Aufgaben

Verfahren	Geheimtext	Klartext
Transposition	RNRLEGEEWEMRIBNEEGUEERN	REGENWURMERLIEBENREGEN
Caesar–Chiffre	Znuyk cnu igt osgmotk gteznotm, igt ixkgzk znk osvuyyohrk.	THOSE WHO CAN IMAGINE ANYTHING, CAN CREATE THE IMPOSSIBLE. (Key 8)
Caesar–Chiffre	URYYB JBEYQ	HELLO WORLD
Monographische Substitution	MEINE OMA	HUYIU MHP
Polygraphische Substitution	YKKQKQLBREQKQRSODZGVCQOKACA-YBOFKMHORAEDZ	DEERERKATORERTISCHMZURSENUNDASGELBSTNOCH
Polyalphabetische Substitution	vhxcpinebuigvhxeokpekcnwvhxrettilvhxtemqo	theappleisinthecornerandthepearistheretoo

Verfahren

Verfahren	Erklärung
Morsezeichen	Besteht aus drei Symbolen: kurzes Signal, langes Signal und Pause
Caesar–Chiffre	Jeder Buchstabe um drei Stellen im Alphabet nach links versetzt
ROT13	Die Zuordnung der Klar- und Geheimtextbuchstaben ist symmetrisch (A → N und N → A)
Atbash	Diese Verschlüsselung ist eine Verschiebe-Chiffre mit dem Schlüssel 25 und entspricht einer Umkehrung des Alphabets (A – und Z → A)
Freimaurerchiffre	Diese Geheimschrift basiert auf der Kabbala der neun Kammern
Häufigkeitsanalyse	Statistische Eigenschaften des verschlüsselten Textes ausgenutzt, um Rückschlüsse auf die unverschlüsselte Nachricht zu z
Playfair–Verfahren	Jedes Buchstabenpaar des Klartextes durch ein anderes Buchstabenpaar ersetzt wird
Vigenère Cipher	Ein Schlüsselwort bestimmt, wie viele und welche Alphabete genutzt werden. Die Alphabete leiten sich aus der Caesar-Subs itution ab
Kasiski-Test	Hilfsmittel zur Entzifferung von Chiffraten, die mit dem Vigenère-Verfahren erzeugt wurden
Enigma	Rotor-Schlüsselmaschine; Wurde zur verschlüsselung des Nachrichtenverkehrs der Wehrmacht verwendet

Definitionen	
Begriff	Erklärung
Kryptologie	Ist eine Wissenschaft, die sich mit der Verschlüsselung und Entschlüsselung von Informationen und somit mit der Informationssicherheit beschäftigt.
Kryptografie	Verschlüsselung von Informationen
Kryptoanalyse	Die Informationsgewinnung aus verschlüsselten Informationen
Verschlüsselung (Chiffrierung)	Vorgang, bei dem ein klar lesbarer Text in eine nicht einfach interpretierbare Zeichenfolge umgewandelt wird
Entschlüsselung (Dechiffrierung)	Beschreibt im weiteren Sinne die Deutung unbekannter Zeichen, Symbole, bzw. deren Umwandlung in bekannte Zeichen
Entzifferung (Brechen, Knacken)	Eine kryptanalytische Methode, die aus einem Geheimtext ohne vorherige Kenntnis des Schlüssels den Klartext gewinnt
Substitution	Ein Element a der Menge A wird genau einem Element b der Menge B zugeordnet
Transposition	Transposition ist das Gegenstück zur Substitution. Die Buchstaben werden nicht ausgetauscht, sondern anders positioniert
Mono- alphabetische Chiffrierverfahren	Gekennzeichnet sind diese Chiffren dadurch, dass derselbe Chiffrierschritt wiederholt angewandt wird