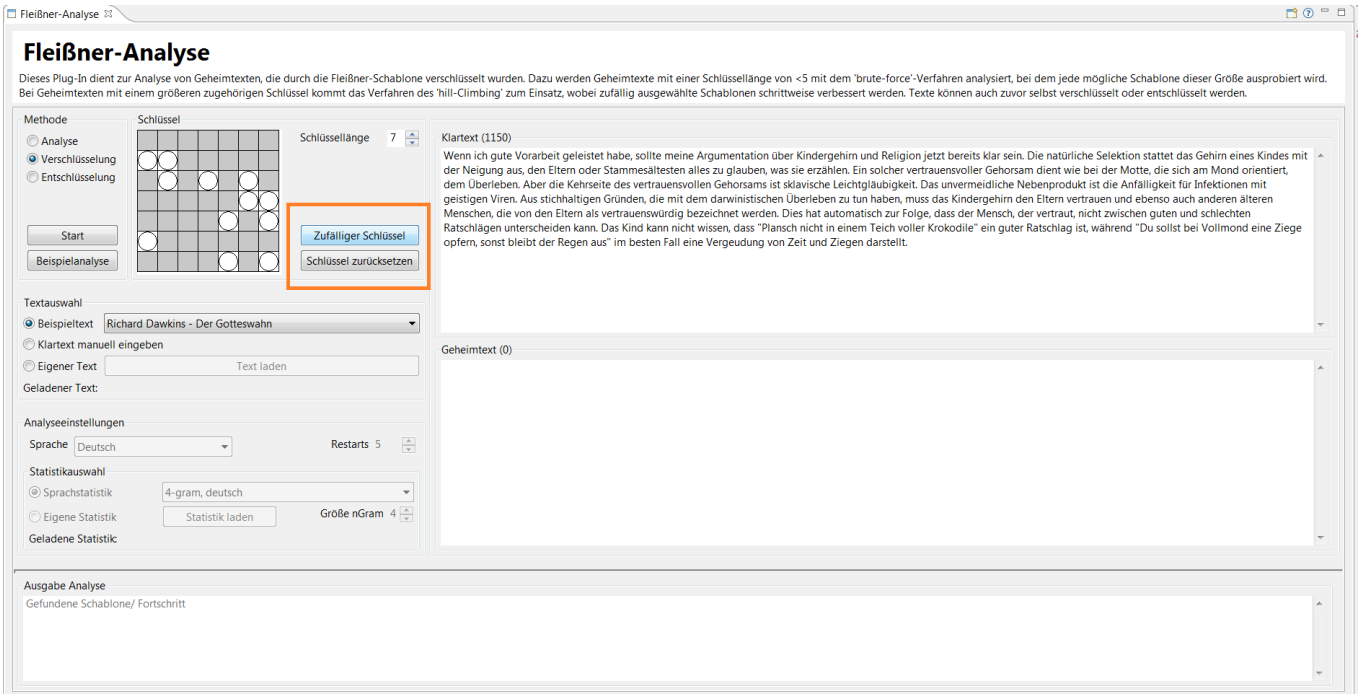


2 Verschlüsselung

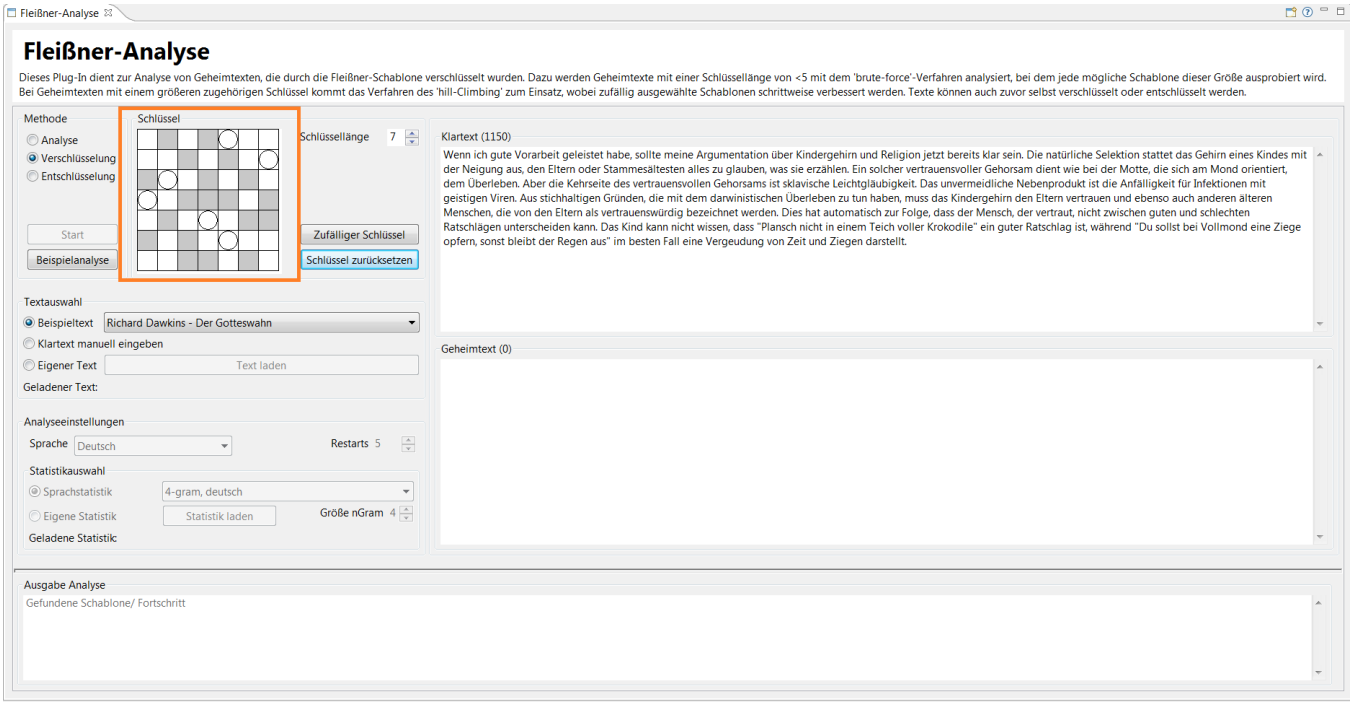
In diesem Plug-In können Klartexte auch selbst verschlüsselt werden. Dazu wird im Abschnitt „Methode“ die Funktion „Verschlüsselung“ ausgewählt.



In dieser Funktion kann nun auch ein Schlüssel gewählt werden. Durch die Betätigung des Buttons „Zufälliger Schlüssel“ wird ein zufälliger Schlüssel erzeugt und angezeigt.



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 die drei zugehörigen Felder blockiert, die durch die Rotation im Verschlüsselungsprozess benötigt werden. Wird ein bereits ausgewähltes Feld noch mal angeklickt, so wird die Auswahl dieses Feldes rückgängig gemacht. Soll die Auswahl aller Felder rückgängig gemacht werden, dient hierzu der „Schlüssel zurücksetzen“-Button.



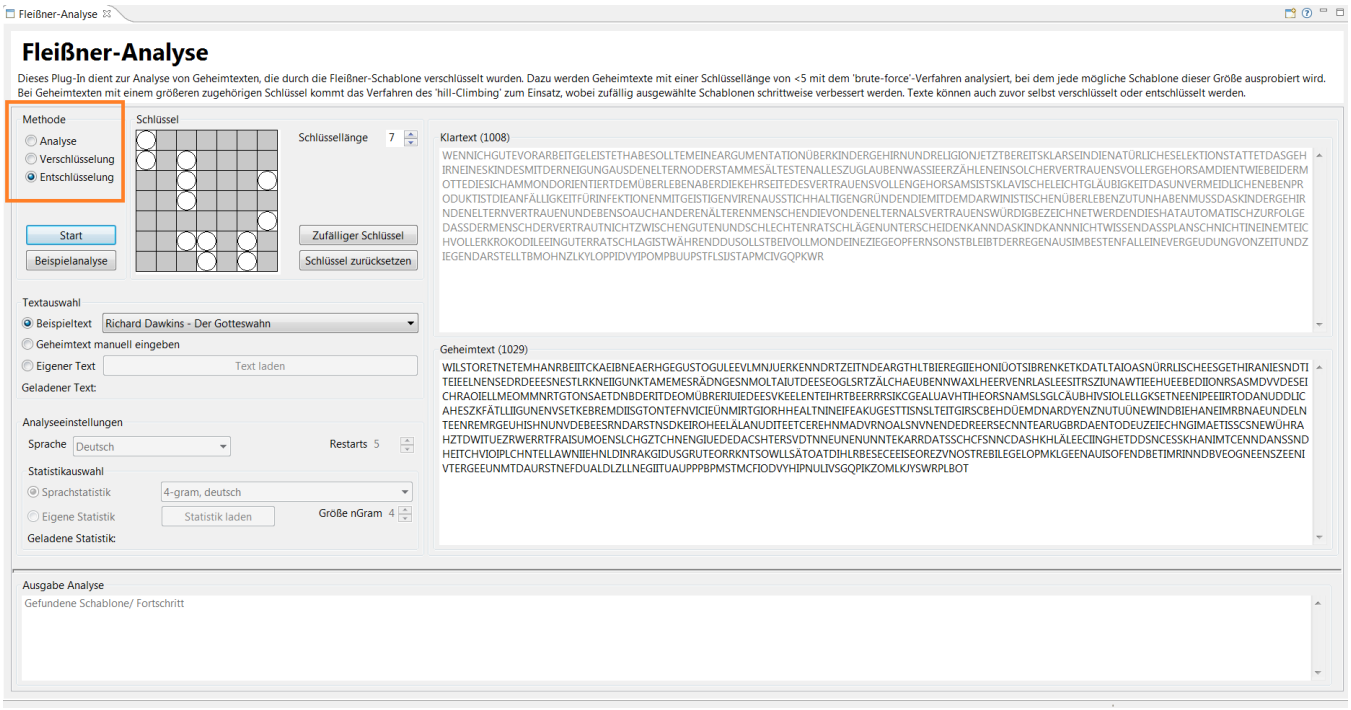
Zur Verschlüsselung ist neben dem Schlüssel auch ein Klartext erforderlich. Dieser kann wie auch in der Analysefunktion aus einer Menge von Beispieltexten gewählt, selbst eingetippt oder geladen werden. Bei der Auswahl von Beispieltexten wird die ausgewählte Funktion des Plug-Ins erkannt und dementsprechend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

Mit der Änderung der Methode zur Analyse oder Verschlüsselung kann mit dem selbst erzeugten Geheimtext nun 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 hier ein nichtleeres Geheimtextfeld benötigt. Die Bedienung der Textauswahl ist hier analog zu den beiden bereits beschriebenen Methoden.