Themen

Häufigkeitsanalyse

Bei monoalphabetischen Verschlüsselungen wie der Caesar-Verschlüsselung wird jeder Buchstabe des Klartextalphabets durch einen Buchstaben oder ein Symbol des Geheimalphabets ersetzt.

Die einzelnen Buchstaben einer Sprache kommen in einem Text unterschiedlich häufig vor. In deutschen Texten kommt beispielsweise das „E“ doppelt so häufig vor wie das „I“ und zehnmal so häufig wie das „K“.

Das nutzt man bei der Häufigkeitsanalyse. Der Erfinder dieses Verfahren zum Brechen monoalphabetischer Verschlüsselungen ist der arabische Gelehrte al-Kindi (800–873). Er gilt damit als einer der Pioniere der Kryptoanalyse, also der Kunst, einen Geheimtext ohne Schlüssel zu entziffern.

Bei der Häufigkeitsanalyse werden die einzelnen Buchstaben des Geheimtextes gezählt und ihre Häufigkeit innerhalb des Geheimtextes ermittelt.

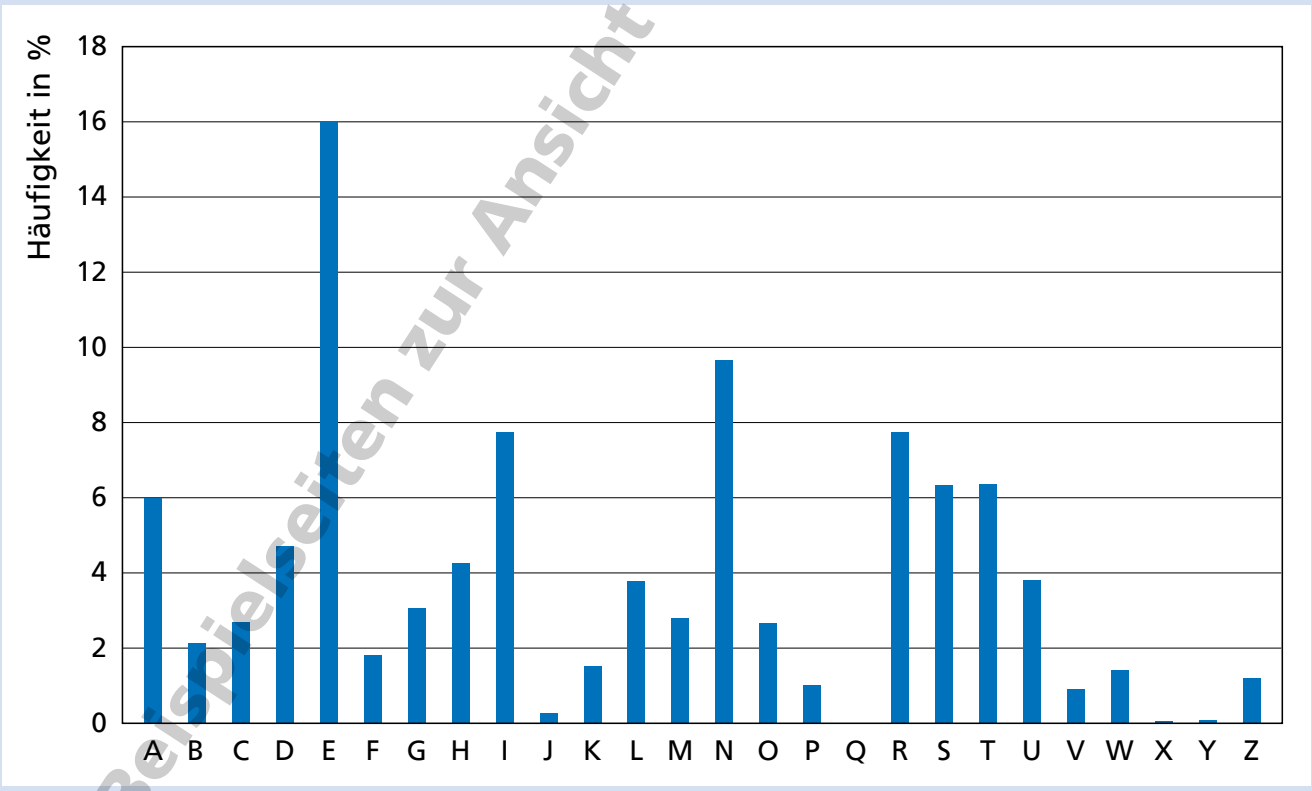
Wenn man die Sprache des Geheimtextes kennt, kann man die Häufigkeitsverteilung dann mit der eines Vergleichstextes oder einer wissenschaftlichen Statistik wie der des Instituts für Deutsche Sprache vergleichen.

Der häufigste Buchstabe oder das häufigste Symbol eines deutschen Geheimtextes steht für das Klartext-E, der zweithäufigste für das N usw.

Ist der Text mit einer einfachen Caesar-Verschlüsselung verschlüsselt, reichen diese beiden Buchstaben aus, um den Schlüssel zu ermitteln und damit den kompletten Text zu entschlüsseln.

Ist der Text mit einer Caesar-Verschlüsselung mit Schlüsselwort verschlüsselt, beginnt man nach dem Ermitteln der Buchstaben E und N zu kombinieren und kurze oder wahrscheinliche Wörter zu erraten. So gewinnt man Buchstabe für Buchstabe hinzu, bis die gesamte Verschlüsselung gebrochen und der Geheimtext entziffert ist.

Häufigkeitsverteilung der Buchstaben in der deutschen Sprache



Häufigkeitsverteilung der Buchstaben in der deutschen Sprache, ermittelt vom Leibniz-Institut für Deutsche Sprache (IDS) in Mannheim aus einer Textsammlung mit insgesamt fast 150 Milliarden Zeichen. (http://www1.ids-mannheim.de/kl/projekte/methoden/derewo.html#derechar (Stand Oktober 2019))

Häufigkeitsanalyse

Aufgabe 1
Wähle einen kurzen deutschen Text von 100 bis 200 Zeichen Länge aus und ermittle die Häufigkeitsverteilung der Buchstaben in diesem Text. Welche Buchstaben kommen am häufigsten vor?

Nutze dafür z. B. die Datei EMS_Haeufigkeitsanalyse.xlsx.

Aufgabe 2
Der folgende deutsche Text wurde mit der Caesar-Verschlüsselung verschlüsselt. (Text_Haeufigkeitsanalyse_2.txt)

KLY HYHIPZJOL NLSLOYAL HS RPUKP ZAHTTAL HBZ LPULY DVOSOHILUKLU BUK LPUMSBZZYLPJOLU HYHIPZJOLU MHTPSPL HBZ KLY YLNPVU ZBLKSPJO CVU IHNKHK TPA OPSML CVU BLILYZLAGLYU BLILYAYBN LY LPULU NYVZZALPS KLZ DLYRZ CVU HYPZA-VALSLZ BUK WSHAVU PUZ HYHIPZJOL KH LY HBJO LPNLUL WOPSVZVWOPZJOL ZJOYP-MALU CLYMHZZAL DPYK LY HBJO HSZ LYZALY WOPSVZVWO KLY HYHIPZJOLU DLSA ILGLP-JOULA ULILU KLY WOPSVZVWOPL ILMHZZAL ZPJO HS RPUKP HBJO TPA WOFZPR HZAY-VUVTPL TLKPGPU BUK RBUZA PU ZLPULU ZJOYPMALU GBY HSJOLTPL ILGDLPMLSAL LY KHZZ ZPJO NVSK BUK ZPSILY HBZ DLUPNLY DLYACVSSLU TLAHSSLU OLYZALSSLU SHZZLU

a) Ermittle die Häufigkeitsverteilung der Buchstaben im verschlüsselten Text.
Welcher Buchstabe kommt am häufigsten vor?
Nutze dafür z. B. die Datei EMS_Haeufigkeitsanalyse.xlsx.

b) Welcher Schlüssel wurde beim Verschlüsseln mit Hilfe der Caesar-Verschlüsselung vermutlich eingesetzt? Begründe deine Vermutung.

c) Überprüfe deine Vermutung, indem du den Text mit dem Gegenstück zu diesem Schlüssel entschlüsselst.

Aufgabe 3
Der folgende deutsche Text wurde mit der Caesar-Verschlüsselung verschlüsselt. (Text_Haeufigkeitsanalyse_3.txt)

UFWTFD NLPDLC HLC PTY CZPXTDNSPC QPWOSPCC PC DZWW OTP GPCDNSWFP-DDPWFYR PCQFYOPY SLMPY OTP SPFEP DPTYPY YLXPY ECLPRE XTE OPCPY STWQP VZYYEP PC XTE DPTYPY PTYSPTEPY RPSPTXP YLNSCTNSEPY LFDELFDNSPY

a) Ermittle die Häufigkeitsverteilung der Buchstaben im verschlüsselten Text.
Welcher Buchstabe kommt am häufigsten vor?
Nutze dafür z. B. die Datei EMS_Haeufigkeitsanalyse.xlsx.

b) Welcher Schlüssel wurde beim Verschlüsseln mit Hilfe der Caesar-Verschlüsselung vermutlich eingesetzt? Begründe deine Vermutung.

c) Überprüfe deine Vermutung, indem du den Text mit dem Gegenstück zu diesem Schlüssel entschlüsselst.

Ende-zu-Ende-Verschlüsselung

Mehr als zwei Stunden täglich verbringen Jugendliche und junge Erwachsene mit der Nutzung von Chat- oder Messengerdiensten. Das ergaben Studien zur Mediennutzung von Jugendlichen in Deutschland, die in den „Grunddaten Jugend und Medien 2020“ zusammengefasst sind. [1)]

Selbstverständlich möchte niemand, dass die mit Freundinnen und Freunden ausgetauschten Nachrichten von Dritten mitgelesen werden. Deshalb haben die Anbieter von E-Mail-, Chat- und Messengerdiensten Verfahren zu Verschlüsselung aller übertragenen Daten etabliert.

Problem der Schlüsselverteilung

Bis in die 1970er Jahre hinein kannte man nur symmetrische Verschlüsselungsverfahren, bei denen Sender und Empfänger einer Nachricht über denselben Schlüssel verfügen müssen.

Das führt im Smartphone-Zeitalter zu der Schwierigkeit, dass für viele geheim kommunizierende Personen auch viele unterschiedliche Schlüssel benötigt werden. Die Anzahl lässt sich aus der Anzahl der Messengerdienst-Nutzer errechnen:

$$\text{Anzahl Schlüssel} = \frac{\text{Nutzer} \times (\text{Nutzer} - 1)}{2}$$

Wollten alle zwei Milliarden WhatsApp-Nutzer miteinander verschlüsselte Nachrichten austauschen, wären dafür zwei Trillionen Schlüssel nötig.

Asymmetrische Verschlüsselung

Das so genannte Schlüsselverteilungsproblem wurde erst 1977 gelöst, als Ronald L. Rivest, Adi Shamir und Leonard M. Adleman am Massachusetts Institute of Technology das nach ihnen benannte RSA-Verfahren entwickelten.

Bei diesem ersten asymmetrischen Verschlüsselungsverfahren verfügt jeder Nutzer über ein eigenes Schlüsselpaar: einen öffentlichen und einen privaten Schlüssel.

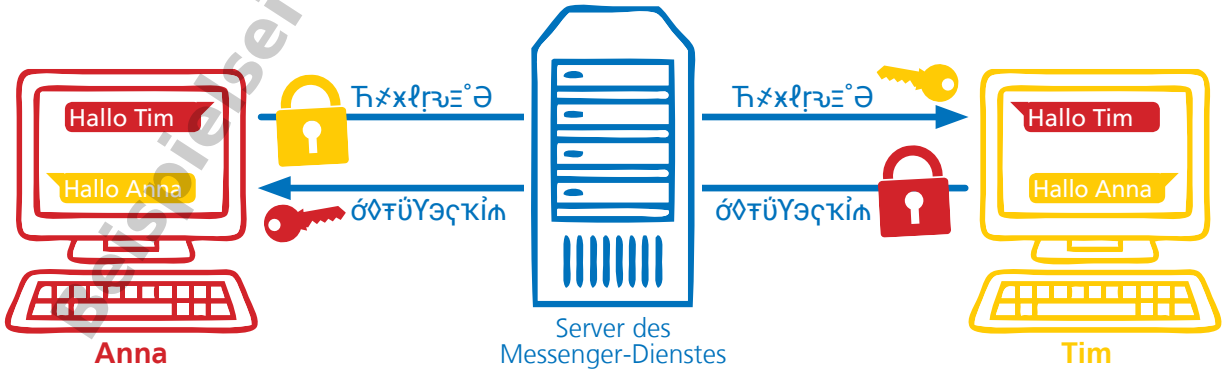
Asymmetrische Verschlüsselungsverfahren benötigen mehr Rechenleistung für das Ver- und Entschlüsseln der Daten, aber sie sind sicherer als symmetrische Verschlüsselungsverfahren. Sie ermöglichen eine sichere Kommunikation im Internet, ohne immense Kosten und Komplexität zu verursachen.

Mit den öffentlichen Schlüsseln können Daten nur verschlüsselt werden. Die öffentlichen Schlüssel aller Nutzer und Nutzerinnen eines Messengerdienstes sind in einem Verzeichnis abgelegt, auf das alle Nutzer und Nutzerinnen des Messengerdienstes zugreifen können.

Möchte Anna eine Nachricht an Tim senden, verschlüsselt sie die Nachricht mit dem öffentlichen Schlüssel von Tim. Die Nachricht ist auf dem Weg zu Tim von niemandem zu entziffern. Nur der zu Tims öffentlichem Schlüssel passende private Schlüssel kann die Nachricht entschlüsseln. Die Antwort an Anna verschlüsselt Tim mit Annas öffentlichem Schlüssel. Und nur sie kann mit ihrem privaten Schlüssel Tims Nachricht entschlüsseln.

Da das Ver- und Entschlüsseln nur beim Sender und Empfänger einer Nachricht möglich ist, spricht man von einer Ende-zu-Ende-Verschlüsselung. Beim Austauschen von Nachrichten bemerkt man davon nichts, denn Messengerdienste wie WhatsApp führen das Ver- und Entschlüsseln vollständig ohne unser Zutun durch.

Ende-zu-Ende-Verschlüsselung bei einem Messengerdienst



[1)] https://www.br-online.de/jugend/izi/deutsch/Grundddaten_Jugend_Medien.pdf (Stand Juni 2021)

Ende-zu-Ende-Verschlüsselung

Aufgabe 1
Stell dir vor, ihr würdet in eurer Klasse über einen Messengerdienst symmetrisch verschlüsselte Nachrichten austauschen.

Wie viele unterschiedliche symmetrische Schlüssel wären notwendig, damit jede Schülerin und jeder Schüler mit allen anderen Schülerinnen und Schülern deiner Klasse Nachrichten austauschen kann?

Aufgabe 2
Beschreibe den Ablauf der Ende-zu-Ende-Verschlüsselung bei einem Messengerdienst.

Aufgabe 3
Warum kann der Betreiber des Messengerdienstes die auf seinem Server zwischengespeicherten Nachrichten nicht lesen?

Aufgabe 4
Worin besteht der wichtigste Unterschied zwischen symmetrischen und asymmetrischen Verschlüsselungen?