Kryptologie

Verschlüsselungstechniken
von Cäsar bis heute

Arnulf May

Inhalt

- Was ist Kryptologie
- Caesar – Verschlüsselung
- Entschlüsselungsverfahren
- Die Chiffrierscheibe
- Bestimmung der Sprache
- Vigenére – Verschlüsselung
- Moderne Verschlüsselungsverfahren

Was ist Kryptologie?

Kryptologie ist die Wissenschaft vom Verschlüsseln, aber auch Entschlüsseln von Botschaften und Texten

Das Wort Kryptologie stammt aus dem Griechischen (kryptos – verborgen)

Was ist Kryptologie?

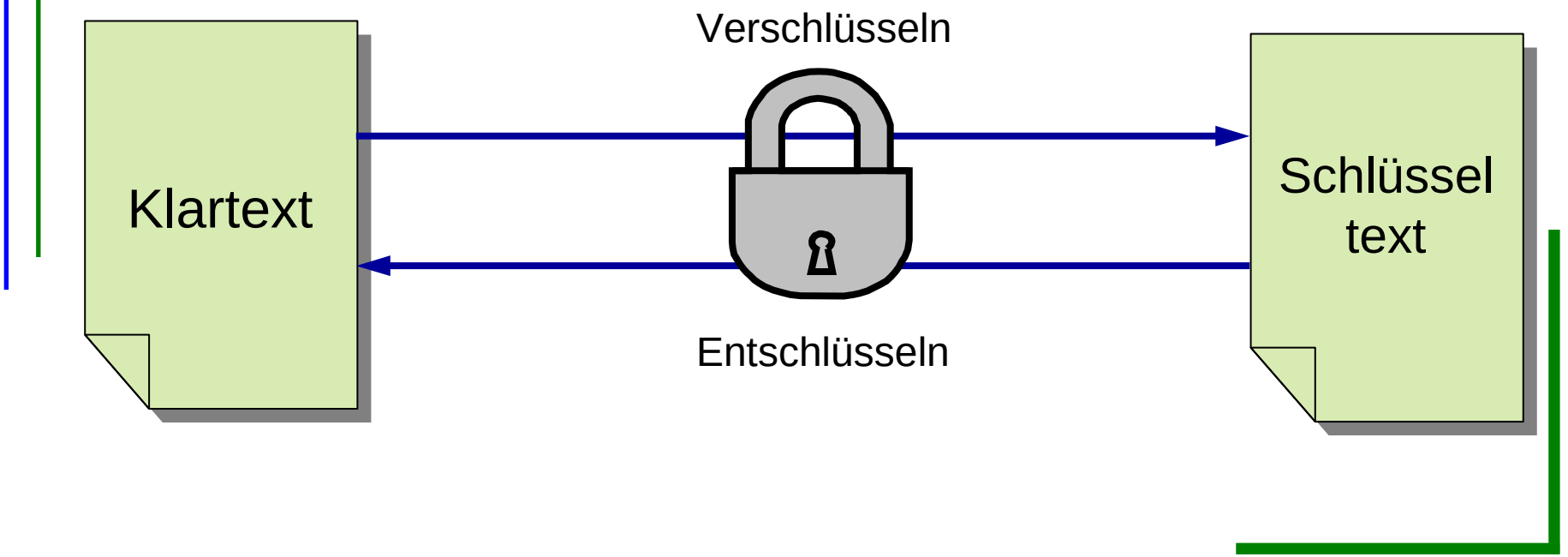
Man unterscheidet zwei Bereiche:

Das Verschlüsseln und die Entwicklung der dazugehörigen Verfahren – Kryptographie

Das Entschlüsseln und die Entwicklung der dazugehörigen Verfahren – Kryptoanalyse

Begriffe

Begriffe der Kryptologie



Einsatzgebiete

Früher: Herrscher, Militär

Heute: Militär, Geheimdienst, Internetuser, Telefon, Handy

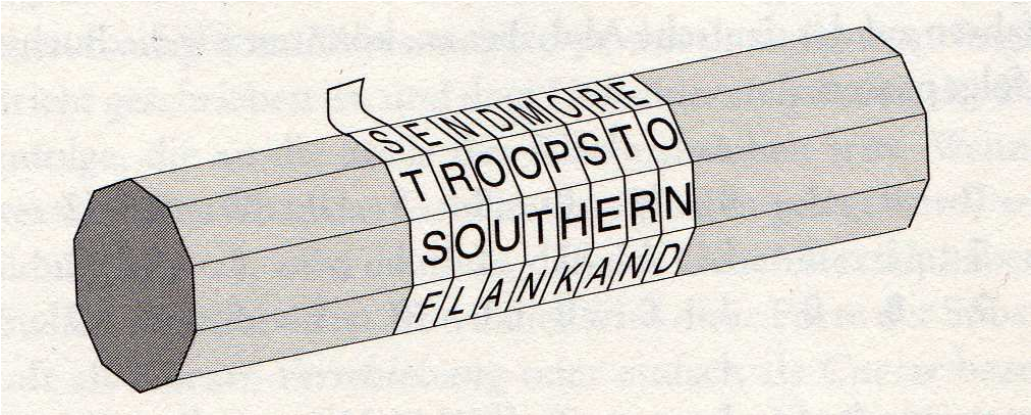
Verfahren und Lösungen durch

Linguistiker, Mathematiker, *Informatiker*, *Physiker*

Die Skytale

Geheime Botschaft der Spartaner

Paperstreifen wurde um einen Stab gewickelt.



Lösung: Aufwickeln auf Stab gleicher Dicke

Die Transposition

Die Buchstaben einer Botschaft werden anders angeordnet

TOM – TMO, OTM, OMT, MTO, MOT

Bei 3 verschiedenen Buchstaben gibt es $3 \cdot 2 \cdot 1 = 6$ Möglichkeiten

Die Transposition

Vorteil: Bei langer Botschaft viele Möglichkeiten

Nachteil: Bei zufälliger Anordnung praktisch nicht entschlüsselbar

Die Caesar – Verschiebung

Die Caesar - Verschiebung ist eines der ältesten Verschlüsselungsverfahren.

Jeder Buchstabe wird durch einen anderen Buchstaben des Alphabets ersetzt. Der Schlüssel ist die Länge der Verschiebung.

Häufigkeitsanalyse

Lösungsschritte

Wie oft kommt jeder Buchstabe vor?

Häufigkeitstabelle gegenüberstellen

Eindeutige Buchstaben ersetzen

Logische Folgerungen und Raten

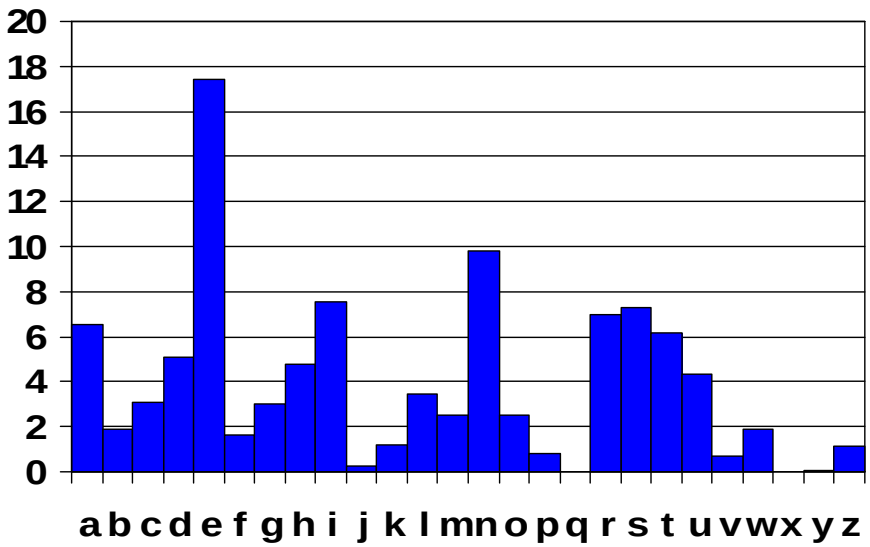
Sprachanalyse

In welcher Sprache ist der Geheimtext geschrieben?

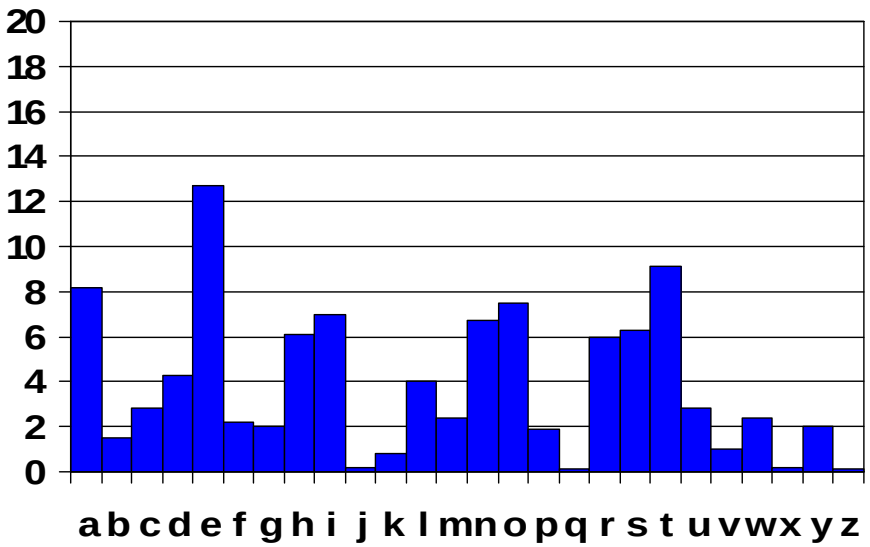
Häufigkeiten der einzelnen Buchstaben unterscheiden sich.

Sprachanalyse

Deutsch



Englisch



Von Cäsar zu Vigenére

Verschlüsselung: CÄSAR

Entschlüsselung: Häufigkeitsanalyse

Ziel: Analyse erschweren, Häufigkeiten müssen verschleiert werden

Von Cäsar zu Vigenére

Alberti – Verschlüsselung:

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

Die Alphabete werden abwechselnd benutzt.
Klartext: Mathematik
Schlüsseltext: QNXLIZEGMX

Die Vigenére - Verschlüsselung

Der Franzose Blaise de Vigenére entwickelte die Methode von Alberti weiter.

Vigenére verwendet bis zu 26 Geheimtextalphabete

Sie werden mit einem Schlüsselwort miteinander verknüpft.

Die Vigenére - Verschlüsselung

Das Vigenére - Quadrat

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

Die Vigenére - Verschlüsselung

Sicherheit:

- je länger der Schlüssel, desto sicherer
- der Schlüssel ver- und entschlüsselt
  ➔ größte Geheimhaltung
- Klartext und Kryptogramm lassen auf Schlüssel schließen
- le chiffre indéchiffrable

Mr. Babbage

Babbage entschlüsselt die sichere Vigenére – Verschlüsselung

Suche nach der Länge des Schlüssels

Häufigkeitsanalyse

Das ONE TIME PAD

Der Schlüssel ist so lang wie die Botschaft

Der Schlüssel besteht aus einer zufälligen Zeichenfolge

Der Schlüssel wird nur einmal benutzt

Das ONE TIME PAD – Probleme

Keine sinnvollen Wörter

Man benötigt viele verschiedene Schlüssel

Der Empfänger muss den Schlüssel kennen und sicher erhalten

Enigma

Die elektronische Version der Chiffrierscheibe

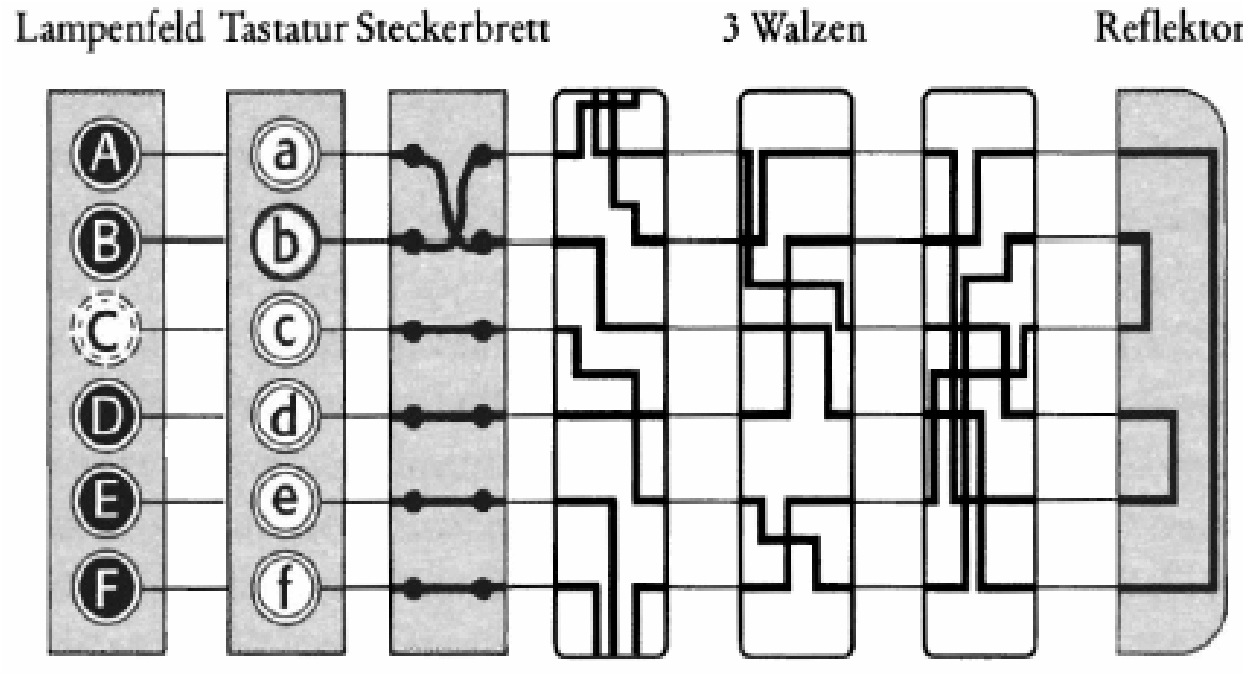
Erfinder: Arthur Scherbius

Einsatz:

Deutsche Wehrmacht im 2. Welt

Enigma – Funktionsweise

Verbesserte Version – Ende des 2. Weltkriegs



Enigma – Möglichkeiten

Walzenstellungen: $26 \cdot 26 \cdot 26 = 17576$

Walzenlagen: $3! = 6$

Steckerbrett: $\frac{26!}{14! \cdot 6! \cdot 2^6} = 100391791500$

Gesamt: $17576 \cdot 6 \cdot 100391791500 > 1 \cdot 10^{16}$

Enigma – Entschlüsselung

Tagesschlüssel – Walzenstellung

Steckverbindungen der 6 Buchstabenpaare

Entschlüsselung durch *Mathematiker*

Marian Rejewski (POL), Alan Turing (GB)

Entwicklung des Computers

Moderne Verschlüsselung

Kryptographen nutzen den Computer

Jedes Zeichen wird in eine Zahlenfolge umgewandelt (0, 1)

ASCII – Code: 7 Bit stehen zur Verfügung

Restklassen, Modulrechnungen

Einwegfunktionen

Alle möglichen Zahlenwerte werden auf eine endliche Menge von Zahlen abgebildet

Entspricht einer Division mit Rest

Ziel: Geheimhaltung des Schlüssels

Restklassen, Modulrechnungen

Beispiel – Uhr

modulo 12
mod (12)

11 + 4 = 3 mod(12)
27 + 40 = 67 = 7 mod(12)

Public-Key-Kryptographie

Asymmetrische Verschlüsselung

Öffentlicher und privater Schlüssel

Jeder kann Mitteilung verschlüsseln, nur einer kann die Mitteilung lesen.

Public-Key-Kryptographie

RSA – Verschlüsselung
Rivest, Shamir, Adleman

Primzahlen, Sieb des Erathostenes

Primzahlen und Restklassen ergeben sichere Verschlüsselung (https://...)

Geschichtlicher Überblick

- 4000 v.Chr. - Hieroglyphen (Entzifferung erst im 20.Jhdt)
- 500 v.Chr. - Skytale
- 100 v.Chr. - Cäsar-Verschiebung
- 1476 - Chiffrierscheibe (Alberti-Scheibe)
- 1523 - Vigenére – Verschlüsselung
- 1918 - One Time Pad
- 1918 - Entwicklung von Enigma
- 1939 - 1945: Enigma, Verschlüsselung in Navajo
- 1975 - öffentlicher Schlüssel
- 1977 - moderne Verschlüsselung (RSA)
- 1988 - Quantenkryptologie