Aufgaben

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

Lösung: ... . -.-. ..- .-. .. - -.--

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

Lösung: ACHTUNGDIEEICHHOERNCH-ENKOMMEN

Aufgabe: Entschlüssle RNRLEGEEW-EMRIBNEEGUEERN 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: „Znuyk 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: Entschlüssle 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

Aufgaben (cont)

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

Lösung: THISISNOTASIMPLEEXAMPLEF-ORBRAEKINGACODEX

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

Lösung: theappleisinthecornerandthepearistheretoo

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 Zygalski and Marian Rejewski

Cäsar

Jahr	50 v. Chr.
Beruht auf	monoalphabet. Subst.
Kryptoanalytische Methode	Häufigkeitsanalyse
Gebrochen	Ja

Vigènere

Jahr	16. Jhdt.
Beruht auf	monoalphabet. Subst.
Kryptoanalytische Methode	Kasiski-Test, Häuf.
Gebrochen	Ja

Freimaurer

Jahr	19. Jhdt.
Beruht auf	Substitution
Kryptoanalytische Methode	Häufigkeitsanalyse
Gebrochen	Ja

One-Time-Pad

Jahr	ab 20. Jhdt.
Beruht auf	polyalphabet. Subst.
Kryptoanalytische Methode	-
Gebrochen	Nein

Enigma

Jahr	ab 1918
Beruht auf	polyalphabet. Subst.
Kryptoanalytische Methode	Brute-Force mit Turing-Bombe
Gebrochen	Ja

Skytale

Jahr	2500 v.Chr.
Beruht auf	Transposition
Kryptoanalytische Methode	Brute-Force
Gebrochen	Ja