thawte®

Die Geschichte der Chiffren

EINE EINFÜHRUNG

Inhaltsverzeichnis

1. Einleitung

Mit der schnellen und inzwischen nahezu allgegenwärtigen Ausweitung des Internets hat auch die Verschlüsselung zur Gewährleistung der Informationssicherheit an Bedeutung gewonnen.

Die Nutzung von Chiffren reicht bis ins alte Ägypten um 3000 v. Chr. zurück. Ursprünglich wurden sie für militärische und diplomatische Zwecke entwickelt, doch in jüngster Zeit hat sich ihr Einsatzgebiet erheblich vergrößert, insbesondere durch das Internet und die schnell wachsenden Datenmengen, die wir in vielen Bereichen unseres Lebens täglich nutzen.

Die Entwicklung der Chiffren und insbesondere der geistigen Duelle zwischen Kryptografen (den Code-Entwicklern) und Kryptoanalysten (den Code-Knackern) ist eine faszinierende Geschichte. Die moderne Kryptografie ist das Ergebnis wiederholter Zyklen aus der Entwicklung von Codes, dem Knacken dieser Codes und der darauf folgenden Entwicklung neuer Codes.

In diesem Whitepaper möchten wir Ihnen eine Einführung in die Geschichte der Chiffren geben. Es stellt die wichtigsten Entwicklungen in der Verschlüsselungstechnik sowie eine Reihe von Maßnahmen vor, die auch bei modernen Chiffren angewendet werden sollten.

2. Chiffren in der Antike

Die ältesten bekannten Chiffren sind ägyptische Hieroglyphen auf Monumenten, die um 3000 v. Chr. errichtet wurden. Hieroglyphen galten als nicht entzifferbar, bis im 19. Jahrhundert der weltberühmte Stein von Rosette entdeckt wurde. Mit den Forschungsarbeiten an diesem Stein begann die Entschlüsselung der Hieroglyphen.

Kehren wir jedoch noch einmal in die Antike zurück. Etwa im sechsten Jahrhundert v. Chr. wurden im griechischen Stadtstaat Sparta sogenannte Skytalen zur Verschlüsselung von Botschaften eingesetzt. Bei diesem Verschlüsselungsverfahren schrieb der Absender seine Botschaft auf einen Streifen Pergament, der um einen dicken Stab, die Skytale, gewickelt war. Dann wurde nur der Pergamentstreifen an den Empfänger geschickt. Wenn dieser einen Stab mit dem gleichen Umfang besaß, konnte er den Pergamentstreifen um diesen wickeln und die Nachricht lesen.

Verfahren wie dieses, die einen Text verschlüsseln, indem sie die Reihenfolge der in ihm enthaltenen Buchstaben ändern, werden als Transpositionsverfahren bezeichnet.

Der nächste Meilenstein war die Entwicklung der Cäsar-Chiffre im ersten vorchristlichen Jahrhundert. Sie verdankt ihren Namen dem römischen Kaiser Julius Cäsar, der dieses Verfahren oft anwendete, und ist bis heute eine der berühmtesten Techniken der Kryptografie.

Die Cäsar-Chiffre funktionierte folgendermaßen: Jeder Buchstabe der Originalnachricht wurde durch den Buchstaben ersetzt, der sich eine bestimmte Anzahl von Positionen weiter hinten im Alphabet befindet. Die Anzahl der Positionen für diese Verschiebung war sowohl dem Absender als auch dem Empfänger bekannt. In diesem Beispiel sind es drei:

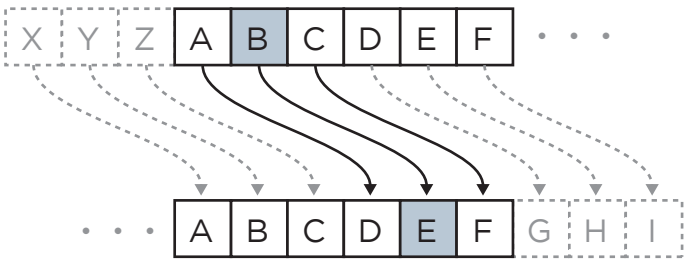

Abbildung 1

Verfahren wie die Cäsar-Chiffre, die jeden Buchstaben eines Textes durch Verschieben im Alphabet verschlüsseln, werden als Verschiebechiffren bezeichnet. Diese Chiffren können durch das Ausprobieren von höchstens 25 Verschiebungen einfach entschlüsselt werden. Durch den Einsatz einer zufälligen Verschiebung kann die Anzahl der möglichen Permutationen jedoch gewaltig gesteigert werden (und zwar auf 26 × 25 × 24 × … > 400 000 000 000 000 000 000 000 000!), wodurch die Entschlüsselung deutlich erschwert wird.

Klartext (nicht verschlüsselter Text)	ABCDEFGHIJKLMNOPQRSTUVWXYZ
Verschlüsselter Text	SMKRATNGQJUDZLPVYOCWIBXFEH

Verschlüsselungsverfahren wie dieses, bei denen eine statische Regel festlegt, wie die Buchstaben des Klartextes zu verschlüsseln sind, werden als Substitutionsverfahren bezeichnet. Die Substitution ist eine klassische und die historisch gesehen meistverwendete Technik der Kryptografie. Selbst die moderne mechanische Chiffriermaschine Enigma nutzte ein fortgeschrittenes Substitutionsverfahren.

Methoden wie die Cäsar-Chiffre, die auf einer Regel für die Substitution der Buchstaben des Alphabets beruhen, werden als einfache Substitutionschiffren bezeichnet. Ihr charakteristisches Merkmal ist die 1:1-Beziehung zwischen Buchstaben im verschlüsselten und im Klartext. Diese Beziehung ermöglicht die Entschlüsselung mithilfe von Häufigkeitsanalysen.

Diese Entschlüsselungsmethode beruht auf Versuchen, die Klartextäquivalente verschlüsselter Buchstaben aufgrund ihrer Häufigkeit im verschlüsselten Text zu erraten. Diese Versuche stützen sich auf linguistische Besonderheiten der Klartextsprache, wie zum Beispiel:

- Im Deutschen kommen die Buchstaben „e“ und „n“ am häufigsten vor. Im Englischen sind es „e“ und „t“ (siehe Abbildung 2).
- Auf „c“ folgt im Deutschen wie im Englischen häufig „h“, auf „h“ jedoch nur äußerst selten „c“.
- Wörter wie „die“, „der“, „und“, „in“, „am“, „zu“, „den“, „das“ und „nicht“ kommen sehr häufig vor.

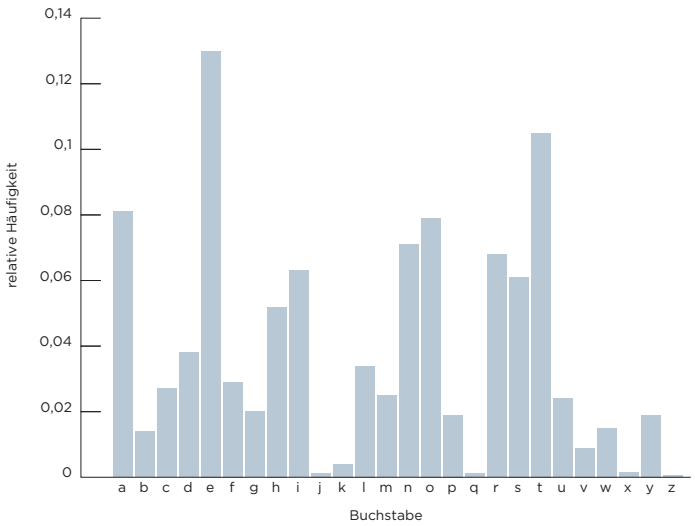

Abbildung 2

Alle bisher beschriebenen Chiffren, ob Transpositions- oder Substitutionsverfahren, bestehen aus einem kryptografischen oder Verschlüsselungsalgorithmus und einem Schlüssel. Der Algorithmus ist die Regel, die zur Verschlüsselung des Klartextes und zur Entschlüsselung des verschlüsselten Textes angewendet wird.

Bei der Verschiebechiffre ist diese Regel beispielsweise die Verschiebung im Alphabet um eine bestimmte Anzahl von Positionen, beim anfangs beschriebenen Transpositionsverfahren ist es das Prinzip, den Text auf einen um eine Skytale gewickelten Pergamentstreifen zu schreiben. Der Schlüssel ist die Anzahl der Positionen für die Verschiebung bzw. der Umfang der Skytale. Wird ein Text mithilfe der Cäsar-Chiffre verschlüsselt und dabei jeder Buchstabe durch den fünf Positionen weiter hinten im Alphabet stehenden Buchstaben ersetzt, ist der Algorithmus derselbe wie in Abbildung 2, aber der Schlüssel ist fünf statt wie oben drei.

3. Chiffren im Mittelalter

Im Mittelalter wurden die oben beschriebenen klassischen Chiffren entschlüsselt und neue, weiterentwickelte kryptografische Verfahren mussten erfunden werden. Gleichzeitig nahmen diplomatische Aktivitäten und damit das Volumen vertraulicher Informationen erheblich zu, so dass die Kryptografie in dieser Periode häufiger und von mehr Personen angewendet wurde.

Die Chiffre der Maria Stuart

Der Nachteil einfacher Substitutionschiffren wie der Cäsar-Chiffre ist die 1:1-Beziehung zwischen verschlüsselten und Klartextbuchstaben. Der Fall der schottischen Königin Maria Stuart im 16. Jahrhundert ist ein berühmtes Beispiel für diese Schwäche. Die Entschlüsselung der Chiffre, die Maria Stuart und ihre Mitverschwörer für ihre Geheimnachrichten benutzten, führte dazu, dass Maria Stuart des Hochverrats beschuldigt und schließlich hingerichtet wurde, weil sie die Ermordung der Königin Elizabeth I. von England geplant hatte.

Die von Maria Stuart und ihren Mitverschwörern benutzte Chiffre war ein sogenannter Nomenklator. Neben Symbolen für einzelne Buchstaben enthielt er auch Symbole für ganze, häufig verwendete Wörter und Sätze. Das setzte voraus, dass der Sender und der Empfänger ein Codebuch besaßen, den Schlüssel zu diesem Algorithmus. Die Entschlüsselung dieser Chiffre war dadurch schwieriger als die ihrer Vorgänger. Für Maria Stuart dürfte das allerdings wenig tröstlich gewesen sein.

Die Vigenère-Chiffre

Bei der Chiffre der Maria Stuart und ähnlichen Beispielen ist die Entschlüsselung durch die 1:1-Beziehung zwischen verschlüsselten und Klartextbuchstaben nicht wesentlich schwieriger als bei einer einfachen Substitutionschiffre. Nomenklatoren bereiten ihren Anwendern ebenfalls Probleme, darunter die Vorbereitung und Weitergabe eines umfangreichen Codebuchs. Die sichere Weitergabe des Schlüssels wurde immer wieder zur Achillesferse, nicht nur im Mittelalter, sondern bis zu den fortgeschrittenen kryptografischen Verfahren der Moderne.

Im 15. Jahrhundert hatte Leon Battista Alberti erstmals die Idee für ein polyalphabetisches Substitutionsverfahren, bei dem mehrere Substitutionsalphabete benutzt wurden. Damit war der Grundstein für weitere Entwicklungen gelegt. Blaise de Vigenère entwickelte die endgültige Form der polyalphabetischen Substitutionschiffren, die relativ sichere Vigenère-Chiffre.

Zur Ver- und Entschlüsselung ist das sogenannte Vigenère-Quadrat erforderlich (siehe Abbildung 3). Um beispielsweise das Wort „Goldmedaille“ mithilfe des Schlüsselworts „Olympia“ zu verschlüsseln, muss man zunächst in der obersten Zeile des Vigenère-Quadrats den ersten Klartextbuchstaben und in der linken Spalte den ersten Schlüsselwortbuchstaben finden. Der Schnittpunkt der so ermittelten Spalte und Zeile enthält den ersten verschlüsselten Buchstaben.

Klartext	GOLDMEDAILLE
Schlüssel	OLYMPIAOLYMP
Verschlüsselter Text	UZJPBMDOTJXT

	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

Abbildung 3

Mit dieser Chiffre erhält man völlig unterschiedliche verschlüsselte Texte, wenn man bei gleichem Klartext das Schlüsselwort ändert. Deshalb ist die Entschlüsselung ohne dieses Schlüsselwort extrem schwierig, auch wenn die Tabelle in die Hände Dritter fällt. Der entscheidende Vorteil dieser Methode ist, dass das Schlüsselwort beliebig lang sein kann. Dadurch ist der sogenannte Zyklus, die Anzahl der verschlüsselten Buchstaben, bevor der erste Buchstabe des Schlüsselworts erneut zum Einsatz kommt, unbestimmt und die Anzahl möglicher Schlüssel unendlich.

Dennoch war die Vigenère-Chiffre kein sofortiger Erfolg. Von Battista Albertis ursprünglicher Idee bis zur Formulierung des Algorithmus vergingen über hundert Jahre. Während dieser Zeit waren weiterhin einfache Substitutionschiffren in Gebrauch. Die im Vergleich zu hergebrachten Verfahren wesentlich kompliziertere Ver- und Entschlüsselung verzögerte die praktische Anwendung der Vigenère-Chiffre weit über die Veröffentlichung im Jahr 1586 hinaus.

Die Uesugi-Chiffre

Eine andere tabellenbasierte Chiffre wurde ebenfalls im 16. Jahrhundert in Japan entwickelt. Die Erfindung dieser auf dem Polybios-Quadrat aufbauenden Verschlüsselungstabelle wird Usami Sadayuki, dem militärischen Berater des Daimyo (feudalen Kriegsherren) Uesugi Kenshin zugeschrieben. Da das traditionelle japanische Alphabet Iroha 48 Buchstaben hat, besteht die Tabelle aus je sieben Zeilen und Spalten. Jedes Symbol wird durch seine Zeilen- und Spaltennummer repräsentiert (siehe Abbildung 4).

7	6	5	4	3	2	1	
we	a	ya	ra	yo	chi	i	1
hi	sa	ma	mu	ta	ri	ro	2
mo	ki	ke	u	re	nu	ha	3
se	yu	fu	wi	so	ru	ni	4
su	me	ko	no	tsu	wo	ho	5
n	mi	e	o	ne	wa	he	6
	shi	te	ku	na	ka	to	7

Abbildung 4

4. Moderne Chiffren: Vom Ersten Weltkrieg bis zu den ersten mechanischen Chiffriermaschinen

Die Entwicklung der Kommunikationstechnik führte zu großen Fortschritten in der Kryptografie und Kryptoanalyse im Verlauf des Ersten Weltkriegs.

Die Kappung der deutschen Kommunikationskabel

Als Großbritannien 1914 in den Krieg eintrat, durchschnitt die britische Marine im Ärmelkanal die deutschen Seekabel für die Kommunikation mit den USA und anderen Ländern. Infolgedessen konnte das deutsche Militär Nachrichten nach Übersee nur über internationale Seekabel, und damit über Großbritannien, oder per Funkübertragung senden. Die deutschen Streitkräfte verschlüsselten also alle Nachrichten, um das Abhören durch die Kriegsgegner zu verhindern. In Großbritannien wurden jedoch alle Nachrichten abgefangen und an eine eigens geschaffene kryptoanalytische Abteilung im britischen Marineministerium, das sogenannte Zimmer 40 (Room 40), weitergeleitet. Dort wurde die deutsche Chiffre entschlüsselt. Die Entschlüsselung der Zimmermann-Depesche war ein Ergebnis dieser Initiative.

Die Zimmermann-Depesche

Der Kriegseintritt der USA änderte den Verlauf des Konflikts in Europa. Arthur Zimmermann, der Außenminister des Deutschen Reichs, hatte einen Plan ersonnen, um den Kriegseintritt der USA zu verhindern. Sollte dieser fehlschlagen, wollte er Mexiko und Japan zu einem Überfall auf die Vereinigten Staaten bewegen. Zimmermann schickte ein Telegramm mit entsprechenden Anweisungen an den deutschen Botschafter in Mexiko. Diese Depesche wurde im „Room 40“ entschlüsselt. Die Briten beschlossen jedoch, die entschlüsselte Nachricht nicht zu veröffentlichen. Ein Grund hierfür war die Befürchtung, dass Deutschland eine neue, sicherere Chiffre entwickeln würde, wenn bekannt würde, dass die Briten die bestehende Chiffre entschlüsselt hatten. Stattdessen beschaffte ein im mexikanischen Telegrafenamt eingeschleuster britischer Spion eine Klartextversion des Telegramms. Diese wurde veröffentlicht und löste die amerikanische Kriegserklärung an Deutschland und den Kriegseintritt der USA auf Seiten der Alliierten aus.

Diese Anekdote zeigt, dass Kryptoanalysten die erfolgreiche Entschlüsselung einer Chiffre nicht unbedingt sofort bekannt geben, sondern zunächst versuchen, die Entschlüsselungsmethode eine Zeit lang zu nutzen. Schließlich hat die Bekanntgabe der Entschlüsselung gewöhnlich die Entwicklung einer neuen, schwerer zu entschlüsselnden Chiffre zur Folge. Dieser ständige Kreislauf aus der Entwicklung und Entschlüsselung immer neuer Chiffren hält bis heute an.

Die ADFGVX-Chiffre

Die von Fritz Nebel, einem Oberst der deutschen Armee, entwickelte ADFGX-Chiffre wurde ab 1918 verwendet. Sie basiert auf einem Polybios-Quadrat, dessen Zeilen und Spalten mit den Buchstaben ADFGX beschriftet sind. Jeder Buchstabe wird als das Buchstabenpaar verschlüsselt, das seine Zeilen- und Spaltenposition in der Tabelle angibt. Soweit ähnelt die ADFGX-Chiffre der Uesugi-Chiffre. Dann wurde das Ergebnis jedoch mithilfe eines Transpositionsverfahren nochmals verschlüsselt. Die ADFGX-Chiffre wurde durch die ADFGVX-Chiffre ersetzt, die auf einer Tabelle mit je sechs Zeilen und Spalten basierte. Die Buchstaben A, D, F, G, V und X wurden zur Verschlüsselung genutzt, weil die ihnen entsprechenden Morsezeichen am einfachsten voneinander zu unterscheiden sind.

	A	D	F	G	V	X
A	d	h	x	m	u	4
D	p	3	j	6	a	o
F	i	b	z	v	9	w
G	1	n	7	0	q	k
V	f	s	l	y	c	8
X	t	r	5	e	2	g

Abbildung 5: die ADFGVX-Chiffre

Wenn die als Schlüssel dienenden Tabellen jeweils nur einmal verwendet werden, ist es praktisch unmöglich, diese Chiffre zu knacken. Dazu müssten allerdings eine große Anzahl dieser Schlüssel an die Front weitergeleitet werden. Der Transport erwies sich insbesondere in Gefechtssituationen als sehr problematisch.

Die Enigma

Die Entschlüsselung von Chiffren wurde erheblich komplexer, als zu Beginn des 20. Jahrhunderts die bis dahin manuell erfolgte Verschlüsselung durch die Entwicklung mechanischer Chiffriermaschinen revolutioniert wurde.

Die als Enigma vermarktete Produktreihe mechanischer Chiffriermaschinen wurde 1918 von dem deutschen Ingenieur Arthur Scherbius entwickelt. Bei der Vermarktung wurden insbesondere die Tragbarkeit und Sicherheit der Geräte hervorgehoben. Zur Zeit der Produkteinführung war der deutschen Armee noch nicht bekannt, dass ihre im Ersten Weltkrieg benutzte Chiffre geknackt worden war. Daher bestand wenig Interesse an der Aufrüstung auf die als zu teuer eingeschätzte Enigma.

Nach der Niederlage bildete sich jedoch die Meinung heraus, dass die Entschlüsselung deutscher Chiffren durch die britische Marine maßgeblich dazu beigetragen hatte und dass die Kryptografie das Schicksal der Nation in Zukunft mitbestimmen würde. Daraufhin wurde der Einsatz von Enigma in den deutschen Streitkräften beschlossen.

Enigma nutzte ein polyalphabetisches Substitutionsverfahren. Das Gerät bestand aus einer als „Zerhacker“ bezeichneten Anordnung aus mehreren Rotoren, die mit den 26 Buchstaben des Alphabets beschriftet waren, und einem Steckfeld, mithilfe dessen einzelne Buchstabenpaare miteinander vertauscht werden konnten. Diese Kombination war der Schlüssel der Chiffre. Nachdem der Zerhacker konfiguriert war, konnte man den Klartext über eine Tastatur eingeben. Dieser wurde dann durch den Zerhacker verschlüsselt und der verschlüsselte Text auf einem Lampenfeld angezeigt. Nach jedem über die Tastatur eingegebenen Buchstaben drehte sich die Rotorenanordnung des Zerhackers eine Position weiter, so dass sich der Schlüssel mit jedem eingegebenen Buchstaben änderte.

Die Verwendung derselben Schlüssel für die Ver- und Entschlüsselung vereinfachte beide Prozesse.

Die Enigma wurde nach ihrem Ersteinsatz in der deutschen Armee weiterentwickelt. Beispielsweise wurde die Anzahl der in einem Zerhacker installierbaren Rotoren von drei auf fünf erhöht. Der Zerhacker nutzte dann jeweils drei dieser Rotoren.

Die Deutschen hatten nahezu absolutes Vertrauen in Enigma. Angesichts der aus Deutschland drohenden Invasionsgefahr wurde in Polen jedoch die Kryptoanalyse vorangetrieben. Dies führte zur Erfindung einer Maschine, die „Bombe“ genannt wurde. Weitere Verbesserungen an Enigma erhöhten jedoch die Anzahl der möglichen Verschlüsselungsmuster und Polen war aus ökonomischen Gründen nicht in der Lage, seine Kryptoanalyseforschung fortzusetzen. Stattdessen übergab Polen seine Forschungsergebnisse 1939 an das sowohl finanziell als auch personell bessergestellte Großbritannien. Zwei Wochen später erfolgte der deutsche Überfall auf Polen, mit dem der Zweite Weltkrieg begann.

Mithilfe des in Polen nachentwickelten kryptografischen Algorithmus’ machten britische Kryptoanalysten große Fortschritte bei der Entschlüsselung des Enigma-Codes. Dabei stellte sich heraus, dass der zur Einstellung der Rotoren nötige Schlüssel eine Kombination aus drei Buchstaben war, die am Anfang jeder verschlüsselten Nachricht zweimal gesendet wurde, so dass der Empfänger seine Enigma für die Entschlüsselung einstellen konnte. Diese Erkenntnis brachte den Durchbruch bei der Entschlüsselung des Enigma-Codes.

Aus der Enigma-Entschlüsselung gewonnene Informationen erhielten den Decknamen „Ultra“ und blieben bis zum Kriegsende eine wichtige Informationsquelle der Alliierten. Die erfolgreiche Entschlüsselung des Enigma-Codes wurde streng geheim gehalten, so dass die Geräte von den Deutschen bis zum Kriegsende ohne Bedenken benutzt wurden. Erst 1974, mehr als 30 Jahre nach der ersten erfolgreichen Entschlüsselung 1940, wurde sie öffentlich bekannt gegeben.

5. Die Gegenwart: Chiffren im Computer- und Internetzeitalter

Seit dem Zweiten Weltkrieg hat es in der Kryptografie weitere gewaltige Veränderungen gegeben. Maschinen für die Ver- und Entschlüsselung wurden durch Computer ersetzt. Seitdem ist durch die rasche Verbreitung von Computern in der freien Wirtschaft die Bedeutung der Kryptografie für geschäftliche Transaktionen, andere zivile Anwendungen und das Militär gestiegen.

Die DES-Chiffre

Wie schon bei Enigma wurde die erfolgreiche Entschlüsselung von Chiffren weiterhin in jedem Land streng geheim gehalten. Das änderte sich 1973 mit der Ausschreibung eines kryptografischen Verfahrens für den Standardgebrauch durch das Normenbüro des US-amerikanischen Wirtschaftsministeriums (damals NBS, heute National Institute of Standards and Technology, NIST).

Wie bereits mehrfach erwähnt, besteht ein kryptografisches Verfahren aus einem Verschlüsselungsalgorithmus und einem Schlüssel. Mit der Veröffentlichung des DES-Algorithmus (Data Encryption Standard) und seiner Annahme durch das NBS im Jahr 1976 begann eine neue Etappe in der Geschichte der Kryptografie: die weltweite Nutzung eines Standardverfahrens für die Verschlüsselung.

Die Kosten für die zivile Anwendung von Chiffren wären sehr hoch, wenn Unternehmen ein kryptografisches Verfahren für jede Nutzung individuell konfigurieren müssten. In den 1970er Jahren schickten Banken beispielsweise einen speziell beauftragten Kurier zu wichtigen Kunden, um ihnen den zur Entschlüsselung von Nachrichten nötigen Schlüssel zu überreichen. Mit dem Wachstum der Banken nahm die Anzahl dieser Schlüssel jedoch immer mehr zu und ihre Auslieferung wurde zum administrativen Albtraum für die Banken. Die Public-Key-Chiffrierung könnte dieses Problem lösen.

Die Veröffentlichung des DES-Algorithmus war ein Meilenstein in der Geschichte der Kryptografie, doch hinsichtlich der Schlüssel unterscheidet DES sich nicht wesentlich von der Cäsar-Chiffre. Beide sind symmetrische Verfahren, das heißt derselbe Schlüssel wird zur Ver- und Entschlüsselung verwendet. Die wichtigste Schwachstelle solcher Verfahren ist die Übermittlung des Schlüssels.

Die Public-Key-Verschlüsselung

Bailey Whitfield Diffie, Martin Hellman und Ralph Merkle sahen das Zeitalter der Computervernetzung voraus und setzten sich das Ziel, das schon seit der Cäsar-Chiffre bekannte Problem der Schlüsselübertragung endgültig zu lösen. Auf einer nationalen Computerkonferenz in den USA 1976 stellten sie die Public-Key-Verschlüsselung vor. Diese nutzt ein aus einem öffentlichen und einem privaten Schlüssel bestehendes Schlüsselpaar zur asymmetrischen Verschlüsselung und macht so die Überlieferung von Schlüsseln überflüssig. Der öffentliche, für die Verschlüsselung verwendete Schlüssel ist allgemein zugänglich. Der zur Entschlüsselung verwendete private Schlüssel ist dagegen nur dem Empfänger bekannt.

Der Diffie-Hellman-Merkle-Schlüsselaustausch nutzt eine Funktion aus der modularen Arithmetik, $Y=A^x \pmod B$. Diese Funktion besagt, dass bei der Teilung von A^X durch B ein Rest Y bleibt. Sie ist eine sogenannte Einwegfunktion, dass heißt, die Ausgangswerte lassen sich nicht oder nur mit sehr großem Aufwand ermitteln, auch wenn die Funktion und das Ergebnis bekannt sind. Die Kommunikationspartner nutzen diese Funktion wie folgt, um den öffentlichen Schlüssel zu berechnen:

- **Die Werte A und B sind Sender und Empfänger bereits bekannt (z. B. A = 7 und B = 11).**
- **Sender und Empfänger haben je einen Wert für X (z. B. X = 3 und x = 6).**
- **Sender und Empfänger berechnen Y unabhängig voneinander anhand der Funktion $Y = A^X \pmod B$. In unserem Beispiel ergibt das Y = 2 und y = 4.**
- **Sender und Empfänger übermitteln ihre Werte für Y aneinander.**
- **Beide setzen ihren eigenen X-Wert und den Y-Wert des anderen in die Formel $Y^X \pmod B$ ein, um einen gemeinsamen Schlüssel zu erhalten. In unserem Beispiel: $Y^x \pmod{11} = 2^6 \pmod{11} = 9$, $y^X \pmod{11} = 4^3 \pmod{11} = 9$**

Mit diesem Verfahren kann die Vertraulichkeit einer über das Internet übertragenen Mitteilung gesichert werden. Diese revolutionäre Erfindung setzte eines der Grundprinzipien der Kryptografie außer Kraft: Der Schlüsselaustausch musste nun nicht mehr im Geheimen erfolgen.

Zu dieser Zeit gab es noch keine Einwegfunktion, die die asymmetrische Ver- und Entschlüsselung mit verschiedenen Schlüsseln ermöglichte. Die Idee konnte also nicht sofort praktisch umgesetzt werden. Diese Lücke wurde durch die Entwicklung der RSA-Chiffre geschlossen.

Die RSA-Chiffre

Das zur Umsetzung des von Diffie, Hellman und Merkle vorgeschlagenen Konzepts nötige mathematische Verfahren wurde von Ronald L. Rivest, Adi Shamir und Leonard M. Adleman am Massachusetts Institute of Technology entwickelt. Der Name dieses Verfahrens zur Public-Key-Verschlüsselung, RSA-Verschlüsselung, leitet sich von den Anfangsbuchstaben der Nachnamen der drei Forscher ab. Die Methode beruht auf der Primfaktorzerlegung großer Zahlen, wie in diesem Beispiel:

95 = 5 × 19
851 = 23 × 37
176653 = 241 × 733
9831779 = 2011 × 4889

In der Public-Key-Verschlüsselung wird die Zahl links des Gleichheitszeichens als öffentlicher und Teil des privaten Schlüssels genutzt. Wenn die Primfaktoren rechts des Gleichheitszeichens sehr große Zahlen sind, ist es schwierig, die Zerlegung in einem realistischen Zeitraum auszuführen. Die mathematische Erläuterung geht über den Rahmen dieses Whitepapers hinaus, aber die Ermittlung des privaten Schlüssels anhand des öffentlichen Schlüssels ist aufgrund der Besonderheiten der Primfaktorzerlegung in der Praxis schwierig.

Historisch interessant ist, dass ein britischer Kryptograf schon vor der Veröffentlichung der RSA-Chiffre einen Algorithmus für die Public-Key-Verschlüsselung entwickelt hatte. Da neue Chiffren zu dieser Zeit jedoch Staatsgeheimnisse waren, blieb dieses äquivalente Verfahren bis 1997 streng geheim.

Die Public-Key-Verschlüsselung ist ein sehr bequemes Verfahren, da der Schlüsselaustausch über das Internet erfolgen und dennoch nur der legitime Empfänger die Nachrichten entschlüsseln kann. Anders ausgedrückt wird das Jahrtausende alte Problem der Schlüsselübertragung mit dieser Methode auf elegante Weise gelöst. Die Entschlüsselung des privaten Schlüssels würde für praktische Zwecke einfach zu lange dauern, auch wenn der öffentliche Schlüssel über das Internet übertragen wird und damit für sehr viele Menschen lesbar ist.

Das folgende einfache Beispiel illustriert, wie über das Internet zu übertragende Daten mit einer Kombination aus der symmetrischen und Public-Key-Verschlüsselung (RSA-Chiffre) von jedermann verschlüsselt werden können. Secure Sockets Layer (SSL) ist ein Protokoll für die sichere Kommunikation zwischen Webserver und -client, das von Netscape Communications eingeführt und in Netscape Navigator eingebunden wurde.

SSL zeichnet sich durch die Ausgabe eines elektronischen Zertifikats aus, das die Identität eines Web-, Mail- o. ä. Servers bestätigt. Beim Aufbau einer SSL-Verbindung dient dieses Zertifikat als Beweis, dass man mit dem richtigen Server verbunden ist. Danach werden Zugriffe durch Dritte, Datenlecks und andere Verletzungen der Datensicherheit durch die Verschlüsselung der Nachrichten verhindert.

Symmetrische Schlüssel, bzw. in der Praxis die Zufallszahlen, aus denen der symmetrische Schlüssel berechnet wird, können bei der Public-Key-Verschlüsselung also problemlos übertragen werden. So kann ein verschlüsselter Datenaustausch etabliert werden, ohne dass die Schlüsselübertragung zur Schwachstelle wird.

Der entscheidende Unterschied zur Verschlüsselung mit symmetrischen Schlüsseln ist, dass der Schlüssel bei der Public-Key-Verschlüsselung nicht geheim gehalten werden muss. Da die Verschlüsselung zeitaufwendig ist, wird eine Hybridmethode verwendet. Der Klartext wird mit einem symmetrischen Schlüssel verschlüsselt und dann mittels Public-Key-Verschlüsselung übertragen.

Die Entschlüsselung der DES-Chiffre

Kehren wir noch einmal zur DES-Chiffre zurück, um deren Entschlüsselung genauer zu untersuchen.

Da der DES-Schlüssel aus 56 Bit besteht, gibt es 256, also ungefähr 72 Billiarden (7,2 × 1016) mögliche Kombinationen. Die Entschlüsselung scheint dadurch praktisch unmöglich, gelang 1994 aber dennoch. Mithilfe immer leistungsfähigerer Computer wird die Entschlüsselung moderner Chiffren immer einfacher.

Verbesserungen der SSL-Verschlüsselung

Um trotz zunehmender Rechenleistung die Sicherheit der SSL-Verschlüsselung zu gewährleisten, wurde die vorgeschriebene Mindestlänge für öffentliche SSL-Schlüssel von 1024 auf 2048 Bit erhöht. Darüber hinaus gibt es Bemühungen, einen digitalen Signaturalgorithmus auf der Basis von SHA-2 für öffentliche Schlüssel einzuführen. Ein Grund für diese Entscheidungen ist, dass Browseranbieter und Zertifizierungsstellen sich bei der Ausarbeitung von Zeitplänen und Richtlinien an den Empfehlungen, kryptografischen Normen und Spezifikationen des NIST orientieren. In jüngster Zeit ist SHA-2 in Unternehmen vor allem in Zusammenhang mit PCI DSS im Gespräch, da PCI DSS die Befolgung der NIST-Empfehlungen beinhaltet.

Weitere Informationen über die Umstellung von 1024- auf 2048-Bit-Schlüssel finden Sie unter www.thawte.com/resources/2048-bit-compliance/index.html.

Alle Benutzer von SSL müssen ihre PC-Browser, Mobiltelefone, Smartphones, andere Endgeräte und Webbrowser auf dem neuesten Stand halten, um neue Hash-Algorithmen und Schlüssellängen rasch nutzen zu können und so die Effektivität der Verschlüsselung zu erhalten.

6. Die Zukunft der Chiffren

Es wurde bereits erwähnt, dass die Geschichte der Kryptografie ein ewiger Kreislauf aus der Erfindung und dem Knacken immer neuer Verschlüsselungsverfahren ist. Ein nennenswerter Meilenstein in dieser Entwicklung ist die Quantenkryptografie.

Laut Definition ist ein Quant eine sehr kleine, unveränderliche Energiemenge, in diesem Fall in Form von Licht, also ein Photon. Die Oszillation von Photonen während ihrer Fortbewegung kann zur Datenübertragung genutzt werden. Ein eventueller Lauschangriff wird dabei immer entdeckt, weil die Oszillation nicht störungsfrei gemessen werden kann.

Während Chiffren in der Vergangenheit als sicher galten, wenn sie nicht in einem praktikablen Zeitraum entschlüsselt werden konnten, beruht die Sicherheit von Quantenchiffren also darauf, dass jeder Abhörversuch umgehend bemerkt wird.

7. Wie sicher ist die SSL-Verschlüsselung?

Die Verschlüsselung mit SSL macht die Entschlüsselung nicht unmöglich, sondern lediglich so zeit- und kostenaufwendig, dass sie sich in der Praxis nicht lohnt. Wenn die Verschlüsselungsstärke nicht dem Typ und der Bedeutung der verschlüsselten Daten entspricht, wird die Entschlüsselung für Hacker interessant und damit vermutlich früher oder später erfolgreich.

Es gab in der Geschichte Zeiten, in denen alle bekannten Chiffren geknackt waren und kein effektives Verschlüsselungsverfahren verfügbar war. Infolge der weiten Verbreitung von Computern und des Internets werden heute jedoch unvergleichlich viel mehr Chiffren genutzt als zu jeder früheren Zeit. Wenn es keine effektiven Verschlüsselungsverfahren gäbe, hätte dies ernsthafte negative Auswirkungen auf die Nutzung des Internets.

Die für SSL verwendete Verschlüsselung kann auch in Zukunft effektiv bleiben, wenn die für Browser, Server und SSL-Zertifikate genutzte Verschlüsselungsstärke mit der steigenden Rechenleistung Schritt hält. Wie bei allen Chiffren muss die Verschlüsselungsstärke jedoch ständig erhöht werden, um die Wirksamkeit zu erhalten.

Benutzer und Anbieter müssen sich bewusst sein, dass ausreichende Gegenmaßnahmen notwendig sind, um das Knacken von Chiffren zu verhindern, und dafür sorgen, dass die erforderlichen Schutzvorrichtungen jederzeit aktiv sind.

Literatur

Singh, Simon: The Code Book. Shinchosha Publishing Co. Ltd., 2001