

Geschichte

der

Kryptographie

Roger Schumacher
Ziegelweg 32
5200 Brugg

Inhaltsverzeichnis

1. Kryptographie	2
1.1 Begriffe der Kryptologie	2
2. Geschichte der Kryptographie	2
2.1 Kryptographie in vorchristlicher Zeit	2
2.2 Entstehung der Kryptoanalyse	3
2.2.1 Polyalphabetische Verschlüsselung	4
2.2.2 Die Vigenère Verschlüsselung	4
2.3 Kryptographie im 19. und 20. Jahrhundert	5
2.4 Erster Weltkrieg	6
2.5 Kryptographische Organisationen	8
2.6 Automatische Chiffrier-Geräte	8
2.6.1 Zylinder-Chiffriergeräte	8
2.6.2 Die Rotormaschine	10
2.6.3 Enigma	11
3. Revolution der Kryptographie	15
3.1 Data Encrypten Standart (DES)	15
3.1.1 Funktionsweise des DES	15
3.2 Public-Key-Verfahren	16
3.3 Aktuell/Zukunft der Kryptographie	17
4. Literaturverzeichnis	18

1. Kryptographie

Der Begriff der Kryptographie ist aus dem Bereich der Kryptologie. Die Kryptologie befasst sich mit dem ver- und entschlüsseln von Nachrichten. Der Begriff stammt aus dem griechischen und bedeutet; kryptos (geheim) und logos (das Wort, der Sinn). Die Kryptologie wird unterteilt in die Kryptoanalyse und die Kryptographie(griech. graphein = schreiben).

Die Kryptographie beschäftigt sich mit der Verheimlichung von Nachrichten, während sich die Kryptoanalyse mit dem Entschlüsseln von geheimen Nachrichten beschäftigt.

1.1 *Begriffe der Kryptologie*

Klartext: Der Klartext ist die Information die der Empfänger erhalten soll.

Geheimtext: Der Geheimtext ist der verschlüsselte Klartext. Dieser Text ist für andere nicht lesbar.

Verschlüsselung: Der Vorgang der Verschlüsselung bezeichnet man als Chiffrierung.

Entschlüsselung: Der Vorgang der Entschlüsselung bezeichnet man als Dechiffrierung.

Schlüssel: Als Schlüssel bezeichnet man geheime Informationen die dazu dienen einen Klartext zu chiffrieren oder einen Geheimtext zu dechiffrieren.

Symmetrisches Verfahren: Von einem symmetrischen Verfahren spricht man, wenn man für die Chiffrierung und die Dechiffrierung den selben Schlüssel verwendet.

Asymmetrisches Verfahren: Von einem asymmetrischen Verfahren spricht man, wenn man für die Chiffrierung und die Dechiffrierung zwei oder mehr Schlüssel verwendet.

Angreifer: Der Angreifer ist ein unbefugter Dritter, welcher sich den Schlüssel oder den Klartext beschaffen will.

2. Geschichte der Kryptographie

2.1 *Kryptographie in vorchristlicher Zeit*

Die ersten Ansätze von Geheimbotschaften sind aus den Hochkulturen von Ägypten, Indien und Mesopotanien bekannt. Eine Variante war, dass man den Sklaven die Schädel kahl rasierte, ihnen die Geheimbotschaft auf den Kopf tätowierte und, nachdem das Haar nachgewachsen war, zum Empfänger schickte. Eine weitere Variante war, dass man Nachrichten in Holzplatten schrieb und anschliessend die Holzplatten mit Wachs überzog.

Diese Art der Nachrichtenversendung arbeitete noch ohne Verschlüsselung der Daten. Die Daten wurden einfach „nicht erkennbar“ verschickt.

Veränderungen von Texten fand man aber bereits in alt-testamentarischen Schriften. In den Büchern Jeremias wurde das Wort „Babel“ an mehreren Stellen durch den Ausdruck „Sheshech“ ersetzt, welcher sich auch einer speziellen Substitution namens „Atbash“ ergibt. Im Atbash werden der erste und der letzte Buchstabe des Alphabets, usw. vertauscht.

Aus der Zeit um 475 v. Chr. ist das erste militärisch genutzte System bekannt. Dabei wurden die Nachrichten auf einen Papyrusstreifen geschrieben, welcher um einen Holzstab mit einem bestimmten Durchmesser gewickelt wurde. Diese Nachricht bestand anschließend aus einer Reihe von Buchstaben, welche erst einen Sinn ergaben, wenn der Empfänger den Papyrusstreifen um einen Holzstab mit demselben Durchmesser aufwickelte.

Julius Cäsar benutzte während seiner Regentschaft ein einfaches Substitutionsverfahren. In diesem Verfahren wurden die Buchstaben des Alphabets um eine bestimmte Anzahl verschoben.

Klartext: A B C D E ...
Schlüssel: 4
Chiffre: E F G H I ...

Diese Art der Chiffrierung ist sehr einfach zu entschlüsseln. Sie wird erst schwieriger, wenn man jede Permutation des Alphabets für die Geheimschrift zulässt. Aber auch diese kann man, wenn man die Häufigkeit berechnet, entschlüsseln.

2.2 Entstehung der Kryptoanalyse

Abu 'Abd al-Rahman al-Khalil ibn Ahmad ibn 'Amir ibn Tamman al Farahidi al-Zadi al Yahmadi gilt als Autor des ersten Werkes über die Kryptoanalyse. Er dechiffrierte Texte für den byzantinischen König. Dabei diente ihm als Basis der richtig geratene Beginn des Klartextes.

Die Buchstaben des Alphabets werden in unserer natürlichen Sprache in verschieden grosser Häufigkeit verwendet. Der Buchstabe e kommt mit 14,3 Prozent am Häufigsten vor, dagegen werden die Buchstaben y, q und x so gut wie nie verwendet. Aufgrund dieser

Häufigkeit verfasste der Gelehrte Al-Kindi im 9. Jahrhundert sein Werk „Abhandlung über die Entzifferung kryptographischer Botschaften“. Diese Dechiffrierung kann aber nur bei der Entschlüsselung von monoalphabetischen Texten angewendet werden.

2.2.1 Polyalphabetische Verschlüsselung

Durch die polyalphabetische Verschlüsselung wurde es erstmals möglich, für dasselbe Zeichen im Klartext verschiedene Chiffre zu verwenden. Leon Battista Alberti stellte in seinem Buch „Modus Scribendi in Zifferas“ eine Methode vor, in welcher zwei konzentrische Scheiben verwendet wurden, auf welchen das Alphabet eingraviert ist. Durch dies erhielt man bei jeder Einstellung der Scheiben 26 verschiedene Verschlüsselungen.

2.2.2 Die Vigenère Verschlüsselung

Als berühmtester Kryptologe des 16. Jh. gilt Blaise de Vigenère. Er arbeitet vor allem im Bereich der polyalphabetischen Verschlüsselung. Während seiner Arbeit verfasste er das Werk „Traicté des chiffres“ und entwickelt die Vigenère Verschlüsselung, welche auf der Vigenère Tabelle und dem Vigenère Algorithmus beruht.

Vigenère Tabelle

	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

2.3 Kryptographie im 19. und 20. Jahrhundert

Die Frage nach der Sicherheit beim Übermitteln von Nachrichten nahm im 19. Jh. durch die Einführung des Telegraphen stark zu. Dabei waren es vor allem die Industrie und die Wirtschaft, welche nach Möglichkeiten verlangten Nachrichten zu chiffrieren. Dabei wurde auf altbewährte Methoden, wie etwa die Vigenère Verschlüsselung, zurückgegriffen.

Daneben wurden aber auch neue Methoden eingesetzt, wie etwa der „Playfair Cipher“. Bei diesem Verfahren wird eine 5 x 5 Matrix verwendet, welche mit den Buchstaben des Alphabets ausgefüllt wird (I/J zusammen).

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

Bevor man jedoch die Matrix ausfüllt wird ein Schlüsselwort (RUP) eingetragen. Anschließend füllt man die leerstehenden Felder mit dem Alphabet aus. Nun kann man mit dem Verschlüsseln des Klartextes beginnen.

- Man betrachtet immer zwei Buchstaben des Klartextes.
 - Klartext: **MEINKLEINERHUNDLAUSTSICH**
- Das Buchstabenpaar befindet sich in verschiedenen Zeilen und Spalten:
 - Zeilenindizes bleiben gleich, Spaltenindizes werden vertauscht:

M(Z3,S5) E(Z2,S3) wird **K(Z3,S5) G(Z2,S5)**

Schlüsselwort: RUP					
R	U	P	A	B	Z1
C	D	E	F	G	Z2
H	I/J	K	L	M	Z3
N	O	Q	S	T	Z4
V	W	X	Y	Z	Z5
S1	S2	S3	S4	S5	

3. Das Buchstabenpaar befindet sich in der selben Zeile:
 - Die Spaltenindizes werden um eins erhöht.

KL wird **QS**

4. Das Buchstabenpaar befindet sich in der selben Spalte:
 - Die Zeilenindizes werden um eins erhöht.

Schlüsselwort: RUP					
R	U	P	A	B	Z1
	D	E	F	G	Z2
H	I/J	K	L	M	Z3
N	O	Q	S	T	Z4
V	W	X	Y	Z	Z5
S1	S2	S3	S4	S5	

Schlüsselwort: RUP					
R	U	P	A	B	Z1
	D	E	F	G	Z2
H	I/J	K	L	M	Z3
N	O	Q	S	T	Z4
V	W	X	Y	Z	Z5
S1	S2	S3	S4	S5	

LA wird **SF**

Bei diesen Verschlüsselungen gelang es immer wieder die Schlüsselwörter herauszufinden. So wurden während dem amerikanischen Bürgerkrieg oft die Worte „Manchester Bluff“, „Come Retribution“ und „Complete Victory“ als Schlüssel verwendet, welche von

Kryptoanalytikern entdeckt und zu ihrem Vorteil genutzt wurden.

Nach den immer wieder auftauchenden Entschlüsselungen verfasste Auguste Kerckhoff 1883 sein Buch „La Cryptographie Militaire“ in welchem er sechs grundlegende Forderungen an ein Kryptosystem stellte:

1. Kryptotext sollte nicht dechiffrierbar sein
2. Das Kryptosystem sollte einfach anzuwenden sein
3. Der Schlüssel sollte einfach und austauschbar sein
4. Der Kryptotext sollte durch den Telegraphen versendbar sein
5. Das Verschlüsselungsmaterial sollte transportierbar sein
6. Die Chiffriermaschine sollte einfach zu gebrauchen sein

2.4 Erster Weltkrieg

Während dem Ersten Weltkrieg spielte die Kryptographie eine wichtige Rolle. Denn wer die Angriffsziele und die Angriffsdaten des Gegners kannte hatte einen schlagentscheidenden Vorteil.

Zu Beginn des Ersten Weltkrieges existierten in England noch keine kryptoanalytischen Einrichtungen. Der Engländer Alfred Ewing gründete das erste kryptologische Büro, welches später unter dem Namen „Room 40“ bekannt wurde. Während dem Krieg arbeiteten bis zu

800 Funker und 80 Kryptoanalytiker (Diese Gruppe setzte sich aus Sprachwissenschaftlern, Altphilologen und Leuten mit einer natürlichen Begabung für Kreuzwort-/Texträtseln zusammen) in dieser Abteilung. Sie entschlüsselten während dem Krieg rund 15'000 Funksprüche. Ihr grösster Erfolg war die Entschlüsselung des Zimmermann-Telegrams. Die Inhalte dieses Telegramms trugen massgeblich dazu bei, dass die USA in den Krieg eintraten.

Das Zimmermann-Telegramm war ein verschlüsseltes Telegramm, das Arthur Zimmermann, der deutsche Staatssekretär des Auswärtigen, am 19. Januar 1917 über die deutsche Botschaft in Washington, D.C. an den deutschen Gesandten in Mexiko sandte

*„Wir beabsichtigen, am ersten Februar uneingeschränkten U-Boot-Krieg zu beginnen. Es wird versucht werden, Amerika trotzdem neutral zu halten. Für den Fall, dass dies nicht gelingen sollte, schlagen wir Mexiko auf folgender Grundlage Bündnis vor. Gemeinsame Kriegführung. Gemeinsamer Friedensschluss. Reichlich finanzielle Unterstützung und Einverständnis unsererseits, dass Mexiko in Texas, Neu Mexico, Arizona früher verlorenes Gebiet zurückerobert. Regelung im einzelnen Euer Hochwohlgeborenen überlassen. Euer Hochwohlgeborenen wollen Vorstehendes Präsidenten streng geheim eröffnen, sobald Kriegsausbruch mit Vereinigten Staaten feststeht, und Anregung hinzufügen, Japan von sich aus zu sofortigem Beitritt einzuladen und gleichzeitig zwischen uns und Japan zu vermitteln. Bitte Präsidenten darauf hinweisen, dass rücksichtslose Anwendung unserer U-Boote jetzt Aussicht bietet, England in wenigen Monaten zum Frieden zu zwingen. Empfang bestätigen.
Zimmermann“*

Dieses Telegramm konnte vom „Room 40“ entschlüsselt werden, da der deutsche Nachrichtendienst bei der Verschlüsselung ihrer Nachrichten so genannte Code-Bücher verwendete. In diesen Büchern wurden den Begriffen/Buchstabenkombinationen fünfstelligen Zahlen zugeordnet (Diese Bücher waren also nichts anderes als grosse Wörterbücher).

Der deutsche Nachrichtendienst verwendete parallel zu den Codebüchern noch eine zusätzliche Verschlüsselung. Zu Beginn des Krieges verschlüsselten sie zusätzlich durch die doppelte Spaltentransposition. Wechselten dann aber ab dem November 1914 auf die Vigenère-Verschlüsselung.

Dem „Room 40“ gelang es Ende 1914 an zwei Codebücher der deutschen Marine zu gelangen, welche vom gesunkenen deutschen Kreuzer *Magdeburg* geborgen werden konnten. Danach mussten sie sich nur noch mit dem Vigenère-Code auseinandersetzen, welcher geknackt werden konnte.

2.5 Kryptographische Organisationen

Nachdem man während dem Ersten Weltkrieg damit begonnen hatte kryptographische Organisationen zu gründen wurden diese Bemühungen nach dem Ende des Krieges weitergeführt, da man die Wichtigkeit (neben den ethischen Bedenken) der Kryptologie als Kriegsentscheidender Faktor erkannt hatte.

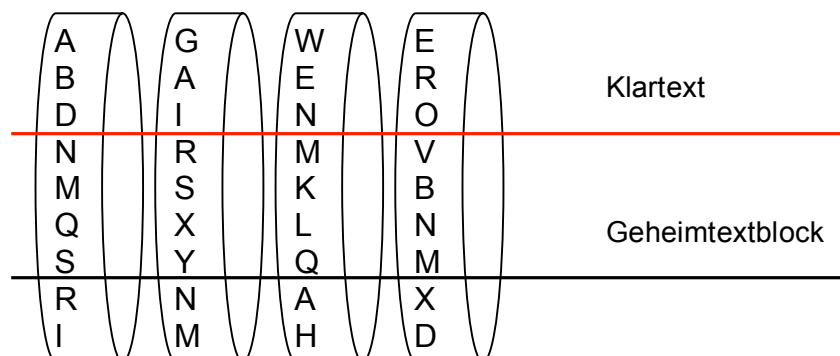
Durch die Forschungsarbeiten der kryptographischen Organisationen gelang es die Schlüssellänge von Vigenère Chiffrierungen zu ermitteln. Ihnen gelang dies, indem sie den Text gegen sich selbst verschoben und dabei beachtet, wann die selben Buchstaben wieder auftauchten. Wenn bei dieser Berechnung Werte erreicht wurden, welche $> 1/26$ waren, war dies ein Indiz, dass die Verschiebung der Schlüssellänge entsprach.

Da der Verschlüsselungsprozess sehr zeitintensiv war, versuchte man diesen zu automatisieren. Durch diese Automatisierung konnten die Qualität der Verschlüsselungen stark verbessert werden und die Effizienz und Verlässlichkeit nahm stark zu.

2.6 Automatische Chiffrier-Geräte

2.6.1 Zylinder-Chiffriergeräte

Der Chiffrierzylinder besteht aus verschiedenen Scheiben, auf welchen aussen je ein permutiertes Alphabet eingestanzt ist. Dabei spielt die Reihenfolge Buchstaben keine Rolle. Diese Scheiben, welche sich unabhängig von einander bewegen lassen, werden anschliessend zu einem Zylinder zusammengebaut. Verschlüsselt wird, indem man den Klartext in einer Zeile des Zylinders einstellt und den Geheimtextblock in einer anderen Zeile abliest.



Die Zylinderchiffrierung weist verschiedene Vor- und Nachteile auf:

Vorteile

- grosser Schlüsselraum
- handlich und leicht zu bedienen
- nicht fehleranfällig
- unabhängige Alphabete

Nachteile

- Alphabete müssen geheim gehalten werden
- Verwendung verschiedener Matrizen ist begrenzt und aufwändig
- Mustersuche möglich

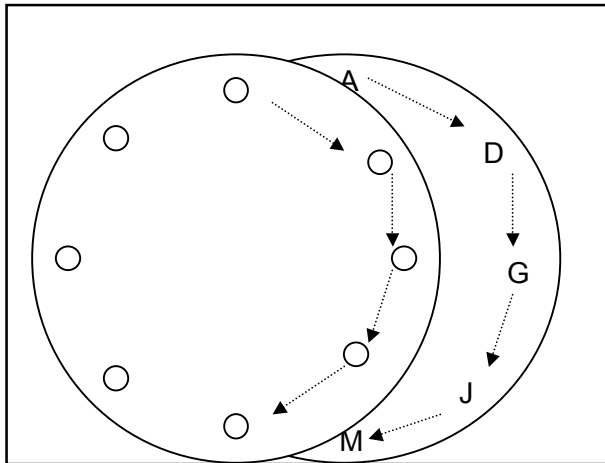
Herstellung/Verwendung

Die ersten Chiffrierzylinder wurden bereits Ende des 18. Jh. hergestellt. Frederik Gribenstierna entwickelte 1786 ein Chiffriergerät mit 57 Scheiben. Dieses Gerät entsprach aber noch nicht dem bekannte Zylinder-Chiffriergerät, da die Scheiben fest waren und es keine Einstellungsmöglichkeiten gab. Die nächste Generation von Zylinder-Chiffriergeräten entwickelte Thomas Jefferson 1795. Er entwarf ein Gerät mit 36 Scheiben, welches aber nie zum Einsatz kam.

Die Zylinder-Chiffriergeräte kamen erst zu Beginn des 20. Jh. zur Anwendung. So verwendete die US Army zwischen 1922 bis 1943 ein Chiffriergerät (M-94), welches auf dem Chiffrierzylinder beruhte. Die Japaner hatten ein ähnliches Chiffriergerät, das CSP-642. Das M-94 bestand aus 25 Aluminiumzylindern. Dabei gab es verschiedene Geräte mit einer verschiedenen Anordnung der Scheiben (Anordnung geheim).

2.6.2 Die Rotormaschine

Der Nachfolger der Chiffrierzylinder waren die Rotormaschinen. Diese wurden in den 20er Jahren des 20. Jh. entwickelt. Die ersten Patente für Rotorchiffriermaschinen wurden von vier unabhängigen Erfindern zwischen 1917 – 1919 angemeldet. Die ersten Rotormaschinen wurden jedoch bereits 1915 von der niederländischen Marine verwendet, welche aber die



Entwicklung und Fertigung geheim hielt, da sie die Chiffriermaschinen während dem Ersten Weltkrieg einsetzten.

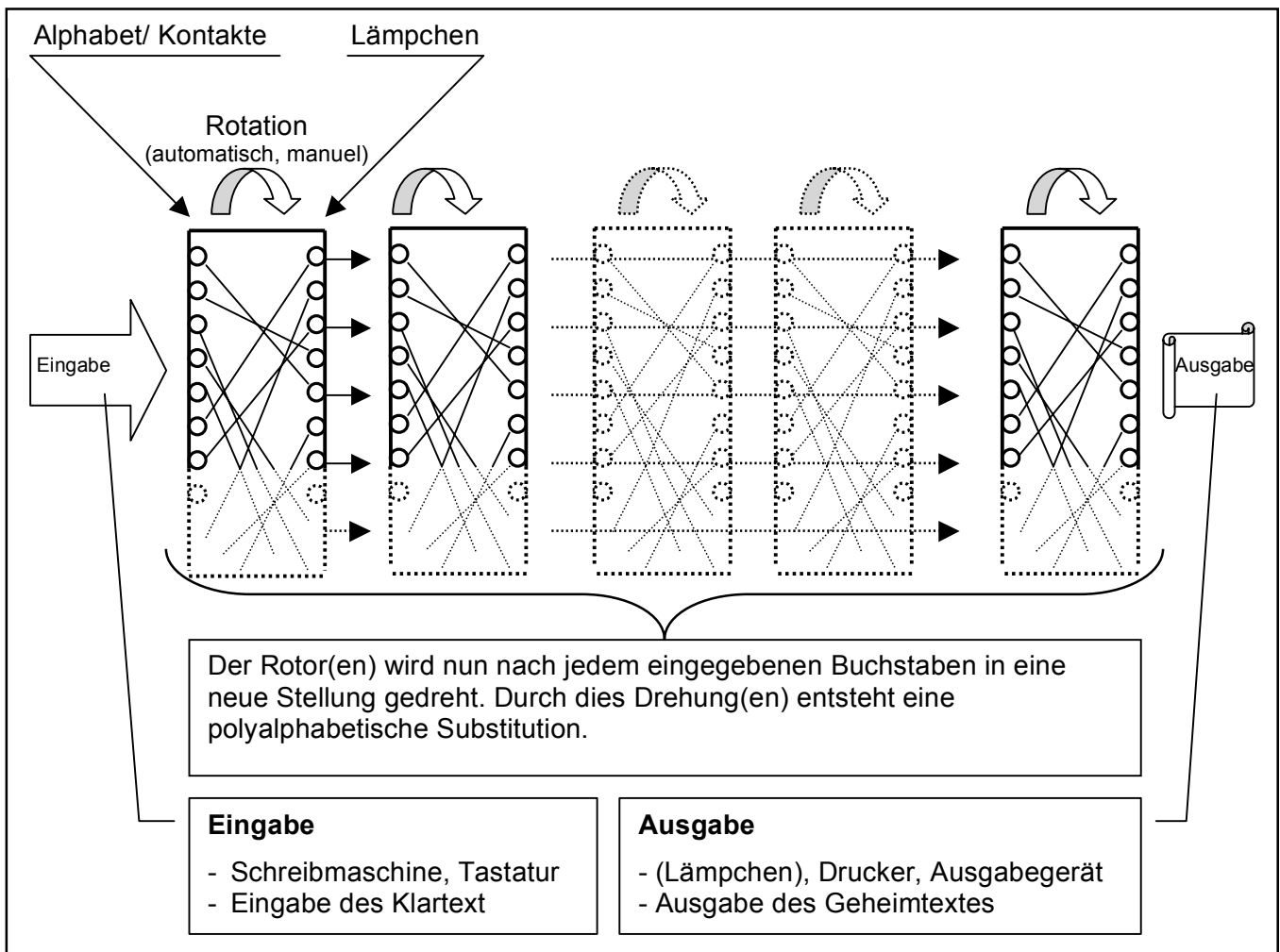
Die Weiterentwicklung und Massenherstellung der Rotorchiffriermaschinen wurde in der Zwischenkriegszeit der beiden Weltkriege stark vorangetrieben (Gründung der „Chiffriermaschinen AG, Scherbius, Enigma

A, B“). Die deutsche Wehrmacht verwendet ab 1926 Rotormaschinen mit 4 Rotoren (Enigma, Modell A) zur Verschlüsselung ihrer Nachrichten und Funkprüchen. Weiterentwicklungen der Enigma wurden von der deutschen Wehrmacht bis zum Ende des Zweiten Weltkrieges verwendet und galten lange Zeit als absolut sicher. Es gelang jedoch den Alliierten gegen Ende des Zweiten Weltkrieges die Nachrichten der Enigma zu entschlüsseln und sich so entscheidend in den Kriegsverlauf einzugreifen.

Funktionsweise der Rotormaschine

Wie es der Name schon sagt besteht die Rotormaschine aus verschiedenen Rotoren. Diese Rotoren sind dicke, elektronisch isolierte Scheiben, auf welchen Schleifkontakte angebracht sind. Das Prinzip der Verschlüsselung arbeitet mit einer mehrfachen Substitution. Auf den gegenüberliegenden Scheiben sind je 26 Schleifkontakte angebracht. Jeder dieser Kontakte entspricht einem Buchstaben des Alphabets. Diese Kontakte sind nun untereinander (ein Kontakt rechts mit einem Kontakt links) unabhängig verbunden. Durch diese unregelmässigen Verbindungen erhält man eine einfache Substitution. Um die Kryptoanalyse zu erschweren kann man, statt nur einer Scheibe, mehrere Scheiben hintereinander schalten.

Rotormaschine



2.6.3 Enigma

Die Enigma ist, wie oben genannt, eine Rotorchiffriermaschine. Sie wurde vom deutschen Elektroingenieur Arthur Scherbius in den 10er Jahren des 20. Jahrhunderts entwickelt und am 23.02.1918 zum Patent angemeldet. Arthur Scherbius gründete 1923 die „Chiffriermaschinen AG (bis 1933)“, welche die Enigma als ziviles, kommerzielles Chiffriersystem (Enigma A – D) vertrieb. Gegen Ende der 20er Jahre zeigten auch verstärkt militärische Stellen Interesse an der Enigma. Nach dem Tod von Arthur Scherbius wurde die Chiffriermaschinen AG 1933 aufgelöst. Die Weiterentwicklung und den Vertrieb übernahm anschliessend die neu gegründete „Chiffriermaschinen-Gesellschaft Heimsoeth und Rinke (bis 1945)“. Dabei wurde die Strategie geändert und man entwickelte die Enigma weiter zum reinen Militärchiffriergerät (Enigma I, Wehrmacht enigma). In der Zwischenkriegszeit und während dem Zweiten Weltkrieg verwendete die deutsche Wehrmacht (und die Schweizer Armee, Enigma K) diese Geräte zur Verschlüsselung ihrer Nachrichten.

Die Hersteller der Enigma waren der Überzeugung, dass eine maschinelle Verschlüsselung nicht manuell entschlüsselt werden könne. Diese Annahme bewahrheitete sich auch. Aber sie berücksichtigten nicht, dass im Gegenzug zur maschinellen Verschlüsselung auch Entschlüsselungsmaschinen entwickelt werden konnten.

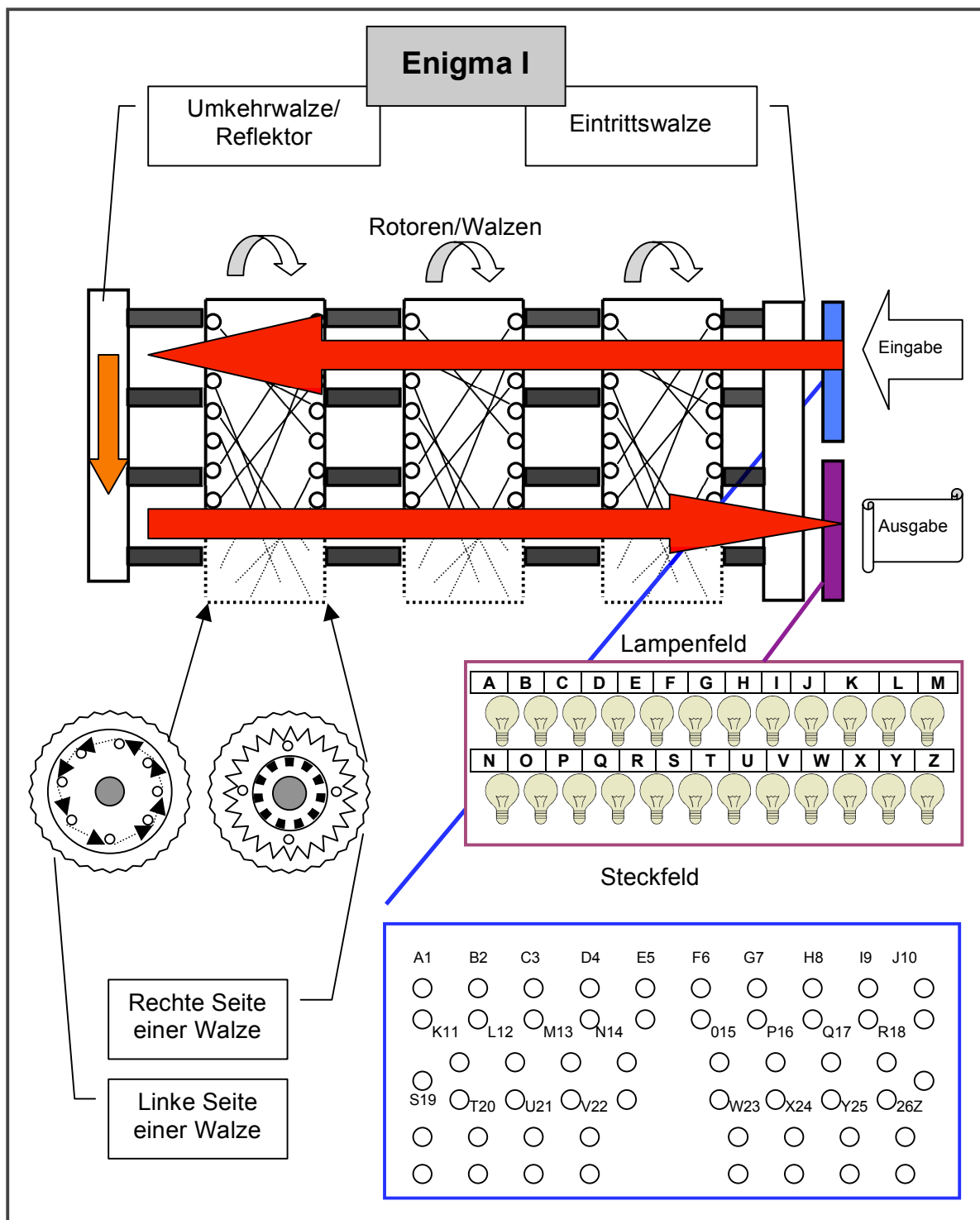
Enigma I, Wehrmachtsenigma

Die Enigma I war eine Weiterentwicklung der älteren Enigma Modelle. Diese Enigma wurde zuerst von der Reichswehr und später von der Wehrmacht eingesetzt. Während dem Zweiten Weltkrieg war die Enigma I das meistgebrauchte Verschlüsselungsgerät.

Die Enigma I sah auf den ersten Blick wie eine gewöhnliche Schreibmaschine aus. Sie bestand aus einer Tastatur, einem Walzensatz von drei austauschbaren Walzen sowie einem Lampenfeld zur Anzeige. Die Walzen besaßen auf beiden Seiten 26 elektrische Kontakte die durch Drähte im Innern, paarweise, frei miteinander verbunden waren.

Der Text wurde durch die Tastatur eingegeben und lief durch die Eintrittswalze (erste Verschlüsselung, keine drehbare Walze) auf die drei rotierenden Walzen und dann auf die Umkehrwalze. Die Umkehrwalze besaß nur auf der rechten Seite Kontakte. Der Strom wurde durch die Umkehrwalze wieder auf die drei Rotoren geleitet und erst dann leuchtete die Lampe des betreffenden Buchstaben auf. Die Umkehrwalze war ein Element, das zum ersten Mal in einer Chiffriermaschine verwendet wurde. Durch sie wurde verhindert, dass ein Buchstabe am Ende wieder auf sich selbst abgebildet werden konnte.

Die Enigma I bestand bis 1939 aus einem Rotorenfeld mit drei Rotoren und wurde später um zwei weitere Rotoren ergänzt. Diese fünf Rotoren waren mit römischen Ziffern gekennzeichnet (I – V). Es wurden bei der Chiffrierung immer nur drei Rotoren verwendet, welche nach einem Codebuch ausgewählt wurden. Speziell bei der Enigma I war, dass sie neben den Walzen noch zusätzlich ein Steckfeld besaß, welches als zusätzliches Sicherheitselement arbeitete. Auf dem Steckfeld konnten zwei Buchstaben miteinander verbunden werden. Wenn man nun den Klartext durch die Enigma schickte, wurden die nicht miteinander verbundenen Buchstaben ganz normal durch das Rotorenfeld verändert. Die Buchstaben, welche jedoch miteinander verbunden waren, wurden zuerst durch die Bedeutung des anderen Buchstabens ersetzt und erst dann durch das Rotorenfeld verändert (M <-> K, dann M = K).



Schwächen der Enigma

Die Enigma galt als sehr sichere Chiffriermaschine, wies jedoch ein paar markante Schwächen auf:

Umkehrwalze: Durch die Umkehrwalze erhofften sich die Ingenieure eine zusätzliche Verbesserung, da ja kein Buchstabe wieder auf sich selbst abgebildet werden konnte und der Strom die Chiffrierung ein zweites Mal durchlief -> fixpunktfreien Permutation. Durch dieses Verfahren wurde jedoch die Verschlüsselungsmöglichkeiten um eins auf 25 reduziert. Diese Einschränkung mag als unwesentliche Kleinigkeit angesehen werden, bot jedoch wieder eine neue Angreifbarkeit des Geheimtextes (Diese Einschränkung hat viel grössere Einflüsse als man glauben möchte. Sie reduziert die Möglichkeiten um den Faktor von $5 * 10^{13}$ Möglichkeiten).

Verwendungszweck: Da die Enigma A – G noch als ziviles, kommerzielles Chiffriergerät verkauft wurde, konnten sich Dechiffrierspezialisten wichtige Kenntnisse zur Funktionsweise der Enigma I durch die älteren Modelle erarbeiten. Der polnischen Mathematiker Marian Rejewski befasste sich bei der Entschlüsselung der Enigma I mit den älteren Modellen der Enigma, bei welchen ihm bereits 1932 ein wichtiger „Einbruch“ in das System gelang. Er entschlüsselte die, von der deutschen Wehrmacht gewählte, Verdrahtungsreihenfolge der Walzen (bei den älteren Modellen war die Tastatur noch „gewöhnlich“ mit der Eintrittswalze verbunden -> normale Tastaturreihenfolge, QWERTZ...). Durch diese sehr guten Kenntnisse über die Permutationstheorie der Enigma gelang es ihm die Verdrahtung des Rotorenfeldes (inkl. der Umkehrwalze) der Enigma I zu erschliessen (Marian Rejewski galt nach diesem Coup als einer der grössten Kryptoanalytiker aller Zeiten).

Walzenlage (Übertragung): Die Walzenlage der Enigma wurde vor dem Senden einer Nachricht jeweils verändert. Damit nun der Empfänger seine Enigma dementsprechend einstellen konnte, wurde jeder Nachricht die Walzenlage (doppelt) vorangestellt. Dies nutzte nun Rejewski wieder und entwickelte zwei Maschinen (Zyklometer und Bomba) um die Rotorenstellung zu entschlüsseln. Dies gelang ihm bis Ende 1938, danach stellten die Deutschen die Verfahrenstechnik um und integrierten fünf, statt nur drei, Rotoren in die Enigma (Erhöhung der Walzenlage von 6 auf 60ig).

Dechiffriermaschinen: Wie bereits erwähnt gab es neben der Entwicklung der Chiffriermaschinen auch einen technischen Fortschritt bei den Dechiffriermaschinen. So entwickelten die Engländer, auf der Basis der polnischen Bomba, eine Dechiffriermaschine (Turing-Bombe), welche pro Umdrehung 26 mögliche Verschlüsselungen der Enigma I entschlüsselte (bei 120 Umdrehungen pro Minute). Wenn man nun mehrer Turing-Bomben miteinander einsetzte, konnte man die ~ 1 Mio. Möglichkeiten der Enigma I in ein paar Minuten entschlüsseln.

3. Revolution der Kryptographie

In der Geschichte der Kryptographie ist, über die Jahrhunderte hinweg, eines immer gleich geblieben. Wollte man eine geheime Nachricht von einem Sender an einen Empfänger schicken, musste man vorher, auf einem sicheren Weg, der Geheimschlüssel der Nachricht ausgetauscht werden. Dies galt auch immer noch Mitte des 20. Jahrhunderts.

Als Vater der modernen Kryptographie gilt der amerikanische Mathematiker Claude Elwood Shannon. Er veröffentlichte 1949 den Artikel „Communication Theory of Secrecy Systems“. In diesem Artikel klärte Shannon die Grundlagen der Kryptographie und erhob die Kryptographie zu einer eigenständigen Wissenschaft. In diesem und weiteren Artikeln (über Informations- und Kommunikationstheorie) zeigte er die starke mathematische Basis der Kryptographie auf.

Nach dem Zweiten Weltkrieg, in welchem noch Maschinen mit Walzen und Steckkontakten verwendet wurden, begann die Ära der elektronischen Rechenmaschinen. Diese Geräte arbeiteten mit mathematischen Algorithmen und Programmen, die eine wesentlich höhere Sicherheit boten. Die ersten „neuen“ Verschlüsselungsmethoden arbeiteten noch mit einem Schlüssel, welcher aber kurz darauf nicht mehr gebraucht wurde.

3.1 Data Encrypten Standart (DES)

Zu Beginn der 70iger Jahre war die NSA (National Security Agency) auf der Suche nach einem neuen Chiffriersystem. Dieses System sollte nur von der Geheimhaltung des Schlüssels abhängig sein, nicht aber von der Geheimhaltung des Algorithmus.

Nachdem zu Beginn kein neues System gefunden wurde, unterbreitetet IBM der NSA Mitte der 70er Jahre einen valablen Vorschlag. Daraufhin entwickelte IBM, in Zusammenarbeit mit der NSA, den DES. Dieser wurde 1976 zum US-Standard.

3.1.1 Funktionsweise des DES

Es handelt sich beim DES um eine Blockchiffre, welche auf Blöcken mit 64 Bit arbeitet.

Funktionsweise:

1. Um die Reihenfolge der Bits zu verändern wird der Eingabeblock und der 64 Bit Schlüssel einer Eingangspermutation unterworfen. Dabei ergeben sich beim Eingabeblock als Ergebnis zwei 32-Bit-Register. Beim 64 Bit Schlüssel erhält man, nachdem die für die Verschlüsselung relevanten 56 Bits bestimmt wurden, zwei 28-Bit-Register.

2. Die Daten werden anschliessend in 16 Iterationen (Substitution und Transposition) verwürfelt.

- Zunächst werden die Bits der "Schlüsselregister" zyklisch um ein bzw. zwei Bit verschoben und 48 der 56 Bit als Rundenschlüssel bestimmt.
- Das rechte Datenregister (R-Block) wird mittels einer Expansion von 32 auf 48 Bit vergrößert. -Daten- und Schlüsselblock werden durch logisches XOR miteinander kombiniert.
- Das Resultat wird in 6 Bit große Abschnitte aufgeteilt und durch acht S-Boxen (Substitutionsboxen) gesandt, die hieraus wiederum 32 neue Bits erzeugen.
- Zum Schluss wird der Block nochmals einer Ausgangspermutation unterzogen.

3. Nachdem die 16 Runden abgeschlossen sind, werden die Register wieder zu einem 64-Bit Block zusammengeführt.

4. Zum Schluss wird noch eine Ausgangspermutation durchgeführt.

Das DES galt lange Zeit als sehr sicher und wurde später durch die Weiterentwicklung (3DES) noch sicherer. Jedoch in der heutigen Zeit der Computertechnik kann es nicht mehr mithalten.

3.2 Public-Key-Verfahren

Bis anhin wurden in der Kryptographie immer symmetrische Schlüssel verwendet, d. h. der Schlüssel für die Ver- und die Entschlüsselung war der gleiche. Eine zweite grosse Neuerung war nun die Verwendung eines asymmetrischen Schlüssels (für die Ver- und die Entschlüsselung zwei unterschiedliche Schlüssel).

Beim Public-Key-Verfahren wird ein Paar zusammenpassender Schlüssel eingesetzt. Der eine Schlüssel ist ein öffentlicher und der andere ein privater.

- öffentlicher Schlüssel: Der öffentliche Schlüssel ist ein bekannter Schlüssel, der zur Verschlüsselung des Klartextes eingesetzt wird. Der öffentliche Schlüssel ist jedoch

für die Entschlüsselung wirkungslos, da der Geheimtext nur mit dem privaten Schlüssel entschlüsselt werden kann.

- privater Schlüssel: Der private (geheime) Schlüssel dient zur Entschlüsselung des Geheimtextes (einer digitale Signatur, einem Message Authentication Code oder einer Authentisierung). Es sollte nur dem Inhaber des Schlüssels bekannt sein.

3.3 Aktuell/Zukunft der Kryptographie

Durch das Internet und den privaten Versand von Nachrichten und Daten wurde es wichtig, dass es auch eine Möglichkeit zur privaten Verschlüsselung von Nachrichten gibt. Der amerikanische Physiker Phil Zimmermann entwickelte daraufhin eine asymmetrische Verschlüsselung für den öffentlichen Gebrauch. Dieses Verschlüsselungsverfahren (Pretty Good Privacy, PGP) wurde 1991 veröffentlicht.

Die neuesten Verschlüsselungsverfahren beruhen neu auf den Gesetzen der Quantenmechanik. Jedoch kann das Verfahren der Quantenkryptographie nur in geographisch begrenzten Netzwerken eingesetzt werden (Rekord, 150 km). Der Grund dafür ist, dass die Signale nicht verstärkt werden können, ohne verändert zu werden.

4. Literaturverzeichnis

Texte:

- Hänni, Rolf (2006). *Einführung in die Kryptographie*. Vorlesungsskript des Institut für Informatik und angewandte Mathematik. Universität Bern.
- Hütter, Arno (2000/01). *Geschichte der Kryptographie*. KV Kryptographie (Skript) des Institut für Systemtheorie Dr. Josef Scharinger

Internet:

- Die Entwicklung der Kryptographie, http://www.it.fht-esslingen.de/~schmidt/vorlesungen/kryptologie/seminar/ws9798/html/krypt_gesch/krypt_gesch-2.html
- Kryptologie – Eine Einführung, Andreas Romeyke, <http://andreas-romeyke.de/privat/Projekt1/ffbr/web.html>

Wikipedia:

- Kryptographie, <http://de.wikipedia.org/wiki/Kryptographie>
- Enigma, http://de.wikipedia.org/wiki/Enigma_%28Maschine%29
- Claude Elwood Shannon, http://de.wikipedia.org/wiki/Claude_Elwood_Shannon
- Öffentlicher Schlüssel, http://de.wikipedia.org/wiki/%C3%96ffentlicher_Schl%C3%BCssel
- Privater Schlüssel, http://de.wikipedia.org/wiki/Privater_Schl%C3%BCssel
- Asymmetrisches Kryptosystem, <http://de.wikipedia.org/wiki/Public-Key-Verfahren>
- DES, http://de.wikipedia.org/wiki/Data_Encryption_Standard