Arbeitsblatt: Verschlüsselung mit einer Ersetzungstabelle

Kurzbeschreibung

Sie probieren mithilfe des Jupyter Notebooks „Monoalphabetische Verschlüsselung mit Ersetzungstabelle“ die Verschlüsselung mithilfe einer Ersetzungstabelle aus und experimentieren damit, solche Verfahren zu knacken.

Notebook herunterladen und selbst ausführen:

https://antje-schweitzer.github.io/Jupyter_Notebooks_KI_und_Maschinelles_Lernen/B5-2.Verschluesselung.Ersetzungstabelle.ipynb

oder Notebook bei Google Colab ausführen:

https://colab.research.google.com/drive/1qszgDRAo_Iankqh53OXYhjaei8o-vaBW?usp=sharing

Einführung – Aufgabe 1

Beim Verschiebeverfahren reichte es, für einen Buchstaben seine verschlüsselte Entsprechung zu kennen. Damit konnte man für alle weiteren Buchstaben ebenfalls ihre verschlüsselten Varianten bestimmen, denn die Abbildung vom Buchstaben auf die verschlüsselte Variante folgte immer derselben Regel.

Etwas schwieriger sind Texte zu knacken, wenn die Zuordnung zufällig ist.

Im ersten Abschnitt des Notebooks finden Sie eine Funktion, die zu einem gegebenen String eine Ersetzungstabelle liefert, die für jeden Klartextbuchstaben des Alphabets eine verschlüsselte Entsprechung speichert. Diese Tabelle ist als Python-Dictionary implementiert. Im Gegensatz zum letzten Notebook mit dem Caesar-Verfahren sind dieses Mal auch Umlaute erlaubt.

Arbeitsblatt „Verschlüsselung mit einer Ersetzungstabelle“ 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 Ersetzungsverfahren“ sowie „Kryptoanalyse beim Ersetzungsverfahren“ 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_ersetzungsverfahren
https://inf-schule.de/kryptologie/historischechiffriersysteme/station_kryptoanalyseersetzungsverfahren

Bei Angabe des Strings „WARUMSOLICHVEKNPTDGBFJQXYZß“ erhalten Sie zum Beispiel ein Dictionary, das die unten stehende Verschlüsselungstabelle enthält.

Probieren Sie die Funktion mit verschiedenen Strings als Argument aus. Probieren Sie auch sehr kurze Wörter sowie längere Sätze aus.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	ß
												wird ersetzt durch														
W	A	R	U	M	S	O	L	I	C	H	V	E	K	N	P	T	D	G	B	F	J	Q	X	Y	Z	ß

Was passiert, wenn Sie einen String angeben, der weniger Buchstaben enthält als das Alphabet? Was passiert, wenn Wörter oder Sätze eingeben?

Aufgabe 2 – Verschlüsselung ausprobieren

Suchen Sie sich einen beliebigen Text und verschlüsseln Sie ihn mit einem selbst ausgedachten Schlüssel. Tauschen Sie Text und Schlüssel mit einer anderen Person aus und entschlüsseln Sie gegenseitig Ihre Nachrichten. Falls Sie nicht mit einer anderen Person zusammenarbeiten, verschlüsseln Sie den Text „Es war einmal eine Auszubildende, die musste in ihrer Ausbildung das Eiscremespiel spielen“ mit dem Schlüssel „Was man nicht alles für eine gute Ausbildung tun muss“ und notieren Sie sich das Ergebnis:

Aufgabe 3 - Verschlüsselung knacken

Versuchen Sie, folgenden Text zu entziffern. Er wurde mit einer Ersetzungstabelle monoalphabetisch verschlüsselt.

ANIS NIJXHNSNJFINE LBKNHJKLNKYNB JIN WPCBBN ANI NIBNH NIJANJKNEELBO. JIN MHANIKNK MB NIBNH KMBZJKNEEN LBU SLJJ TN BMXR QNKKNH SNRH ANYINRLBOJQNIJN QNBIONH NIJ ANJKNEENB. ANI AEMLNS RISSNE LBU ANI RCRNB KNSFNHMKLHNB QIHU ANJCBUNHJ PINE NIJ PNHZMLDK. ANI ZMEKNB KNSFNHMKLHNB LBU JXRENXRKNS QNKKNH SLJJ SMB UMONONB PINE QNBIONH NIJ ANJKNEENB. MLßNHUNS JIBU UIN MAJMKYYMRENB MB QCXRNBNBUKMONB ISSNH RCNRNH MEJ LBKNH UNH QCXRN. PMBIEEN PNHZMLDK JIN UMBB LNAHIONBJ ANJCBUNHJ RMNLDIO, MANH NHUANNHN ZMLDNB JIXR UMBB MLXR OMBY PINEN.

Analysieren Sie dazu zunächst die Häufigkeiten der Buchstaben im Geheimtext. Die Funktion hierfür finden Sie im Notebook.

Machen Sie dann einen ersten Rateversuch. Das Notebook bietet hierfür eine Funktion, die die Buchstaben im Geheimtext aufgrund ihrer Häufigkeiten zuordnet: der im Text am häufigsten enthaltene Buchstabe wird dem im Deutschen häufigsten Buchstaben E zugeordnet, der zweithäufigste dem N, und so weiter. Dies klappt natürlich nicht immer, aber oft reicht dies schon, um Teile des Texts entschlüsseln zu können.

Notieren Sie die Ausgabe mit dem Geheimtext und dem teilweise entschlüsselten Text hier:

Erraten Sie anschließend die restlichen Buchstaben – entweder durch wiederholte Angabe der korrekten Ersetzungen, oder durch wiederholtes Austauschen von Buchstaben jeweils so, dass Sie nach und nach immer mehr Wörter entziffern können.

Notieren Sie sich anschließend den Schlüssel und den komplett entschlüsselten Klartext hier.

Aufgabe 4 – Diskussion

Diskutieren Sie in der Gruppe: Wie sicher sind Sie, dass Ihr Schlüssel genau dem Schlüssel entspricht, der zum Verschlüsseln dieses Texts verwendet wurde?