

Aufgaben

Aufgabe: Verwandle mit einem Python-Programm das Wort „SECURITY“ in Morsecode.

Lösung: ... -.-. -.-. -.-. -.-. -.-.

Aufgabe (Python oder Notepad++): Knacke diesen Geheimtext: AGCNOCDHCMHI-HHMTOEUEEENNNIRK. Was ist der Schlüssel?

Lösung: ACHTUNGDIIEICHHOERNCH-ENKOMMEN

Aufgabe: Entschlüssele RNRLEGEWEEMR-IBNEEGUEERN mit dem Gartenzaunverfahren Lösung:

ZigZag fuer Tiefe 4:

R N R L
E G E E W E M
R I B N E E G U
E E R N

Aufgabe: Berechne alle 26 Rotationsmöglichkeiten (= verschiedene Schlüssel), um den Geheimtext, ein Zitat von Alan Turing, zu entschlüsseln: „Znyuk cnu igt osgmotk gteznotm, igt ixkgzk znk osvuyyohrk.“

Lösung: THOSE WHO CAN IMAGINE ANYTHING, CAN

CREATE THE IMPOSSIBLE (Schlüssel 6)

Aufgabe: Verschlüssele unter Linux mit tr den Klartext „ATBASH“.

Lösung: NGONFU

Aufgabe: Verschlüssele mit der obigen Tabelle den Klartext „MEINE OMA“.

Lösung: HUYIU MHP

Aufgabe: Entschlüssele die Nachricht auf der Kaffeetasse, die man im Shop der NSA im National Cryptologic Museum in Fort Meade kaufen kann! Achtung: Auch die NSA macht Fehler :-)

Lösung: NATEONAMSECURITZAGENCZ

Aufgabe: Entschlüssele unter Verwendung des Schlüssels „CRYPTO“ die Nachricht „YKKQKQLBREQKQRSODZGVCQOKAC-AYBOFKMHORAEDZ“ mit Hilfe der Webseite <https://www.dcode.fr/playfair-cipher> (Achtung: Die Lösung erscheint immer in der Spalte ganz links oben!

Aufgaben (cont)

Lösung: THISISNOTASIMPLEEXAMPLEF-ORBRAEKINGACODEX

Aufgabe: Entschlüssele den englischen Text „vhxcpinebuighvhxeokpeknwvhxrettilvh-xtemqo“ via Website <https://www.dcode.fr/vigenere-cipher>: zuerst mittels Kasiski-Test die Key-Länge ermitteln, dann mit „Knowing the Key-Length“ broken! Es ginge auch über „Knowing a Plaintext Word“, weil z. B. in englischen Texten oft das Wort „THE“ vorkommt.

Lösung: theappleisinthecornerandthepearis-theretoo

Aufgabe: In Poznan (ehemals Posen, heute Stadt in Polen) gibt es ein kleines, aber feines Museum zu Ehren der drei polnischen Codebreaker, die die erste Enigma entschlüsselt haben. Es hat die Form einer echten Enigma und steht vor der Universität. Wie hießen die drei? Was ist ihre Geschichte? Wie wurden sie von den Engländern (auch lange nach dem Krieg noch) behandelt? Welchen Anteil hatte Alan Turing an der Entschlüsselung? Wann wurde er rehabilitiert bzw. begnadigt?

Lösung: Jerzy Rozycki, Henryk Zygaliski and Marian Rejewski

Cäsar

Jahr 50 v. Chr.

Beruh auf monoalphabet. Subst.

Kryptoanalytische Methode Häufigkeitsanalyse

Gebrochen Ja

Vigènere

Jahr 16. Jhdt.

Beruh auf monoalphabet. Subst.

Kryptoanalytische Methode Kasiski-Test, Häuf.

Gebrochen Ja

Freimaurer

Jahr 19. Jhdt.

Beruh auf Substitution

Kryptoanalytische Methode Häufigkeitsanalyse

Gebrochen Ja

One-Time-Pad

Jahr ab 20. Jhdt.

Beruh auf polyalphabet. Subst.

Kryptoanalytische Methode -

Gebrochen Nein

Enigma

Jahr ab 1918

Beruh auf polyalphabet. Subst.

Kryptoanalytische Methode Brute-Force mit Turing-Bombe

Gebrochen Ja

Skytale

Jahr 2500 v.Chr.

Beruh auf Transposition

Kryptoanalytische Methode Brute-Force

Gebrochen Ja