Im Rahmen der Grundausbildung sollen Sie die eben gelernten Methoden selbst anwenden. Sie müssen dafür eine Reihe von Aufgaben absolvieren. In jeder Aufgabe gibt es einen Teil (Codewort), den Sie sich notieren sollten. Sobald Sie alle Aufgaben bearbeitet haben, fügen Sie auf einem Zettel alle Codewörter (CW1-CW5) zu einem einzigen Codewort der Form CW1CW2CW3CW4CW5 zusammen. Dieses zusammengesetzte Codewort nennen Sie einem Ihrer Vorgesetzten. Sie erhalten daraufhin das Passwort für Ihren ersten Auftrag.

Aufgabe 1 – Skytale anwenden

Öffnen Sie CrypTool 2 (Start → Programme → CrypTool 2 → CrypTool 2) und klicken Sie links oben auf „Neu", um ein neues Projekt zu beginnen. Ziehen Sie nun per „drag und drop" aus der Kategorie der „Klassische Verfahren" (links) die Skytale auf den Arbeitsbereich in der Mitte. Mit der Skytale allein können Sie noch nicht arbeiten; Sie benötigen noch eine Ein- bzw. Ausgabe. Klicken Sie dafür auf die Kategorie „Werkzeuge" und ziehen sich von da eine „Texteingabe" und eine „Textausgabe" auf den Arbeitsbereich. Verbinden Sie nun den grauen Ausgang (Ausgabetext, String) der Texteingabe mit dem grauen Eingang der Skytale (Eingabetext, String). Des Weiteren verbinden Sie den grauen Ausgang der Skytale (Ausgabetext, String) mit dem lila Eingang der Textausgabe (Eingabedaten, Object). Geben Sie nun in die Texteingabe folgenden Text ein „**DIE SKYTALE IST DAS AELTESTE BEKANNTE VERSCHLUESSELUNGSWERKZEUG**.", z. B. indem sie auf die Maximieren-Schaltfläche klicken. Alternativ können Sie mit einem Doppelklick auf die Texteingabe die Detailansicht öffnen, und diese mit dem roten X anschließend wieder schließen. Klicken Sie nun auf die Skytale, und stellen Sie rechts in den Parametern einen Stabdurchmesser von 5 ein. Führen Sie das Projekt aus, indem Sie oben den „Starten"-Button klicken. Um das Ergebnis zu betrachten, öffnen Sie nun auch die Textausgabe mittels der Maximieren-Schaltfläche. Alternativ können Sie auch die Detailansicht durch Doppelklick auf die Textausgabe aktivieren.

Ihr erstes Codewort ist nur ein einzelner Buchstabe: Notieren Sie sich den *zweiten* Buchstaben der verschlüsselten Nachricht.

Aufgabe 2 – Skytale knacken

Benutzen Sie CrypTool 2.1, um den folgenden Text zu entschlüsseln:

```
Sieed,_eCsEopksi_wioeTb_a_edetd_EadnssaneeA"lenee_inwu.drth_eg_of___
_rzsegrg_dSi_u__ita_acse_nMb_b_sytibuötfe__t,nrrg.ü__Pa_fe_l_ri_rlia
csiD_s_ieschecadt_n_thehhsi__zb__nrk_e"_
```

Wechseln Sie dazu in den Reiter „Startcenter" und öffnen das Beispielprojekt „Skytale Brute-Force-Analyse" in den Vorlagen unter Kryptoanalyse→Klassisch. Löschen Sie nun zunächst den vorhandenen Text aus der Texteingabe (links oben). Kopieren Sie anschließend den hier gegebenen Text in die Texteingabe. Wechseln Sie zusätzlich bei der Komponente „CryptoolDictionary" das Wörterbuch auf „Deutsch". In der „Enthält"-Komponente setzen sie die „Anzahl der zu findenen Treffer" auf 10. Wenn Sie nun auf „Starten" klicken, sollte der Klartext nach wenigen Sekunden in der unteren Textausgabe mit dem Namen „Plaintext" erscheinen, die den wahrscheinlichsten Klartext enthält. Die obere Textausgabe erhält alle möglichen Klartexte.

Ihr zweites Codewort ist direkt im entschlüsselten Text gegeben und besteht aus drei Buchstaben. Bitte notieren Sie sich diese.

Aufgabe 3 – Caesar anwenden

Für diese Aufgabe verwenden wir CrypTool 1.4. Öffnen Sie dafür CrypTool 1 (Start → Programme → CrypTool → CrypTool) und schließen Sie den „Willkommensbildschirm“ und das Fenster mit „startbeispiel-de.txt“. Klicken Sie nun links oben auf das Symbol „Neu“, um ein neues leeres Fenster zu erzeugen. In diesem Fenster geben Sie nun folgenden Text ein: „**Bei Caesar handelt es sich um eine Verschiebechiffre, die von Julius und Augustus Caesar angewendet wurde.**“. Klicken Sie nun im Menu auf ***Ver-/Entschlüsseln → Symmetrisch (klassisch) → Caesar / ROT13***. Es öffnet sich eine Dialogbox mit den Einstellungen für das Caesarverfahren. Geben Sie nun den Buchstaben W als Alphabetzeichen in der Gruppe zur Schlüsseleingabe ein. Sie sollten sehen, wie sich im unteren Bereich („Information zur Verschlüsselung“) das untere Alphabet (Chiffrealphabet) auf „WXYZABCDEFGHIJKLMNOPQRSTUV“ ändert. Klicken Sie anschließend auf „Verschlüsseln“. Es öffnet sich ein neues Fenster mit dem verschlüsselten Text.

Ihr drittes Codewort besteht wieder aus drei Buchstaben. Betrachten Sie dabei das *vorletzte* Wort der *verschlüsselten* Nachricht und notieren Sie sich daraus die *Buchstaben 3-5*.

Aufgabe 4 – Caesar knacken

Auch diese Aufgabe lösen wir mit CrypTool 1.4. Gegeben ist der folgende verschlüsselte Text:

Qtx Rpthpg dstg paavtbtxc qtx Ktghrwxtqjcvhrwxuugtc vxqi th xchvthpbi cjg hd kxtat Bdtvaxrwztxitc, lxt th Qjrwhipqtc xb Paewpqti vxqi. Sxtht sjgrwojegdqxtgtc xhi htaqhi dwct Rdbejitgwxaut ztxc Egdqatb. Cdrw hrwctaatg vtwi th ltcc bpc sxt wptjuxvhitc Qjrwhipqtc qtigprwiti. Sph Rdstldgi ujtg sxtht Pjuvpqt xhi IGDC.

Klicken Sie zunächst auf „Neu“ um sich ein neues leeres Fenster in CrypTool zu erzeugen. Kopieren Sie obigen Text da hinein. Klicken Sie nun im Menu auf ***Analyse → Symmetrische Verschlüsselung (klassisch) → Ciphertext only → Caesar***. Achten Sie nun auf die verschiedenen Fenster, die auftauchen. Als letztes erscheint ein Fenster mit dem entschlüsselten Klartext.

Das vierte Codewort ist direkt im entschlüsselten Text gegeben. Bitte notieren Sie sich dieses.

Aufgabe 5 – Substitution anwenden

Führen Sie mit Hilfe von CrypTool 1.4 eine monoalphabetische Substitution an folgendem Text durch:

Die Buchstaben oder Zeichen oder auch Buchstabengruppen oder Zeichengruppen des Klartextes werden nach Vorgabe dieses einen Alphabets, das auch Schlüsselalphabet oder Geheimalphabet genannt wird, durch andere Buchstaben, Zeichen oder Gruppen ersetzt. Zur Entzifferung monoalphabetischer Verschlüsslungen ohne bekannten Schlüssel führt man eine Häufigkeitsanalyse der Buchstaben durch und kann so auf gewisse Buchstaben schließen, woraus dann Wörter und somit immer mehr Assoziationen zu Klartextbuchstaben gezogen werden können.

Schließen Sie zunächst alle noch offenen Fenster in CrypTool, damit Sie den Überblick behalten. Klicken Sie nun wieder auf „Neu“, um ein neues leeres Fenster zu erzeugen. Kopieren Sie sich den gegebenen Text in dieses Fenster. Klicken Sie nun auf Ver-/Entschlüsseln → Symmetrisch (klassisch) → Substitution / Atbash. Geben Sie in der nun erscheinenden Dialogbox den Schlüssel „ADCOYOTEQM“ ein und klicken Sie auf Verschlüsseln.

Das fünfte Codewort besteht wieder aus 3 Buchstaben. Notieren Sie sich die ersten drei Buchstaben des verschlüsselten Textes.

Aufgabe 6 – Substitution knacken (Zusatzaufgabe)

Versuchen Sie, den in Aufgabe 5 erzeugten Text mit Hilfe der automatischen Häufigkeitsanalyse in CrypTool 1.4 zu entschlüsseln. Selektieren Sie dazu das Fenster mit dem verschlüsselten Text und klicken Sie im Menu von CrypTool auf ***Analyse → Symmetrische Verschlüsselung (klassisch) → Ciphertext only → Substitution***. Probieren Sie die beiden angebotenen Verfahren mit verschiedenen Optionen und vergleichen Sie die Ergebnisse.

Abschluss der Grundausbildung

Schreiben Sie die fünf gefundenen Codewörter auf einen Zettel in der Form CW1CW2CW3CW4CW5 und kontaktieren Sie damit Ihren Vorgesetzten. Sie erhalten dann das Passwort für Ihren ersten Auftrag.