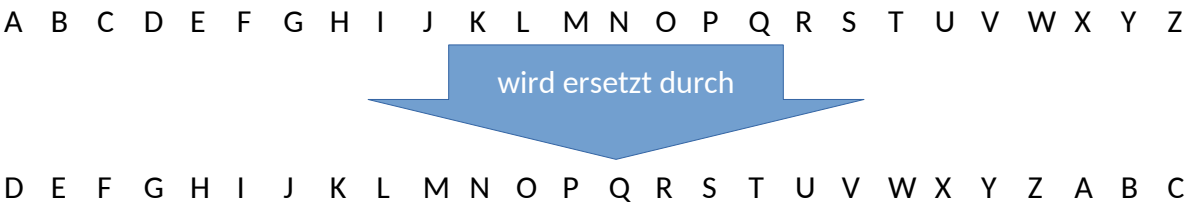
Arbeitsblatt: Ein historisches Verschlüsselungsverfahren

Kurzbeschreibung

Sie probieren ein historisches Verschlüsselungsverfahren aus – von Hand und in einem Jupyter Notebook.

Einführung – Aufgabe 1

Der römische Staatsmann und Feldherr Julius Caesar (* 100 v. Chr. in Rom; † 44 v. Chr. in Rom) benutzte ein einfaches Verfahren zum Verschlüsseln von Nachrichten. Er ließ jeden Buchstaben durch einen im Alphabet um 3 Einheiten verschobenen Buchstaben ersetzen.



Falls Sie in Gruppen arbeiten: Verschlüsseln Sie je ein Wort Ihrer Wahl und lassen Sie andere in Ihrer Gruppe das Wort wieder entschlüsseln.

Falls Sie alleine arbeiten: verschlüsseln Sie das Wort „GEHEIMNIS“ und entschlüsseln Sie das Wort „KDFNHUDQJULII“.

Schreiben Sie die Ergebnisse hier auf.

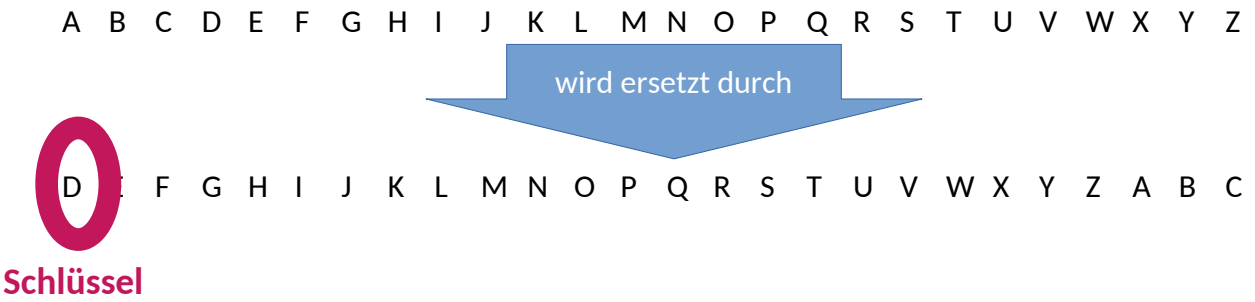
Arbeitsblatt „Ein historisches Verschlüsselungsverfahren“ von Antje Schweitzer, Uni Stuttgart / Projekt KI B³ – KI in die berufliche Bildung bringen, Version 16.09.24. Das Projekt KI B³ wird gefördert als InnoVET-Projekt aus Mitteln des Bundesministeriums für Bildung und Forschung.

Das Arbeitsblatt basiert auf den Stationen „Chiffrierung mit dem Verschiebeverfahren“ sowie „Kryptoanalyse beim Verschiebeverfahren“ von Stefan Schweickert, Klaus Becker und Michael Becker, inf-schule.de, beide lizenziert unter CC BY SA 4.0.

URLs der Originale:
https://inf-schule.de/kryptologie/historischechiffriersysteme/station_verschiebeverfahren
https://inf-schule.de/kryptologie/historischechiffriersysteme/station_kryptoanalyseverschiebeverfahren

Der Schlüssel – Aufgabe 2

Das von Caesar benutzte Chiffrierverfahren wird etwas flexibler, wenn man die Verschiebezahl frei wählen kann. Der Empfänger der Nachricht sollte die Verschiebezahl kennen, damit er die Nachricht problemlos entschlüsseln kann. Caesar verwendete die Verschiebezahl 3. Dabei wird der Klartextbuchstabe A zu dem Geheimtextbuchstaben D. Anstelle der Verschiebezahl können sich Sender und Empfänger auch auf den Buchstaben einigen, der im Geheimtext anstelle des Buchstaben A erscheint. Diesen Buchstaben nennt man Schlüssel.



Verwenden Sie das Jupyter Notebook „Monoalphabetische Verschlüsselung nach Caesars Verschiebeverfahren“, um einen Text Ihrer Wahl zu verschlüsseln. Verwenden Sie einen anderen Schlüssel als Cäsar. Sie können den Geheimtext zusammen mit dem Schlüssel an jemand anderen zum Entschlüsseln weitergeben.

Verwenden Sie das Notebook außerdem, um Ihre Ergebnisse aus Aufgabe 1 zu kontrollieren.

Notebook herunterladen und selbst ausführen:

https://antje-schweitzer.github.io/Jupyter_Notebooks_KI_und_Maschinelles_Lernen/B5-1.Verschluesselung.Caesar.ipynb

oder Notebook bei Google Colab ausführen:

https://colab.research.google.com/drive/1sVg2phe_5kTJxgrioC1UxVbMVWd2gU1B?usp=share_link

Vom Schlüssel zur Verschiebezahl – Aufgabe 3

Erklären Sie, wie man (ohne ein Programm zu verwenden!) …

… aus der Verschiebezahl den Schlüsselbuchstaben ermitteln kann.

… aus dem Schlüssel die Verschiebezahl ermitteln kann.

Caesars Verschlüsselung mit 'Brute Force' knacken – Aufgabe 4

Mit 'Brute Force', zu Deutsch 'roher Gewalt', ist meist ein Verfahren gemeint, bei dem man nicht unbedingt intelligent, dafür aber mit viel Ausprobieren vorgeht. Hier ist damit gemeint, einen verschlüsselten Text durch Ausprobieren aller in Frage kommenden Schlüssel zu entschlüsseln.

Nutzen Sie die Funktionen im Notebook und programmieren Sie eine Schleife über alle möglichen Verschiebezahlen, um den folgenden Text zu entschlüsseln. Sie finden den Text auch im Notebook.

OXKLVAENXLLXENGZ WBXGM SNK ZXAXBFATEMNGZ OHG BGYHKFTMBHG, UXBLIBXELPXBLX NF FBEBMTXKBLVAX GTVAKBVAMXG ZXAXBF NXUXKFBMMXEG SN DHXGGXG HWXK LVAKBYMEBVAX FBMMXBENGZXG HWXK TUZXLIXBVAXKMX WTMXG ZXZXG NGUXYNZMXL „FBMEXLXG“ SN LVANXMSXG. WBX PBLLXGLVATYM WXL „ZXAXBFXG LVAKXBUXGL“ PBKW TEL DKRIMHZKTIABX UXSXBVAGXM, TUZXEXBMXM OHG TEMZKBXVABLVA „DKRIMHL“, WXNMLVA „OXKUHKZXG“, „ZXAXBF“ NGW „ZKTIAXBG“, WXNMLVA „LVAKXBUXG“. BAKX NKLIKNXGZX EBXZXG BG WXK TGMBDX, FHXZEBVAXKPXBLX GHVA PXBMXK SNKNXVD, WXGG WBX ZXAXBFATEMNGZ PTK FXGLVAXG LXBM CXAXK XBG PBVAMBZXL TGEBXZXG.

Lassen Sie sich jeweils das Ergebnis unter Angabe des ausprobierten Schlüssels ausgeben und suchen Sie sich das korrekte Ergebnis heraus. Wie lautete der Schlüssel? Wie die ersten drei Wörter?

Caesars Verschlüsselung intelligent knacken – Aufgabe 5

Eine intelligentere Methode ist es, die Buchstabenhäufigkeiten im verschlüsselten Text zu untersuchen. Nutzen Sie die Funktion `buchstaben_frequenzen` im Notebook, um den verschlüsselten Text zu analysieren. Welcher Buchstabe ist im verschlüsselten Text am häufigsten?

Welcher Buchstabe ist Ihrer Vermutung nach im Originaltext am häufigsten? Überprüfen Sie es, indem Sie die Funktion `buchstaben_frequenzen` auf den oben entschlüsselten Text anwenden. Wie können Sie damit den Schlüssel bestimmen?

Bewerten Sie die Sicherheit des Verschiebeverfahrens. Wie schwierig/leicht ist es, einen abgefangenen Geheimtext ohne Kenntnis des Schlüssels zu entschlüsseln?