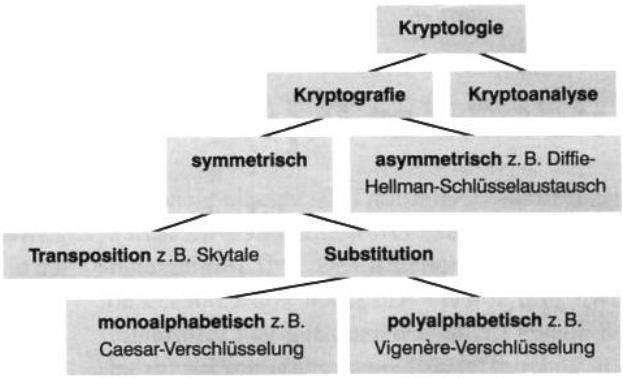
Historische Einordnung kryptographischer Verfahren

Die folgenden Texte sind aus Mathematik lehre 219 | 2020 entnommen.

❶ WISSENSWERT

Kryptografische Verfahren und Schlüsselübergabe



Kryptografische Verfahren lassen sich in symmetrische und nichtsymmetrische bzw. asymmetrische Verfahren aufteilen. Bei symmetrischen Verfahren einigen sich Sender und Empfänger einer geheimen Botschaft auf einen gemeinsamen und auszutauschenden Schlüssel. Dieser Schlüssel dient sowohl der Verschlüsselung einer unverschlüsselten Nachricht (`klartext`) als auch der Entschlüsselung des verschlüsselten Textes (`GEHEIMTEXT`). Die symmetrischen Verfahren differenziert man noch weiter in Transposition und Substitution. Während bei einer Transposition lediglich die Reihenfolge der Zeichen verändert wird (vgl. Abschnitt zu Skytale in **Kasten 2**), werden bei der Substitution Buchstaben und Zeichen durch andere ersetzt. Bei der Substitution unterscheidet man zwischen mono- und polyalphabetischen Verfahren. Monoalphabetische Verfahren verwenden nur genau ein Geheimtextalphabet, d. h. dass jedes Zeichen eines Klartextes durch genau ein anderes Zeichen des Geheimtextalphabets ersetzt wird. Polyalphabetische Verfahren verwenden mehrere Geheimtextalphabete nach festgelegten Regeln, sodass verschiedene Zeichen eines Klartextes durch denselben Buchstaben im Geheimtext abgebildet werden können (vgl. die Artikel **Unverständlich, sinnlos, zufällig?** sowie **Kryptoanalyse**). Neben den symmetrischen gibt es auch asymmetrische Verfahren, bei denen Sender und Empfänger einer Nachricht bei der Ver- und bei der Entschlüsselung unterschiedliche Schlüssel verwenden. Ein öffentlicher Schlüssel, der nicht geheim gehalten wird, dient dabei der Verschlüsselung eines `klartextes` in einen `GEHEIMTEXT`. Dieser Text kann dann nur mit dem privaten Schlüssel des Empfängers dechiffriert werden. Das Besondere ist, dass Sender und Empfänger einer geheimen Botschaft dadurch nicht mehr gezwungen sind, einen Schlüssel auszutauschen, bevor sie miteinander kommunizieren (vgl. den Artikel **Pssst ... Schlüsselvereinbarung ohne Schlüsselübergabe**). Oft wird asymmetrisch ein Schlüssel ausgetauscht, um danach (etwas weniger rechenintensiv) symmetrisch zu kommunizieren.

❷ WISSENSWERT

Verschlüsselungsverfahren in historischer Übersicht

Steganografie (5. Jhd. v. Chr)

Bereits aus dem 5. Jahrhundert v. Chr. sind Geheimschriften überliefert. Der im Exil lebende Demaratos wollte die Griechen vor der Invasion des persischen Herrschers Xerxes warnen. Damit seine Nachricht nicht als solche erkennbar war, ritze er sie auf eine Holzplatte und übergoss diese mit Wachs. So konnte die Nachricht unerkannt nach Griechenland gelangen. Teilweise wurden auch Nachrichten auf die Köpfe von Sklaven tätowiert, die anschließend Haare darüber wachsen ließen und die Nachrichten auf diese Weise unerkannt übermitteln konnten. Diese Form der Nachrichtenübermittlung, bei der verschleiert wird, dass überhaupt eine Nachricht versendet wurde, heißt Steganografie. Sie ist von der Kryptografie zu unterscheiden, bei der die Existenz einer Nachricht zwar bekannt sein mag, die Informationen jedoch durch ein Verfahren verschlüsselt wurde.

Skytale (5. Jh.) [Symmetrisch: Transposition]

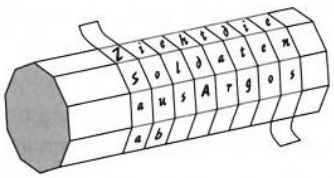


Abb. 1: Skytale mit aufgewickeltem Papierstreifen

Die Skytale-Verschlüsselung ist das älteste bekannte militärische Verschlüsselungsverfahren. Um einen Stab mit einem bestimmten Durchmesser – der sogenannte Skytale (altgriechisch für „Stock" oder „Stab") – wird ein Papierstreifen (früher Leder oder Pergament) gewickelt **(Abb. 1)**. Entlang des Stabs schreibt man nun auf den Papierstreifen die geheime Botschaft. Anschließend wickelt man den Papierstreifen wieder ab. Auf diese Weise wird z. B. aus dem Klartext `zieht die soldaten aus argos ab` der Geheimtext `ZSAA IOUB ELS HDA TAR DTG IEA ENS`. Ein Bote kann nun den Papierstreifen an den Empfänger übermitteln. Die Person, die diese Nachricht empfangen soll, kann die Botschaft genau dann entschlüsseln, wenn sie den Papierstreifen um einen Skytale des gleichen Durchmessers wickelt. Über den Durchmesser des Skytales müssen sich jedoch Sender und Empfänger zuvor geheim geeinigt haben.

Caesar-Verschlüsselung (100–44 v. Chr.) [Symmetrisch: Substitution, monoalphabetisch]

Der römische Feldherr Gaius Julius Caesar verwendete zahlreiche Geheimschriften, unter denen die nach ihm benannte Caesar-Verschlüsselung die bekannteste ist. Hierbei wird jeder Buchstabe des Alphabets durch einen anderen ersetzt. Das Geheimtextalphabet wird um eine bestimmte Anzahl an Stellen gegenüber dem Klartextalphabet verschoben. Caesar hat das Geheimtextalphabet nach Überlieferungen stets um drei Stellen nach hinten verschoben. Dadurch wird z. B. aus dem Klartext `mathematik` der Geheimtext `PDWKHPDWLN`. Um den Geheimtext zu entschlüsseln, muss der Empfänger übermittelt bekommen, um wie viel Stellen das Geheimtextalphabet (in welche Richtung) verschoben wurde. Da jeder Klartextbuchstabe genau einem Geheimtextbuchstaben zugeordnet wird, handelt es sich beim Caesar-Verfahren um ein monoalphabetisches Verschlüsselungsverfahren. Ein so verschlüsselter Text ist durch Raten und Häufigkeitsanalysen allerdings auch von Unbefugten leicht zu entschlüsseln (vgl. den Artikel **Kryptoanalyse**).

```
klartextalphabet
a b c d e f g h i j k l m n o p q r ...
↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓
D E F G H I J K L M N O P Q R S T U ...
GEHEIMTEXTALPHABET
```

Vigenère-Chiffre (16. Jh.) [Symmetrisch: Substitution, polyalphabetisch]

Die von Johannes Trithemius entwickelte und später von Blaise de Vigenère aufgegriffene Vigenère-Chiffre erweitert die Idee der Caesar-Verschlüsselung, indem nicht nur eine, sondern mehrere der 26 möglichen Verschiebungen des Alphabets verwendet werden. Über ein Schlüsselwort wird für jeden Buchstaben des Klartextes einzeln bestimmt, um wie viele Stellen das Alphabet verschoben wird. Soll der Klartext `kryptologie` mithilfe des Schlüsselwortes `MATHE` verschlüsselt werden (vgl. **Abb. 2**), wird für den ersten Buchstaben `k` des Klartextes das Alphabet entsprechend des ersten Buchstabens *M* des Schlüsselwortes verschoben – also um 12 Stellen (vgl. **Caesar – Vigenère – One-Time-Pad. Unverständlich, sinnlos, zufällig**). Dadurch entsteht der Geheimtextbuchstabe `W`. Der zweite Buchstabe wird nicht verändert, da aufgrund des Schlüsselworts um 0 Stellen verschoben wird. Im Gegensatz zur Caesar-Verschlüsselung kann so ein Geheimtextbuchstabe für mehrere Klartextbuchstaben stehen (vgl. die Verschlüsselung des zweiten und dritten Klartextbuchstabens), weshalb die Vigenère-Chiffre eine polyalphabetische Verschlüsselung ist.

SCHLÜSSEL:	*M A T H E M A T H E M*
klartext:	k r y p t o l o g i e
GEHEIMTEXT:	W R R W X A L H N M Q

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

Abb. 2: Vigenère-Quadrat

Durch die Verwendung mehrerer Geheimtextalphabete wird eine Entschlüsselung mittels Häufigkeitsanalyse erschwert. Trotzdem gelang es Charles Babbage im 19. Jahrhundert, Vigenère-verschlüsselte Texte zu knacken, indem er durch geschickte Analyse von (genügend langen) Nachrichten zunächst die Länge des Schlüsselworts ermittelte. Anschließend kann die Nachricht für jeden Buchstaben des Schlüsselworts wie ein Caesar-verschlüsselter Text entziffert werden.

Enigma (1918) [Symmetrisch: Substitution, polyalphabetisch]

Die Enigma ist eine Verschlüsselungsmaschine, die im Zweiten Weltkrieg von der deutschen Wehrmacht verwendet wurde. So wie die Vigenère-Chiffre eine Weiterentwicklung der Caesar-Verschlüsselung ist, kann die Enigma als Hintereinanderschaltung der Vigenère-Chiffre verstanden werden. Im Grundmodell der Enigma wird dies durch drei Walzen realisiert. Drückt man auf der Tastatur der Enigma einen Klartextbuchstaben, fließt Strom durch die Walzen, der auf dem Lampenfeld einen der Geheimtextbuchstaben aufleuchten lässt. Anschließend drehen sich die Walzen um eine Position weiter. Die Schemenzeichnung in **Abb. 3** zeigt beispielhaft die Verkabelung der Tastatur mit dem Lampenfeld über eine Walze, durch die der Klartextbuchstabe a mit dem Geheimtextbuchstaben E verschlüsselt wird. Durch die geheime mechanische Anordnung der Walzen entsteht eine äußerst komplexe, polyalphabetische Verschlüsselung. Auch bei diesem Verschlüsselungsverfahren mussten umfangreiche Schlüssel zur Einstellung der Walzen ausgetauscht werden. Unter großen Anstrengungen gelang es maßgeblich dem britischen Mathematiker Alan Turing im Forschungszentrum Bletchley Park, die Chiffrierung der Enigma zu knacken, sodass die britischen Alliierten nahezu sämtliche Funksprüche der Wehrmacht nicht nur abfangen, sondern auch entziffern konnten.

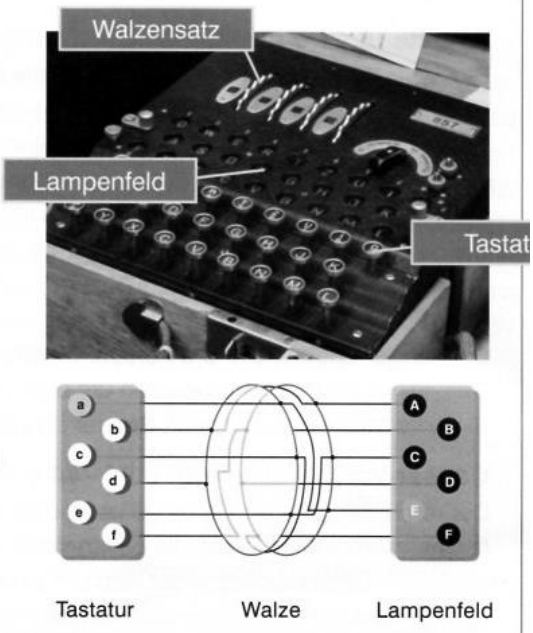


Abb. 3: Beschriftete Enigma-Verschlüsselungsmaschine sowie Schemenzeichnung der Walzenverkabelung

RSA-Verfahren (1977) [Asymmetrisch]

Auf der Grundlage des Diffie-Hellman-Schlüsselaustauschs (vgl. den Artikel **Pssst ...**) entwickelten Ronald L. Rivest, Adi Shamir und Leonard Adleman 1977 das nach ihren Initialen benannte RSA-Verfahren. Es basiert auf einem öffentlichen und einem privaten Schlüssel. Um die Grundidee des Verfahrens zu verstehen, kann man sich vorstellen, dass der Empfänger einer Nachricht einen Briefkasten besitzt, zu dem nur er selbst Zugang hat. Möchte der Sender eine Nachricht schicken, wirft er diese in den Briefkasten des Empfängers. Der Briefkasten dient somit als öffentlicher Schlüssel. Der Empfänger kann nun den Briefkasten mit seinem privaten Schlüssel öffnen. Auf diese Weise haben Sender und Empfänger eine geheime Nachricht ausgetauscht, ohne dass dazu ein Schlüsselaustausch notwendig war – es handelt sich also um ein asymmetrisches Verfahren. Vor Entwicklung des RSA-Verfahrens gab es ausschließlich symmetrische Verfahren, bei denen Sender und Empfänger vor dem Austausch von Nachrichten den Schlüssel austauschen mussten, was stets eine Schwachstelle des jeweiligen Systems darstellte.

Zero-Knowledge-Beweis (1989)

Bei Zero-Knowledge-Beweisen kommunizieren eine beweisende und eine verifizierende Person miteinander. Die beweisende Person überzeugt die verifizierende mit einer hohen Wahrscheinlichkeit davon, dass sie über ein geheimes Wissen verfügt, ohne dieses Wissen dabei preiszugeben. Das Prinzip soll wie folgt verdeutlicht werden*: Eine farbenblinde Person besitzt zwei Bälle, die sich bis auf ihre Farbe gleichen. Eine Person, die Farben sehen kann, möchte die farbenblinde Person nun davon überzeugen, dass sich diese Bälle voneinander unterscheiden, ohne etwas über deren Farben preiszugeben. Dafür könnte die farbenblinde Person beide Bälle hinter den Rücken nehmen und dann einen Ball zeigen. Anschließend nimmt sie diesen Ball wieder hinter den Rücken und zeigt erneut einen der beiden Bälle. Die sehende Person soll jeweils sagen, ob die farbenblinde Person den Ball hinter dem Rücken gewechselt hat. Wären beide Bälle identisch, könnte die sehende Person nur mit einer Wahrscheinlichkeit von 50 % die korrekte Antwort geben. Da sie die Bälle jedoch anhand ihrer Farben unterscheiden kann, genügen bereits 20 Wiederholungen dieses Tests, damit die farbenblinde Person der sehenden Person mit einer Wahrscheinlichkeit von etwa 1 zu 1 Million vertrauen kann, dass sie die Bälle voneinander unterscheiden kann.

Blockchain (1991)

Die in den 1990er-Jahren entwickelte Idee der Blockchain wurde maßgeblich durch ihre Implementation in der digitalen Währung Bitcoin bekannt. Die Blockchain-Technologie besteht im Kern aus der Codierung von Transaktionen durch sog. Hashs. Verschiedene Teilnehmende eines Netzwerks versuchen bei einer Transaktion, einen Konsens über diesen Hash zu finden. Erst wenn dieser Konsens besteht, wird die Transaktion in Form eines Blocks in die globale Kette aus Blöcken, die sogenannte Blockchain, aufgenommen (vgl. den Artikel **Blockchains und Hashfunktionen**).