Leistungsnachweis CAS Informatik und Informatikdidaktik

Frühlingssemester 2020 / 21

Fachdidaktik Datenwissenschaften

Aufgaben zum Thema Geheimschriften und Verschlüsselung

Verfasst von:

Daniel Spadin

Betreut durch:

Prof. Dr. Juraj Hromkovic

Geheimschriften

Vorwissen und Zielsetzung

Die drei Aufgaben zeigen verschiedene Arten, eine Nachricht zu verschlüsseln. Mit CAESAR und Vigenère sind die SuS bereits vertraut. Aufgabe 1 + 2 sollen diese Verschlüsselungsarten nochmals vertiefen. Aufgabe 3 zeigt eine dritte Verschlüsselungsmethode, die die Buchstabenhäufigkeiten der deutschen Sprache berücksichtigt.

In Aufgabe 1 wird die Methode CAESAR vertieft. Da die SuS bereits mit CAESAR vertraut sind, ist die Verschiebung nicht immer gleich, sondern ändert sich von Buchstabe zu Buchstabe. Somit haben die SuS eine zusätzliche Herausforderung zu meistern.

Aufgabe 2 ist eine Weiterentwicklung der Vigenère-Verschlüsselung. Bei der Viginère-Verschlüsselung verwendet man im Vergleich zur CAESAR Methode nicht mehr immer das gleiche Alphabet (monoalphabetische Substitution), sondern arbeitet mit einem Schlüsselwort, welches vorgibt, welches Alphabet benutzt wird. Das Besondere an dieser Aufgabe ist, dass sich der Schlüssel laufend ändert. Die Änderung scheint zunächst rein zufällig, es wird sich aber zeigen, dass sich dahinter eine einfache Rechenmethode versteckt.

Bei Aufgabe 3 kann man anhand eines Beispiels schon einige verschlüsselte Buchstaben bestimmen. Anhand des Beispiels und dem Wissen, dass der Buchstabe E in der deutschen Sprache am häufigsten vorkommt, kann die anfangs schwierig erscheinende Aufgabe mittels eines Lückentextes erstaunlich schnell gelöst werden.

Aufgabe 1

Voraussetzungen

Die SuS der 1. Oberstufe haben bereits einfache Dechiffrierungen mit Buchstaben vertauschen gemacht. Die Kryptosysteme CAESAR und SKYTALE sind den SuS bereits bekannt.

Es folgt eine etwas schwierigere Dechiffrierung.

Aufgabe

Das Wort HALLO wird in meinem sehr ausgeklügelten Geheimcode wie folgt geschrieben.

HALLO

LDPOS

Versuche nun den folgenden Satz zu dechiffrieren.

HHVIVRWFLLWWKUYHR

Lösung

Da der Buchstabe L aus dem Wort HALLO einmal mit P und einmal mit O dechiffriert wird, kann es sich nicht um eine monoalphabetische Verschlüsselung handeln. Anhand dieses Wissens und der Kenntnis über Caesar müssen die SuS nur noch herausfinden, um wie viele Positionen die Buchstaben verschoben werden. Die Buchstaben werden immer abwechselnd um 4 und dann um 3 Positionen nach hinten im ABC verschoben.

4	**3**	**4**	**3**	**4**	**3**	**4**	**3**	**4**	**3**	**4**	**3**	**4**	**3**	**4**	**3**	**4**
D	E	R	F	R	O	S	C	H	I	S	T	G	R	U	E	N
H	H	V	I	V	R	W	F	L	L	W	W	K	U	Y	H	R

Aufgabe 2

Voraussetzungen

Die SuS haben bereits die Vigenère-Verschlüsselung kennengelernt. Die Vigenère-Verschlüsselung soll nun sicherer gemacht werden, indem sich das Schlüsselwort laufend ändert.

Beispiel

Ein einfaches Beispiel für ein fortlaufendes Schlüsselwort wäre das ABC. Ich durchlaufe das ganze ABC und wenn man durch ist, beginnt man von vorne.

Schlüssel	A	B	C	D	E	F	G	H	I
Verschlüsselung	S	D	J	X	P	Y	G	N	M
Originaltext	S	C	H	U	L	T	A	G	E

Aufgabe A

„Guten Morgen“ wird wie folgt codiert:

GUTENMORGEN

GVVHNOOUHGO

Der Schlüssel ist hier etwas komplizierter und generiert sich über Buchstabenmultiplikationen. Zu beachten ist, dass sich das Schlüsselwort so zufällig wie möglich ändert, dahinter aber ein klares Prinzip steht. Wenn der Algorithmus bekannt ist, kann die Nachricht schnell entschlüsselt werden. Die folgenden Schritte erklären, wie das Schlüsselwort generiert wird.

Schritt	Schlüssel	Erklärung
1	(a + b) (c + d)	→ Binom ausmultiplizieren
2	ac + ad + bc + bd	→ Ausmultiplizierte Binome werden getrennt (gelb / blau) → Aus Teil 1 (gelb) wieder ein Binom machen (a + c) (a + d) → Aus Teil 2 (blau) wieder ein Binom machen (b + c) (b + d)
3	aa + ad + ca + cd	→ Binom aus Teil 1 (gelb) ausmultiplizieren
4	bb + bd + cb + cd	→ Binom aus Teil 2 (blau) ausmultiplizieren
5	(e + f) (g + h)	→ Wieder zu Schritt 1 mit anderen Buchstaben

Nun kannst du den Code aus den Schritten 1 bis 5 ablesen. Es werden nur die Buchstaben abgelesen. Operationszeichen werden nicht berücksichtig beim Ablesen des Codes. Es entsteht folgendes Schlüsselwort für die Dechiffrierung mit Vigenère:

ABCDACADBCBDAAADCACDBBBDCBCDEFGH…….

Versuche nun den folgenden Satz zu entschlüsseln.

GVVHNOOUHGOLCHHHKSUHEBOLGM

Aufgabe B

Versuche mit obigem Schlüssel eine eigene Nachricht zu verschlüsseln.

Lösung

Aufgabe A

GVVHN OOUHGO LCH HHKSUH EBOLGM

GUTEN MORGEN ICH HEISSE DANIEL

Aufgabe B (mögliche Lösung)

DANIEL

DBPLEN

Aufgabe 3

Voraussetzung

Die SuS haben sich bereits die Häufigkeit von Buchstaben in deutschsprachigen Texten angeschaut. Sie wissen, dass mit der Analyse von Buchstabenhäufigkeiten Texte dechiffriert werden können. Zudem ist den SuS bekannt, dass der Buchstabe E mit Abstand am häufigsten vorkommt in der deutschen Sprache.

Aufgabe

Das Wort HOFFNUNG wird wie folgt dechiffriert.

HOFFNUNG

TPFFIKID

Versuche nun den folgenden Satz zu dechiffrieren. Die Länge der einzelnen Wörter ist schon bekannt.

AISOUTJKAOOAJKID MES TEJFA RAN TLAKFEDBAESOLILJHOA.

Lösung

Die Aufgabe kann mit Hilfe eines Lückentextes gelöst werden. An der Verschlüsselung der doppelt vorkommenden Buchstaben F und N und deren Verschlüsselung mit F und I lässt sich erkennen, dass es sich um eine monoalphabetische Verschlüsselung handelt. Zudem wissen wir bereits, wie das Wort Hoffnung verschlüsselt wird. Da in deutschen Texten der Buchstabe E am häufigsten vorkommt, kann davon ausgegangen werden, dass der Buchstabe A den Buchstaben E verschlüsselt, weil das A in der Verschlüsselung am häufigsten zu finden ist. Man erhält somit folgenden Lückentext.

E N _ _ _ H _ U E _ _ E _ U N G _ _ _ H _ _ F E _ E _ H _ E U F _ G _ E _ _ _ _ N _ _ _ _ E.

Die weiteren Buchstaben können jetzt relativ leicht herausgefunden werden, auch ohne die Analyse weiterer Buchstabenhäufigkeiten.

Hintergrundinformation

Die Aufgabe wurde aus den Buchstabenhäufigkeiten der deutschen Sprache und der Plansprache Esperanto entwickelt. Der häufigste Buchstabe „e“ der deutschen Sprache wurde durch den häufigsten Buchstaben „a“ der Plansprache Esperanto ersetzt. Der zweithäufigste Buchstabe „n“ wurde durch „i“ ersetzt usw. Esperanto wurde deshalb gewählt, weil in dieser Sprache der Buchstabe A und nicht wie in den meisten (lateinischen) Sprachen der Buchstabe E am häufigsten vorkommt.

Die Lösung der Dechiffrierung lautet:

ENTSCHLUESSELUNG MIT HILFE DER HAEUFIGKEITSANALYSE.

Reflexion

Aufgabe 1 war von den SuS gut lösbar, wenn sie vorher schon mit Caesar gearbeitet haben. Die Zahl der Verschiebung wurde schnell erkannt und der Satz dechiffriert. Bei Aufgabe 2 hatten die SuS anfangs grosse Probleme. Einige SuS hatte noch immer Mühe, Vigenère zu verstehen. Nachdem die SuS das Prinzip aber verstanden haben, war es den meisten SuS möglich, das Wort zu entschlüsseln und die meisten konnten sogar ein eigenes Wort verschlüsseln. Aufgabe 3 war für die SuS anfangs schwierig. Nach dem Tipp mit dem Lückentext konnte man aber mit vereinten Kräften schnell die Lösung finden.