Mathematik-Modellierungstage 2020  
Mi. 15.01 und Do. 16.01.2020  
Thema 1: VERSCHLÜSSELUNGSMETHODEN

EINLEITUNG

Die Verschlüsselung von Botschaften stellt ein zentrales Element der elektronischen Nachrichtenübermittlung im aktuellen Informationszeitalter dar. In je größerem Umfang die Speicherung und Übermittlung von Daten auf digitale Medien übertragen wird, desto wichtiger werden sichere Verschlüsselungsmethoden.

Das Thema mag auf den ersten Blick mysteriös klingen: Geheimdienste, Hacker oder militärische Anwendungen sind oft die ersten Assoziationen. Doch man braucht gar nicht so weit zu blicken: täglich verwendete Nachrichtendienste wie *WhatsApp*, *iMessage*, *Signal* oder *Threema* benutzen eine so genannte Ende-zu-Ende Verschlüsselung (end-to-end encryption – „E2E“), die garantiert, dass eine Nachricht nur von Absender und Empfänger und sonst von niemandem dazwischen gelesen werden kann. Verschlüsselungstechniken verbergen sich auch hinter dem bekannten Kürzel *https* (*hypertext transfer protocol secure*). Dieses Übertragungsprotokoll für Inhalte von Internetseiten wurde 1994 eingeführt und gewährleistet eine abhörsichere Datenübertragung zwischen Server und Anwender (Client). Man sieht: Verschlüsslung ist überall und wird von uns täglich verwendet.

ZIELE

Die genaue Funktionsweise der oben genannten, aktuellen Verschlüsselungsmethoden ist komplex und ihr Verständnis setzt großes Fachwissen in den Bereichen Mathematik und Programmierung voraus. In dieser Arbeit soll es deshalb vielmehr um die Erarbeitung einfacherer Methoden zur Ver- und Entschlüsselung gehen, die zum Teil schon seit der Antike in Gebrauch sind.

Besonders interessant ist die Entschlüsselung geheimer Botschaften. In dieser Hinsicht sollen Texte auf die Häufigkeit der darin vorkommenden Buchstaben hin analysiert werden und mit Softwareunterstützung (Excel oder Wolfram) **Buchstabenhäufigkeitsprofile** für verschiedene Sprachen erstellt werden. So soll erkannt werden, in welcher Sprache ein verschlüsselter Text verfasst ist. Mit etwas Glück kann der Text dann auch entschlüsselt werden!

Nicht direkt mit Verschlüsselung hat die so genannte **Gödelisierung** von Worten zu tun. Dennoch stellt dieses Verfahren eine wichtige Grundlage für die Darstellung eines Wortes als Zahl. Ziel ist es, ein Wort in eine Zahl umzurechnen, sodass aus dieser Zahl wieder eindeutig das ursprüngliche Wort gelesen werden kann.

Ist dann noch Zeit und Motivation übrig, soll die grundlegende Arbeitsweise einer asymmetrischen Verschlüsslung am Beispiel der **RSA-Verschlüsselung** erarbeitet werden.

AM ENDE...

geht es wie im vergangenen Jahr darum, die gewonnenen Erkenntnisse anschaulich darzustellen und vor zahlreich erscheinendem Publikum zu präsentieren.

SCHRITT FÜR SCHRITT

1. Erfinde selbst Möglichkeiten, Nachrichten zu verschlüsseln. Lasse deiner Phantasie freien Lauf und versuche einzuschätzen, wie leicht (oder schwer) deine Verschlüsselung geknackt werden kann. Versuche, die verschlüsselten Nachrichten deines Kollegen bzw. deiner Kollegin zu entschlüsseln.
2. Informiere dich im Internet über verschiedene historische Verschlüsselungsmethoden, z.B. Caesar-Code, Vigenère-Chiffre, ... und versuche, eigene Texte zu verschlüsseln.

Eine sehr gute Seite zu diesem Thema ist <https://www.cryptool.org/de/>

1. Lies die rot markierten Passagen zum Caesar-Code aus dem Skript „RSA – Primzahlen zur Verschlüsselung von Nachrichten“ (Seiten 4, 5, 7, 8, 9) und bearbeite dann die Aufgaben auf Seite 22.

Gib den Unterschied zwischen symmetrischen und asymmetrischen Verschlüsselungsverfahren an.

1. Benutze Excel, um eine Caesar-Verschlüsselung durchzuführen.

YouTube-Videos zur Hilfe

Botschaften mit dem Cäsar-Code verschlüsseln: <https://www.youtube.com/watch?v=4tdKnv3gJW0>

Caesar Cipher Solver 2/3: <https://www.youtube.com/watch?v=pIzcZvXBo98>

Caesar Cipher Solver 3/3: <https://www.youtube.com/watch?v=ZP3D171tVmc>

Text in einzelne Buchstaben auftrennen:

<https://supportnet.de/excel-formeln-einzelne-zeichen-eines-strings-auf-zellen-aufteilen4660/>

1. Lies auf Seite 8 den mit dem Stern markierten Absatz erneut durch. Um diese Buchstabenhäufigkeitsverteilungen soll es nun gehen.

Ziel ist es, mit Excel die Häufigkeiten der Buchstaben in verschiedenen Sprachen herauszufinden und jeweils ein Häufigkeitsprofil anzugeben, das typisch für die jeweilige Sprache ist.

Hilfreich: <http://www.excelformeln.de/formeln.html?welcher=96>

1. Versuche herauszufinden, in welcher Sprache der folgende Text geschrieben ist und um wie viele Zeichen er versetzt wurde.

JGY KXYZK YINARZNKGZKX NGHKT COX 1995 GTRÄYYROIN JKX 50-PGNX-LKOKX JKX KNKSGROMKT RKNXKXHORJATMYGTYZGRZ SKXGT OS QAXNGAY BUT SKXGT GAL JOK HÜNTK MKHXGINZ. JGY YZÜIQ TGTTZK YOIN JOK ZXKVVK. COK YU ULZ NGHK OIN SOZ JKT YINÜRKXT ATJ YINÜRKXOTTKT JKT ZKDZ MKYINXOKHKT ATJ JA NGYZ ONT SOZ BOKR QÖTTKT ATJ BKXZXGAKT OT JOK PATMKT SKTYINKT GAL JOK HÜNTK MKHXGINZ. JGY RKZFZK MKSKOTYGSK YINARZNKGZKX SGINZKT COX OS PGNXK 2017. OT GTRKNTATM GT JKT XUSGT YAVKXMAZK ZGMK BUT SGXQ NGJJUT YINXOKH JOK QRGYYK JOK HÜNTKTLGYYATM SKOTK KOMKTK CKRZ ATJ JA NGYZ JOK QUSVRKDK ZNKSGZOQ JKY GAZNOYSAY MKSKOTYGS SOZ JKT YINÜRKXT OT JKOTKS ZNKGZKX OT JKX GRZYZGJZ ÄAYYKXYZ ÜHKXFKAMKTJ ASMKYKZFZ. FCOYINKT JOKYKT HKOJKT YINARZNKGZKXT ROKMKT PGNXK ATJ PÄNXROIN HXGINZKT COX KOT ZNKGZKXYZÜIQ SOZ YINÜRKXT ATJ YINÜRKXOTTKT GAL JOK HÜNTK. JA MRGAHZKYZ OSSKX GT ONXK HKMKOYZKXATMYLÄNOMQKOZ, NGYZ ONTKT JGJAXIN BKXZXGAKT ATJ YKRHYZYOINKXNKOZ MKMKHKT, NGYZ SOZ ONTKT JOYQAZOKXZ, YOK GAIN SGTINSGR JOQZOKXZ, GHKX YOK YOTJ OSSKX JKOTKT XKMOKGTCKOYATMKT MKLURMZ, CKOR YOK OT JKOTKX RKOJKTYINGLZROINKT GXHKOZ ATJ OT JKOTKT ÜHKXFKAMKTJKT GXMASKTZKT KOT BUXHORJ LÜX YOIN YGNKT, YOIN BUT JOX KXTYZ MKTUSSKT LÜNRZKT ATJ JGJAXIN OSSKX YZÄXQKX OT ONXK XURRKT NOTKOTCAINYKT.

Mit einem Online-Tool kannst du den Text nun wieder entschlüsseln.

<https://www.cryptool.org/de/cto-chiffren/caesar>

1. Suche nun selbst Texte in verschiedenen Sprachen, verschlüssle sie mit dem Online-Tool und erstelle Häufigkeitsprofile.
2. Wenn noch Zeit und Motivation besteht, informiere dich zum zum Thema Gödelisierung:

Gödelisierung

<https://www.youtube.com/watch?v=tdePgobellU>

Fundamentalsatz der Algebra

<https://www.youtube.com/watch?v=qv4sLT55c0k>

Die Primfaktorzerlegung großer Zahlen kannst du in Geogebra erledigen:

Ansicht > CAS > Faktorisiere

1. Erstellt gemeinsam eine Präsentation, die ca. 7 bis 8 Minuten dauert, spannend ist und die Ergebnisse eurer Arbeit verständlich darstellt.