

KV Kryptographie
Wintersemester 2000 / 2001

Geschichte der Kryptographie

Arno Hütter, 9055520, 881 (Kapitel 1)

Institut für Systemtheorie
Dr. Josef Scharinger

Inhaltsverzeichnis

1. Geschichte der Kryptographie vor 1945	1
1.1 Kryptographie in vorchristlicher Zeit	1
1.2 Entstehen der Kryptoanalyse	3
1.3 Kryptographie während der Renaissance	5
1.4 Kryptographie im 17. und 18. Jahrhundert	9
1.5 Kryptographie im aufkommenden Industriezeitalter	10
1.6 Kryptographie zu Beginn des 20. Jahrhunderts	13
1.6.1 Exkurs: One Time Pads	13
1.6.2 Erster Weltkrieg	14
1.6.3 Zwischenkriegszeit	15
1.6.4 Zweiter Weltkrieg	16
2. Geschichte der Kryptographie nach 1945	20
Literaturverzeichnis	21

1. Geschichte der Kryptographie vor 1945

1.1 Kryptographie in vorchristlicher Zeit

Erste frühe Varianten von Steganographie, also des Ansatzes, geheime Botschaften auf einem Trägermedium (welches wiederum selbst eine Botschaft sein kann) zu versenden, sind aus den Hochkulturen Ägyptens, Indiens und Mesopotamiens bekannt. So wurden Nachrichten auf die rasierten Köpfe von Sklaven tätowiert, und diese - nachdem das Haar nachgewachsen war - zu den Empfängern geschickt. Oder es wurden Einkerbungen in Holzplatten mit Wachs aufgefüllt, und die gesamte Platte mit Wachs überzogen. Jäger transportierten Mitteilungen im Bauch von Hasen, die sie kurz zuvor erlegt hatten. Eine weitere Variante waren kleine Löcher in Buchstaben auf Papyrusrollen, die erst bei Gegenlicht sichtbar wurden.

In der Zeit um 1900 vor Christus wurde im alten Ägypten der Sarg von Khnumhotep II, der Architekt der Monument der Pharaos Amenemhet II war, neben den bekannten Hieroglyphen mit einer Reihe unüblichen Zeichen versehen. Ähnliche hieroglyphische Transformationen wurden auch am Sarkophag von Pharaos Seti I entdeckt. Diese Inschriften enthielten damit bereits ein kryptographisches Grundelement, nämlich die Substitution von Symbolen. Da diese abgewandelten Hieroglyphen teilweise direkt neben ihren bekannten Pendanten gleicher Bedeutung aufscheinen wird vermutet, daß diese weniger der Verschlüsselung von Texten dienten, als vielmehr gesellschaftlichen Rang und Autorität des Verstorbenen besonderen Ausdruck zu verleihen, und auch die speziellen Kenntnisse des Schreibers zu verdeutlichen.

[3]



Abbildung 1: Ungebräuchliche (links) und übliche (rechts) Hieroglyphen gleicher Bedeutung

Die Verschleierung von Texten fand auch in alt-testamentarischen Schriften Anwendung. In den Büchern Jeremiah etwa wurde das Wort "Babel" an mehreren Stellen durch den Ausdruck "Sheshech" ersetzt, welcher sich aus einer speziellen Substitution namens "Atbash" ergibt. Im Atbash wird der erste Buchstabe des hebräischen Alphabets durch den letzten ersetzt und umgekehrt. In gleicher Weise wird auch mit dem zweiten bzw. vorletzten Buchstaben vorgegangen, und umgekehrt. Daneben existierten noch weitere ähnliche Substitutionsverfahren wie das Albam (durch Aufspaltung des Alphabets in zwei Hälften und jeweils wechselseitige Ersetzung der Zeichen) oder das Atbah (numerische Äquivalente zu den Buchstaben). Wie schon im alten Ägypten hatten diese Substitutionen hauptsächlich rituelle und mystische Bedeutung. So wurden etwa astronomische Kenntnisse über die Dauer eines Mondzyklus und Annahmen über das Alter des Universums mit Hilfe des Atbash niedergeschrieben.

Aus der Zeit um 475 vor Christus ist das erste militärisch genutzte kryptographische System bekannt. Der spartanische General Pasionius benutzte eine sogenannte Skytale, um verschlüsselte Befehle an seine Truppen zu versenden.

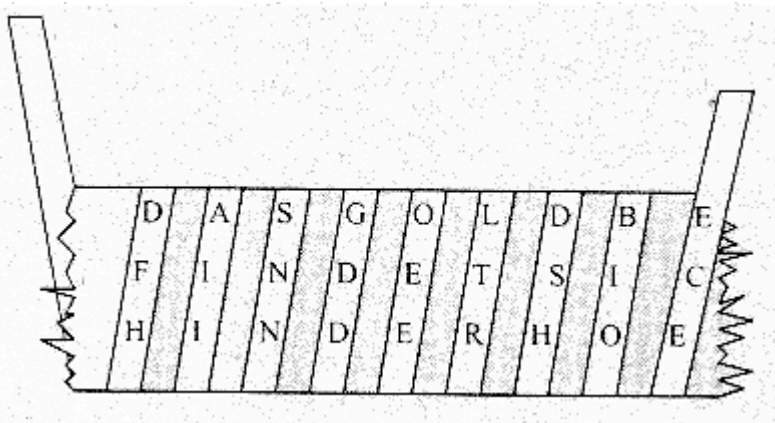


Abbildung 2: Spartanische Skytale

Eine Skytale war ein Holzstab mit definiertem Durchmesser, um den ein Papyrusstreifen gewickelt wurde. Entlang des Stabes wurde dann die Nachricht erfasst, der Papyrusstreifen abgerollt und sodann verschickt. Der Empfänger mußte in Besitz einer exakt gleich beschaffenen Skytale sein, um die Botschaft lesen zu können. Würde der Papyrusstreifen einem Gegner in die Hände fallen, enthielte er nichts anderes als eine keinen Sinn ergebende Folge von Buch-

staben. Es handelt sich dabei um nicht mehr oder weniger als eine frühe Form einer Transposition. [2]

Während Julius Caesars Regentschaft um 50 vor Christus wurde ein einfaches Substitutionsverfahren angewendet, indem man die Buchstaben des Alphabets um eine bestimmte Stellenanzahl nach rechts verschob. Bemerkenswert daran erscheint v.a. der Umstand, daß sich dieses Verfahren erstmals durch inhärente Variabilität auszeichnet. Der Ver- und Entschlüsselungsprozeß basieren nicht aus einer einzigen Übersetzungsvorschrift, sondern werden durch den Verschlüsselungsalgorithmus sowie einen Schlüssel realisiert. Der Verschlüsselungsalgorithmus läßt sich durch den Vorgang des Verschiebens des Klartextalphabets beschreiben, der Schlüssel ist die Anzahl der Stellen.

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

Schlüssel: 3

Chiffrat: 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

Es war relativ einfach, diese Form der monoalphabetische Verschlüsselung so zu verallgemeinern, daß die Zahl der möglichen Schlüssel explosionsartig zunimmt, indem jede Permutation des Alphabets als Geheimentalphabet zugelassen wird, z.B.

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

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

Aus heutiger Sicht mag dieses Verfahren primitiv und unsicher erscheinen, zu Zeiten Caesars war es jedoch mehr als ausreichend und fand über mehrere Jahrhunderte Anwendung.

1.2 Entstehen der Kryptoanalyse

Die ersten kryptoanalytischen Ansätze gehen auf den arabischen Raum zurück. Hier wurde das erste - heute leider verschollene Buch - über Kryptographie verfaßt. Der Autor mit dem

unaussprechbaren Namen Abu 'Abd al-Rahman al-Khalil ibn Ahmad ibn 'Amr ibn Tamman al Farahidi al-Zadi al Yahmadi entschlüsselte Chiffre für den byzantinischen Kaiser auf Basis eines richtig geratenen Beginns des Klartextes - eine kryptoanalytische Vorgehensweise, die selbst noch im 2. Weltkrieg Anwendung fand.

Der Gelehrte Al-Kindi erkannte im 9. Jahrhundert die unterschiedliche Häufigkeit von Buchstaben in einer natürlichen Sprache als Möglichkeit, einen monoalphabetisch verschlüsselten Text zu entschlüsseln, und thematisierte dies in seinem Werk "Abhandlung über die Entzifferung kryptographischer Botschaften". Natürliche Sprachen haben meist relativ wenig Buchstaben, die sehr ungleichmäßige Häufigkeiten aufweisen. In einem monoalphabetisch verschlüsselten Text können diese Strukturen wiedergefunden werden und bilden einen Angriffspunkt für das Brechen der Chiffrierung. [12]

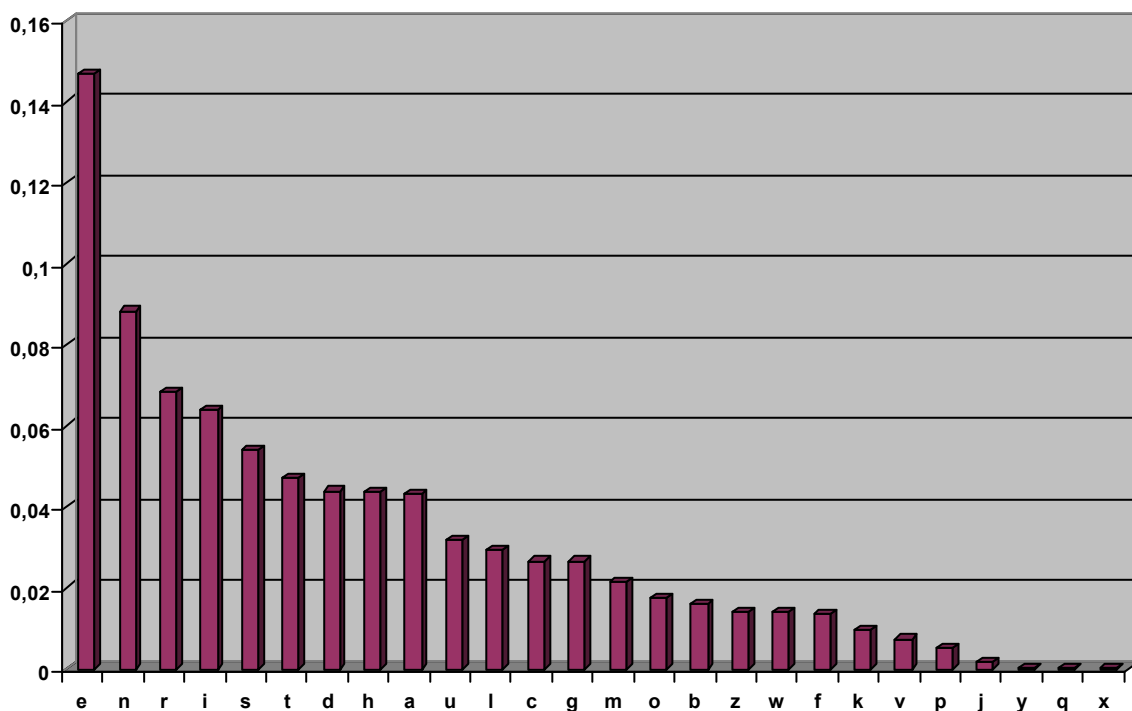


Abbildung 3: Wahrscheinlichkeit des Auftretens von Buchstaben in der deutschen Sprache [1]

Eine einfache Verbesserung stellte der Vorschlag dar, jeden Buchstaben durch genau eine Zahl, etwa im Intervall zwischen 1 und 99 zu ersetzen. Die verbleibenden 73 Zahlen könnten dann mit unterschiedlicher Häufigkeit über den Text verstreut werden und würden es einem

Angreifer erschweren, durch statistische Analyse Rückschlüsse auf den verwendeten Schlüssel zu ziehen. Nachteilig war allerdings der Aufwand bei Chiffrierung und Dechiffrierung, sowie die Übermittlung und Verwahrung des Schlüssels. Je umfangreicher ein Schlüssel war, desto schwerer war es, diesen geheim zu halten.

1.3 Kryptographie während der Renaissance

Im dunklen europäischen Mittelalter spielte die Kryptographie nur eine untergeordnete Rolle. Als diplomatische Beziehungen zwischen den Ländern an Bedeutung gewannen, und ausländische Botschafter vermehrt Nachrichten in die Heimat versandten, wurde auch der Ruf nach verbesserten Methoden zur Verschlüsselung laut. Die bekannten Prinzipien von Substitution und Transposition wurden erweitert durch

- ?? Spezielle Substitutionsalphabete (ähnlich dem erweiterten Caesarianische Code)
- ?? Additionsschematas (Hinzufügen von unnötigen Buchstaben oder Ziffern zwischen jeder Silbe des Chiffrats)
- ?? Symbolische Substitution (Ersetzen von Zeichen durch Punkte, Striche oder andere bedeutungslose Symbole)
- ?? Steganographie

Dennoch glichen diese Verfahren ihren antiken Vorläufern, und hatten auch ähnliche Schwächen. So ist überliefert, daß Königin Maria von Schottland bei ihrer Konspiration gegen Königin Elisabeth von England eine mangelhaft verschlüsselte Botschaft zum Verhängnis wurde, welche im Zuge ihrer Gerichtsverhandlung einer Kryptoanalyse unterzogen und entschlüsselt wurde.

Die erste polyalphabetische Verschlüsselung geht auf Leon Battista Alberti zurück. Damit war es erstmals möglich, ein und dasselbe Zeichen des Klartexts durch verschiedene Zeichen im Chifftrat darzustellen. Alberti schlug in seinem Buch "Modus Scribendi in Zifferas" 1466 vor, für Verschiebechiffrate eine zwei konzentrischen Kupferscheiben zu benutzen, die je

weils das Alphabet enthielten und gegeneinander verdreht werden konnten. Jede Einstellung der Scheiben ergab eine der 26 verschiedenen Verschlüsselungen. Nach einigen verschlüsselten Worten wurden die Scheiben gedreht und somit der Schlüssel verändert. Häufigkeitsanalysen waren dadurch wirkungslos. [3]

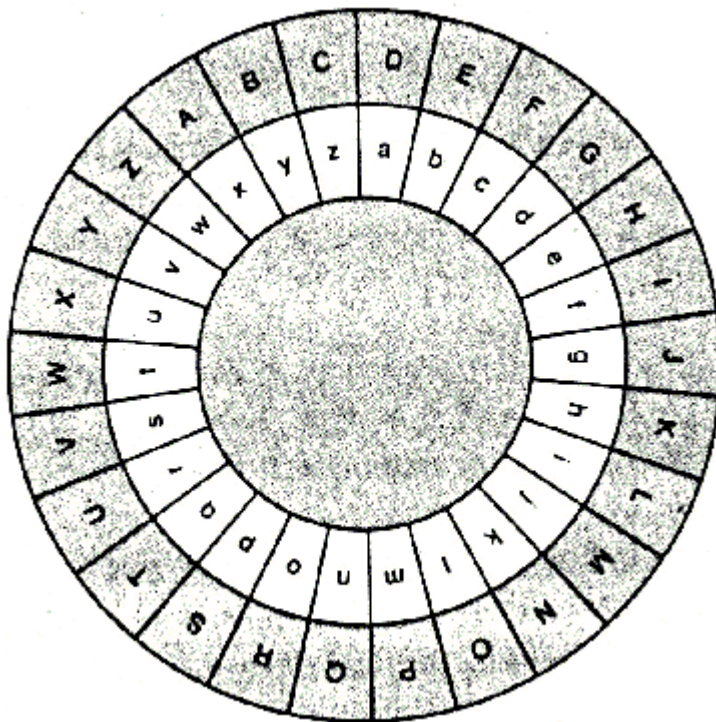


Abbildung 4: Alberti Scheibe

Wenngleich die ursprünglich überlieferte Form dieser Methode einige Schwachstellen aufweist, bedeutete dieses Verfahren einen Meilenstein in der Weiterentwicklung der Kryptographie.

Der Abt Johannes Trithemius (1462-1516) verfaßte die erste Serie von gedruckten Bücher über Kryptographie namens "Polygraphia". Darin beschrieb er unter anderem eine steganographische Verschlüsselungsform, in der jeder Buchstabe des Klartextes durch ein Wort im Chiffrat repräsentiert wurde, und der verschlüsselte Text als Ganzes ein grammatikalisch korrektes Gebet ergab. Trithemius beschrieb auch erstmals polyalphabetische Verschlüsselung in der heute noch verwendeten Form von Substitutionstabellen, wie etwa der folgenden:

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
Schlüssel (t_0): F G U Q H X S Z A C N D M R T V W E J B L I K P Y O
Schlüssel (t_1): Y O F G U Q H X S Z A C N D M R T V W E J B L I K P
Schlüssel (t_2): P Y O F G U Q H X S Z A C N D M R T V W E J B L I K
Schlüssel (t_3): G U Q H X S Z A C N D M R T V W E J B L I K P Y O F

Giovan Batista Belaso erweiterte diese Methode 1553, und fügte vor jedem Codierungsabschnitt des Klartexts ein Schlüsselwort ein, dessen Anfangsbuchstabe in Kombination mit dem Anfangsbuchstaben des nächsten Worts Auskunft darüber gab, welcher Schlüssel der Trithemius-Verschlüsselung als nächster angewendet werden sollte.

Der berühmteste Kryptologe des 16. Jahrhunderts war Blaise de Vigenere. Er arbeitete im diplomatischen Dienst in Rom, wo er in Kontakt mit der Papal Curia trat, eine Gruppe von Kryptologen die in Diensten des Papstes standen. In seinem 1585 erschienen Buch "Traicté des Chiffres" dokumentierte er den damaligen Stand der kryptologischen Forschung, und konzentrierte sich vor allem auf polyalphabetische Verschlüsselung. Die von ihm entwickelte Vigenere Verschlüsselung basiert auf der Vigenere Tabelle und dem Vigenere Algorithmus:
[3]

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

Um einen Klartext zu chiffrieren, wurde zunächst ein Schlüsselwort definiert, und durch mehrfache Wiederholung auf die Länge des Klartextes gebracht. Durch Anwendung der Vigenere Tabelle (spaltenweise das Zeichen des Schlüssels, zeilenweise das Zeichen des Klartextes) konnte erreicht werden, daß hier z.B. das erste M in ein X umgewandelt wird, das zweite in ein G, usw.

Schlüsselwort: L U R I D

Schlüssel: L U R I D L U R I D L U R I

Klartext: M E E T A T M I D N I G H T

Chiffre: X Y V B D E G Z L Q T A Y B

Durch die Eliminierung von Wortgrenzen (etwa durch Verwendung von fünf Zeichen lange Buchstabengruppen), Mischung der Alphabete und die Verwendung von langen Schlüsselwörtern konnte eine sehr starke Verschlüsselung erzielt werden, welche etwaige Angreifer vor beinahe unlösbare Probleme stellten.

1.4 Kryptographie im 17. und 18. Jahrhundert

Seltsamerweise wurde dieses Verfahren damals nur relativ selten eingesetzt - die Regierungen vertrauten großteils weiterhin auf ihre alten diplomatischen Nomenklaturen. Francois de Callieres, ein Botschafter Ludwigs XIV, stellte 1716 fest: *"I do not speak of certain ciphers, invented by professors in a University and upon rules of Algebra or Arithmetick; which are impractical by reason of their too great Length, and of the Difficulties in using them; but of common Cyphers which all Ministers make use of, and with which one may write a Dispatch almost as fast as with ordinary Letters"*. [7]

Tatsächlich hatten die damals existierenden polyalphabetischen Verfahren den Nachteil, daß sich ein kleiner Fehler bei der Verschlüsselung oder der Übertragung die gesamte Nachricht kaskadiert ausbreitete und damit unlesbar machte. Das Risiko, eine wichtige Botschaft könnte dadurch völlig unbrauchbar werden, war vielen Diplomaten zu groß, und so griffen sie auf altbewährte, wenngleich viel unsicherere Methoden zurück.

Seit Beginn des 18. Jahrhunderts waren von den meisten europäischen Herrschaftshäusern sogenannte "Cabinets Noirs" (schwarze Kammern) eingesetzt worden, welche für die Ver- und Entschlüsselung der diplomatischen Post bzw. von abgefangenen feindlichen Botschaften verantwortlich waren. Eine der berühmtesten Kammern war die "Geheime Kabinets-Kanzlei"

in Wien, wo täglich bis zu 100 Briefe dechiffriert wurden. Mit Beginn der industriellen Revolution und dem Untergang einiger totalitärer Regime um 1840 wurden diese Einrichtung vielfach wieder aufgelöst.

Der Vater der amerikanischen Kryptographie war James Lovell. Er war ein Anhänger der amerikanischen Unabhängigkeitsbewegung. Es gelang ihm, zahlreiche englische Chiffrate zu entschlüsseln, was mitentscheidend für den britisch-amerikanischen Krieg war.

1.5 Kryptographie im aufkommenden Industriezeitalter

Mitte des 19. Jahrhunderts führte die Verbreitung des elektrischen Telegraphen zu einer breit geführten öffentlichen Diskussion über dessen Sicherheit. Der Inhalt aller übermittelten Botschaften war den Telegraphenbeamten an Sende- und Empfangsstation zugänglich, genauso wie das Abhören der Leitung ohne größere Probleme möglich war. Eine Stellungnahme der englischen Telegraphengesellschaft verdeutlicht diese Besorgnis:

"Means should also be taken to obviate one great objection, at present felt with respect to sending private communications by telegraph -- the violation of all secrecy.... The clerks of the English telegraph Company are sworn to secrecy, but we often write things that it would be intolerable to see strangers read before our eyes. This is a grievous fault in the telegraph, and it must be remedied some simple yet secure cipher ... should be introduced, by which means messages might to all intents and purposes be "sealed" to any person except the recipient." [3]

Dennoch wurden telegraphische Botschaften weiterhin nur in manchen Fällen - meist für militärische Zwecke - verschlüsselt übertragen.

Industrie und Wirtschaft verlangten ebenfalls vermehrt nach der Möglichkeit, Nachrichten chiffrieren zu können. Es existierten kaufmännische Codebücher, die den Anforderungen jedoch nicht genügten. und so griff man auf altbewährte Methoden zurück, wie etwa die Vige-

nerer Verschlüsselung, welcher sich großer Beliebtheit erfreute - durch den Telegraphen war es auch möglich, etwaige verstümmelte Nachrichten sofort erneut zu senden (die Fehleranfälligkeit war ja ursprünglich ein Hauptkritikpunkt gewesen).

Eine Möglichkeit des Unterdrückens ungleich verteilter Häufigkeiten von Buchstaben ist die Verwendung von Bigrammen. Dabei wurden zwei aufeinanderfolgende Zeichen als eine Einheit behandelt. Da dennoch eine gewisse digraphische Korrelation beim Auftreten von Buchstabengruppen bestand, gab es für die Kryptoanalytiker dennoch Mittel und Wege, derartige Codes zu brechen. Einer der bekanntesten digraphische Substitutionsalgorithmus war der "Playfair Cipher", der Mitte des 19. Jahrhundert von dem englischen Physiker Charles Wheatstone entwickelt wurde. [10]

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

In eine Matrix von 5 x 5 Buchstaben wurde zunächst ein Schlüsselwort geschrieben (hier: MTS), daraufhin wurde die Matrix mit dem Rest des Alphabets gefüllt. I und J wurden gleich behandelt. Der Klartext mußte aus einer geraden Anzahl von Zeichen bestehen, um dies zu erreichen wurde gegebenenfalls ein X angehängt. Daraufhin wurden je zwei Buchstaben des Klartexts betrachtet, und nach folgenden regeln verschlüsselt:

- ?? Das Buchstabenpaar befindet sich in verschiedenen Zeilen und Spalten: Zeilenindizes bleiben gleich, Spaltenindizes werden vertauscht (Bsp.: aus ME wird SC)
- ?? Das Buchstabenpaar befindet sich in der selben Zeile: Die Spaltenindizes werden um eins erhöht (Bsp.: aus TA wird SB)
- ?? Das Buchstabenpaar befindet sich in der selben Spalte: Die Zeilenindizes werden um eins erhöht (Bsp.: aus YL wird AR)

Klartext: ME RC HA NT TA YL OR SZ SC HO OL

Chiffrat: SC OF LM BI AB AR PU BX ME OV RH

Im amerikanischen Bürgerkrieg (1861-1865) waren vielfach relativ einfache Verschlüsselungen im Einsatz. Die Truppen der Konföderation benutzten oftmals eines der drei Wörter "Manchester Bluff", "Complete Victory", and "Come Retribution" als Schlüssel, die sehr bald von Kryptoanalytikern der Union entdeckt und zu ihrem Vorteil genutzt wurden.

1863 gelang es dem preußischen Offizier Friedrich W. Kasiski, eine mögliche Vorgehensweise zum Brechen der Vigenere Verschlüsselung aufzuzeigen. Dabei genügt es Schlüssellängen richtig abzuschätzen. Geht man etwa von einem Schlüsselwort der Länge fünf aus, so wird der erste, sechste, elfte, usw. Buchstabe des Chiffrats zu einem neuen Chiffrat zusammengefügt, das daraufhin einer Häufigkeitsanalyse unterzogen werden kann. Kasiski ermittelte Schlüssellängen, indem er Wiederholungen von Zeichenketten im Chiffrat suchte. Die Distanz zwischen diesen Wiederholungen gaben einen Hinweis auf mögliche Schlüssellängen, meist wurde der größte gemeinsame Teiler der Distanzen gesucht. Dieses Verfahren führte oftmals erst nach einigen Versuchen zum Erfolg, stellte aber einen entscheidenden Fortschritt beim Brechen von polyalphabetischen Verschlüsselungen dar.

1883 schrieb Auguste Kerckhoffs in seinem Buch "La Cryptographie Militaire" sechs grundlegende Forderungen an ein funktionierendes Kryptosystem nieder:

- ?? Ciphertext should be unbreakable in practice
- ?? The cryptosystem should be convenient for the correspondents
- ?? The key should be easily remembered and changeable
- ?? The ciphertext should be transmissible by telegraph
- ?? The cipher apparatus should be easily portable
- ?? The cipher machine should be relatively easily to use

1.6 Kryptographie zu Beginn des 20. Jahrhunderts

1.6.1 Exkurs: One Time Pads

1917 entwickelten Major Joseph Mauborgne und Gilbert Vernam das One Time Pad. In seiner klassischen Ausführung besteht ein One Time Pad aus einer sehr langen Folge von zufällig gewählten Schlüsselbuchstaben, die mehrere Seiten Papier füllen können, welche wiederum zu einem Block zusammengebunden werden. Der Sender chiffriert nun jedes Zeichen des Klartexts mit einem Schlüsselbuchstaben auf dem Block. Die Verschlüsselung basiert auf einer einfachen Addition von Klartext- und Schlüsselzeichen modulo 26.

Dabei wird jeder Schlüsselbuchstabe genau einmal und für eine einzige Nachricht verwendet. Der Sender vernichtet danach die benutzten Seiten seines Schlüsselblocks. Für die nächste Nachricht werden neue Schlüsselbuchstaben herangezogen. Der Empfänger ist in Besitz eines identischen Blocks und dechiffriert die einzelnen Zeichen des Chiffretexts anhand der selben Schlüsselzeichen. Auch er vernichtet im Anschluß daran die benutzten Abschnitte seines Schlüsselblocks.

Klartext: O N E T I M E P A D

Schlüsselsequenz: T B F R G F A R F M

Chiffre: I P K L P S F H G Q

Da

$$(O + T) \text{ MODULO } 26 = I$$

$$(N + B) \text{ MODULO } 26 = P$$

$$(E + F) \text{ MODULO } 26 = K$$

So unglaublich es erscheint, hinter dieser scheinbar simplen Methode verbirgt sich ein theoretisch perfektes Verschlüsselungskonzept. Solange kein Angreifer Zugriff auf das One Time

Pad erhält ist dieses System absolut sicher. Da jede Schlüsselsequenz absolut zufällig erzeugt wird ist, kann ein bestimmtes Chiffre mit der selben Wahrscheinlichkeit von jedem potentiellen Klartext der gleichen Länge stammen. Dem Kryptoanalytiker bietet sich somit keinerlei Angriffsfläche für eine Kryptoanalyse.

Es existieren jedoch ebenso schwerwiegende Vorbehalte gegen diese Methode, welche deren Anwendbarkeit in der Praxis bis auf einige Ausnahmen stark einschränken. Ein Schwachpunkt ist die Forderung nach der Generierung einer großen Anzahl von zufälligen Schlüsselbuchstaben: Pseudozufallszahlen-Generatoren kommen dafür nicht in Frage, da diese immer Regelmäßigkeiten aufweisen. Die Länge der Schlüsselsequenzen stimmen mit der Länge der Nachrichten überein, und dürfen unter keinen Umständen mehrfach verwendet werden. Damit sind One Time Pads bestenfalls für kurze Mitteilungen geeignet, aber nicht für Kommunikationskanäle mit mehreren Mbit pro Sekunde. Dazu kommt das Problem der Weitergabe des Schlüssels und die Notwendigkeit einer ständigen Synchronisation was die Position auf dem Schlüsselblock betrifft. [11]

Dennoch wurden und werden One Time Pads verwendet, vorzugsweise wenn geringe Datenmengen mit höchsten Sicherheitsansprüchen sicher übertragen werden sollten. Gerüchten zufolge wurden Gespräche über das berühmte rote Telefon zwischen den Vereinigten Staaten und der ehemaligen Sowjetunion mit einem One Time Pad verschlüsselt. Zahlreiche Mitteilungen sowjetischer Spione wurden ebenfalls auf diese Weise chiffriert - diese existieren heute noch und sind bis in alle Ewigkeit geschützt, solange die damals verwendeten One Time Pads nicht zur Verfügung stehen

1.6.2 Erster Weltkrieg

Zu Beginn des 20. Jahrhunderts wurde der Krieg in Europa zunehmend wahrscheinlicher. Die Nationen verstärkten ihre Bemühung auf kryptologischem Gebiet. In England existierte eine Gruppe von Kryptologen mit dem Namen "Room 40". Unter anderem gelang ihnen die Decodierung der Verschlüsselung der deutschen Marine. Dies wurde insofern vereinfacht, als

die Deutschen oftmals politische und nationalistische Schlüsselworte verwendeten, und diese in regelmäßigen Intervallen änderten. Auch Funkübertragungen wurden vermehrt das Ziel kryptoanalytischer Angriffe. Französische Experten konnten während des ersten Weltkriegs deutsche Signale abfangen, und überwandern deren einfache doppelte spaltenweise Transposition mühelos. [2]

1.6.3 Zwischenkriegszeit

1917 gründeten die Amerikaner eine kryptographische Organisation namens MI-8. Während und nach des Krieges analysierte diese Abteilung alle Arten von Geheimnachrichten, verschlüsselten Botschaften und Codes. 1929 wurde MI-8 aufgrund von moralischen Bedenken des damaligen amerikanischen Präsidenten Hoover geschlossen. Der damalige Leiter der Abteilung Herbert Osborne Yardley verfaßt daraufhin ein Buch namens "The American Black Chamber", in dem er die Arbeit und Erkenntnisse der MI-8 detailgetreu beschrieb. Das Buch wurde ein Bestseller.

Ende der 20er Jahre gelang es William F. Friedman, dem Leiter der Chiffrierabteilung der amerikanischen Armee und Vorgängerorganisation der heutigen NSA, auf zuverlässige Art und Weise, Schlüssellängen von Vigenere Chiffrierungen zu ermitteln: verschiebt man einen polyalphabetisch verschlüsselten Text buchstabenweise gegen sich selbst, berechnet die Verhältniszahl des Auftretens gleicher Buchstaben an der selben Stelle und ergeben sich Werte größer als $1/26$, so ist dies ein deutlicher Hinweis darauf, daß der Abstand der Verschiebung der Schlüssellänge entspricht.

Zu dieser Zeit arbeitete man auch daran, Verschlüsselung zu automatisieren. Die Grundverfahren blieben vielfach die gleichen, aber die Effizienz und Verlässlichkeit der Verschlüsselung wurde stark verbessert. So entwickelte der Amerikaner Gilbert S. Vernam für AT&T ein System, das Telephon- und Telegraphenimpulse über einen Schlüssel in chiffrierte Impulse übersetzte.

1929 veröffentlichte Lester S. Hill seinen Artikel "Cryptography in an Algebraic Alphabet". Er ersetzte Buchstaben durch numerische Werte, und verschlüsselte den Klartext über Polynomgleichungen in Matrizenform. Diese Methode eliminierte beinahe alle Zeichenwiederholungen und konnte durch statistische Verfahren nicht gebrochen werden, hatte aber - wie sich später herausstellte - eine andere Schwäche: bei Kenntnis zweier verschiedener Chiffre ein und desselben Klartextes durch Verwendung verschiedener Gleichungssysteme konnten die Gleichungssysteme gelöst werden. [2]

Ein großer Fortschritt in der Entwicklung elektromechanischer Kryptographie war die Erfindung des Rotors. Dieser bestand aus einer beidseitig beschichteten Scheibe mit jeweils 26 Messingkontakten für je einen Buchstaben. Eine Seite stellt den Signaleingang, die andere den Ausgang dar, die Zuordnung ließ sich über einen elektrischen Impuls steuern. Ein einfacher Rotor konnte damit einen monoalphabetischen Substitutionsalgorithmus implementieren. Er übernahm das Signal einer Schreibmaschinentastatur und wandelte diesen in ein chiffriertes Zeichen um. Nach jedem Buchstaben wird der Rotor um eine Position gedreht, und ermöglicht damit eine progressive polyalphabetische Substitution mit einer Periodenlänge 26. Ein zweiter Rotor erhöht diese Zahl auf 676, bei fünf Rotoren sind es 11.881.376 - bei einer derartigen Periodenlänge sind extrem umfangreiche Chiffre nötig, damit eine Frequenzanalyse zielführend ist. Problematisch sind allerdings Wiederholungen innerhalb von Chiffresegmenten von 26 Zeichen. [2]

1.6.4 Zweiter Weltkrieg

Die berühmteste Chiffriermaschine des zweiten Weltkriegs war zweifellos die ENIGMA. Sie wurde bereits 1918 von Arthur Scherbius und ging 1925 in Serienfertigung. Das deutsche Militär kaufte zwischen bis 1945 über 30.000 ENIGMAS - man wollte eine Wiederholung eines kryptographischen Debakels wie im ersten Weltkrieg um jeden Preis verhindern. Die ENIGMA ermöglichte die Verwendung von ca. 159.000.000.000.000.000 unterschiedlichen Schlüsseln. So fortschrittlich dies auf den ersten Blick auch schien, war dieses Gerät

letztlich aber nichts anderes als eine komplizierte Buchstaben-Substitutions-Maschine und hatte einige fatale Schwachstellen.

Die Deutschen änderten ihre Schlüssel täglich. Die Konfigurationsräder der ENIGMA wurden entsprechend justiert, dann beliebig weiterbewegt, und der resultierende Output zweimal hintereinander eingetippt. Das verschlüsselte Ergebnis wurde erneut zur Konfiguration der Maschine herangezogen. Sich wiederholende Sequenzen wie die doppelte Eingabe sind oftmals Ansatzpunkt für die Kryptoanalyse, so auch hier.

Durch einen glücklichen Umstand waren einige interne Kenntnisse über die Funktionsweise der ENIGMA an Frankreich und in weiterer Folge an Polen gelangt. Unter der Leitung von Marian Rejewski begann ein Team polnischer Experten an der Entschlüsselung zu arbeiten - notwendig dafür waren möglichst viele mit ein und demselben Schlüssel chiffrierte Nachrichten. Nachdem man genug Informationen gesammelt hatte, begann man eine Replik der ENIGMA zu rekonstruieren. [3]



Abbildung 5: Die ENIGMA

1940 wurden die Arbeiten Rejewskis von Großbritannien fortgesetzt. Man gelangte in den Besitz eines Codebuchs der deutschen Marine, und konnte dadurch weitere Fortschritte erzielen. Am schwierigsten gestaltete sich die Entschlüsselung von Hitlers persönlicher Variante der ENIGMA, einer Lorenz SZ40, die über zwölf austauschbare Rotoren verfügte. Eines Tages wiederholte ein deutscher Funker eine Nachricht aufgrund von Übertragungsproblemen, und kürzte dabei ungeduldig einige Worte ab. Die beiden stark ähnelnden Nachrichten boten den Briten mehr als genug Material. Zur Entschlüsselung setzte man Alan Turings Universal-

rechner ein - innerhalb von wenigen Minuten konnten abgefangene Botschaften so dechiffriert werden. Fünf Monate vor der Landung der Alliierten in der Normandie konnte man sämtliche deutsche Übertragungen mitverfolgen, ein unschätzbare und kriegsmitentscheidender Vorteil.

2. Geschichte der Kryptographie nach 1945

Literaturverzeichnis

- [1] Bauer, Goos: "Informatik 1", 4. Auflage, Springer Verlag, München 1990
- [2] Cohen, F.: "A Short History of Cryptography", <http://all.net/books/ip/Chap2-1.html>
- [3] Glikman, A.: "The Work of Cryptography in the Age of Digital Transmission: Codes & Ciphers In Mystical Authority, Rationalized Machines, and Public Keys", <http://ccwf.cc.utexas.edu/~glik/crypto-hist/crypto-hist.html>
- [4] Deavours, C.: "Cryptology yesterday, today, and tomorrow", Artech House, Norwood, Mass.1987
- [5] Dupuy, P.: "Early Cryptology", <http://fly.hiwaay.net/~paul/cryptology/history.html>
- [6] Ellison, C.: "Cryptology Timeline", <http://world.std.com/~cme/html/timeline.html>
- [7] Leary, T.: " Cryptology in the 16th and 17th Centuries", <http://home.att.net/~tleary/cryptolo.htm>
- [8] N.N.: "Cryptographic Timeline", <http://library.thinkquest.org/28005/flashed/timemachine/timeline.shtml>
- [9] N.N.: "Timeline of Cryptology", <http://www.math.nmsu.edu/~crypto/Timeline.html>
- [10] Pell, O.: "Cyptology", <http://www.ridex.co.uk/cryptology/index.html>
- [11] Schneier, B.: "Angewandte Kryptographie", 1. Auflage, Addison Welsey, Bonn 1996
- [12] Tiemann, V.: "Symmetrische / klassische Kryptographie", http://www.wiwi.uni-bielefeld.de/StatCompSci/lehre/material_spezifisch/statalg00/caesar/caesar.html