Einführung

Kryptologie ist eine Wissenschaft, die sich mit der Verschlüsselung und Entschlüsselung von Informationen beschäftigt. Lässt sich unterteilen in:
•Kryptografie: Verschlüsselung von Informationen.
•Kryptoanalyse: Informationsgewinnung aus verschlüsselten Informationen.
Begriffe:
•Verschlüsselung (Chiffrierung): Ein lesbarer Text wird in eine nicht leserliche Zeichenfolge umgewandelt.
•Entschlüsselung (Dechiffrieren): Deutung unbekannter Zeichen, Symbole bzw. die Umwandlung in bekannte Zeichen.
•Entzifferung (Brechen, Knacken): Eine kryptanalytische Methode bei der aus einem Geheimtext ein Klartext gewonnen wird.

Atbash

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A

Eine Verschiebe-Chiffre mit dem Schlüssel 25 und entspricht somit einer Umkehrung des Alphabets.

Gartenzaun-Verfahren

Gartenzaun-Verfahren: Wenn man den Text entschlüsseln will, muss man nur die Buchstaben in zwei Zeilen schreiben und jeden zweiten Buchstaben hochziehen. Man kann auch mehr als zwei Zeilen verwenden.

Freimaurerchiffre

Das Alphabet besteht aus Symbole. Hier sieht man des US-amerikanische System

Aufgabe 1: Python Morsecode

Aufgabe 4: Cäsar-Chiffre

„Znuyk cnu igt osgmotk gteznotm, igt ixkgzk znk osvuyyohrk.“
6 mal verschieben
Those Who can imagine anYthing, can create the impossible.

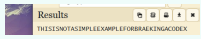
Aufgabe 7: Monographische Substitution

MEINE OMA
HUYIU MHP

Aufgabe 10: crypto interactive website

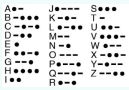
YKKQKQLBREQKQRSODZGVCQOKACA-YBOFKMHORAEDZ mit CRYPTO als Schlüssel

Aufgabe 10: crypto interactive website



YKKQKQLBREQKQRSODZGVCQOKACA-YBOFKMHORAEDZ mit CRYPTO als Schlüssel

Morsecode

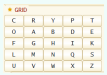


Morsezeichen: Zeichensatz zur Übermittlung von Buchstaben und Ziffern.
Symbole:
• Kurzes Signal
• Langes Signal
• Pause

Cäsar-Chiffre und ROT13

Jeder Buchstabe der Nachricht wird um drei Stellen im Alphabet nach links versetzt. Jeder Buchstabe im normalen Alphabet wird dann durch den im neuen ersetzt. Verschlüsselung mit dem Schlüssel 13.

Playfair–Verfahren



Mithilfe eines bestimmten Alphabets wird der Text entschlüsselt.
Key plus alle restlichen Buchstaben aus dem Alphabet.

Aufgabe 2: Skytale

A C H T U N G D I E E I C H H O
E R N C H E N K O M M E N
ACHTUNGDIEEICHHOERNCHENK-
OMMEN

Aufgabe 5: ROT13 entschlüsseln

Aufgabe 8: Freimaurerchiffre

NATEONAM
SECURITZ
AGENCZ

Aufgabe 11: Playfair-Verfahren

Theappleisinthecornerandthepearistheretoo
– Key muss durch 3 teilbar sein

Skytale

Skytale ist ein sehr altes Verschlüsselung-sverfahren. Man benötigte einen Holz-Stab mit bestimmtem Durchmesser.
Der Schlüssel ist der Durchmesser.

Häufigkeitsanalyse

Bei dieser Methoden werden statistische Eigenschaften des verschlüsselten Textes ausgenutzt, um Rückschlüsse auf die unverschlüsselte Nachricht zu ziehen.
Je länger der verschlüsselte Text, desto sicherer ist die Häufigkeitsanalyse.

Monographische Substitution

Ein Verschlüsselungsverfahren, bei dem nur ein einziges Alphabet zur Verschlüs-selung, also zur Umwandlung des Klartextes in den Geheimtext, verwendet wird.

Kasiski-Test

Wenn bestimmte Wörter oder Wortteile öfter auftreten kommt dieser Test ins Spiel (meistens bei der Vigenère-Verschlüssel-ung).
Es wird ein verschlüsselter Text nach gleichen Zeichenfolgen untersucht und der Abstand zwischen diesen Buchstaben ermittelt.
Der Abstand dieser Zeichenketten ist dann ein Vielfaches der Schlüsselwortlänge.

Aufgabe 3: Gartenzaun-Verfahren

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

Aufgabe 6: ROT13 verschlüsseln

Aufgabe 9: Häufigkeitsanalyse

YXDY PQ YJC XZPVPYW YA ICQDEPZC
AYJCEQ XQ YJCW QCC
YJCUQCVRCQ. XZEXJXU VPSDAVS

tact is the ability to describe others as they see
themselves. abraham lincoln

Aufgabe 12: Enigma Geschichte

Wie heißen die drei Wissenschaftler, die die Enigma entschlüsselt haben?
• Marian Rejewski: Hat nach dem Krieg weiter geforscht.
• Jerzy Różycki: Ist noch vor Ende des Krieges verstorben
• Henryk Zygalski: Nach dem Krieg als Mathelehrer tätig.
Alan Turing war während des zweiten Weltkrieges an der Entzifferung von Funksprüchen beteiligt, die mit der Enigma verschlüsselt wurden.
Am Weihnachtsabend, dem 24. Dezember 2013 sprach Königin Elisabeth II eine königliche Begnadigung aus.