Der Schlüssel zur Verschlüsselung

Ein Überblick über die Geschichte und Entwicklung von kryptografischen Algorithmen und deren Entschlüsselung

digicert®

Inhalt

Einleitung

Verschlüsselung gibt es bereits seit über 5.000 Jahren, doch erst mit der zunehmenden Bedeutung des Internets und dem wachsenden Datenstrom, der Tag für Tag online ausgetauscht wird, hat sie auch im Alltag Einzug gehalten.

Die Geschichte der Chiffren und Verschlüsselung ist spannend: ein ewiger Wettstreit zwischen Kryptografen, die neue kryptografische Algorithmen austüfteln, und Kryptoanalytikern, die sie früher oder später knacken. Dann beginnt der Kreis von Neuem.

Dieses Whitepaper gibt einen Überblick über die Geschichte der Chiffren und die wichtigsten Entwicklungen in der Verschlüsselungstechnik und stellt eine Reihe von Maßnahmen vor, die auch bei modernen Chiffren angewendet werden sollten.

Wie alles begann

Als die ältesten Chiffren der Welt gelten die ägyptischen Hieroglyphen, die bereits um 3000 v. Chr. als Schriftzeichen verwendet wurden und erst im 19. Jahrhundert entziffert werden konnten. Da nur sehr wenige Menschen das Lesen von Hieroglyphen lernten, können sie als eine Art Kryptografie angesehen werden.

Etwa im sechsten Jahrhundert v. Chr. wurden im griechischen Stadtstaat Sparta sogenannte Skytalen zur Verschlüsselung von Botschaften eingesetzt. Dabei schrieb der Absender seine Botschaft auf einen Streifen Pergament, der um einen dicken Stab, die Skytale, gewickelt war (siehe Abbildung 1). Der Pergamentstreifen konnte dann nur von einem Empfänger gelesen werden, der einen Stab desselben Umfangs besaß.

Verfahren wie dieses, bei denen die Reihenfolge der Buchstaben geändert wird, werden als Transpositionsverfahren bezeichnet.

Abbildung 1

Im ersten Jahrhundert v. Chr. entstand dann die Cäsar-Chiffre, benannt nach dem römischen Kaiser Julius Cäsar, der dieses Verfahren häufig verwendete. Bis heute ist sie eine der berühmtesten Techniken der Kryptografie. Dabei wird jeder Buchstabe der Originalnachricht durch den Buchstaben ersetzt, der im Alphabet um eine bestimmte Anzahl von Positionen, die nur dem Sender und Empfänger bekannt ist, versetzt ist.

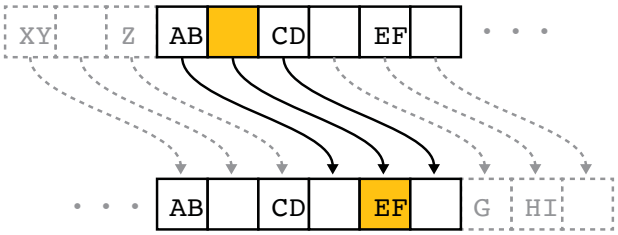

Abbildung 2

Verfahren wie dieses, die Buchstaben im Alphabet verschieben, werden als Verschiebechiffren bezeichnet.

Diese Chiffren können durch das Ausprobieren von höchstens 25 Verschiebungen einfach entschlüsselt werden. Durch die Nutzung zufälliger Zuordnungen 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 verschlüsselt)	ABCDEFGHIJKLMNOPQRSTUVWXYZ
Verschlüsselter Text	SMKRATNGQJUDZLPVYOCWIBXFEH

Ein Verschlüsselungsverfahren, bei dem die Buchstabenfolge nach einem festen Schema verändert wird, wie oben gezeigt, wird als Substitutionsverfahren bezeichnet. Dies ist historisch gesehen die meistverwendete Kryptografiemethode, auf der auch die moderne mechanische Chiffriermaschine Enigma beruhte, auf die unten näher eingegangen wird.

Allerdings können alle Substitutionschiffren, einschließlich der einfacheren Cäsar-Chiffre, mithilfe einer Häufigkeitsanalyse entschlüsselt werden. Dabei wird versucht, von der Häufigkeit der Buchstaben im verschlüsselten Text auf ihr Klartextäquivalent zu schließen. Diese Versuche stützen sich auf linguistische Besonderheiten der Klartextsprache, zum Beispiel:

- Im Deutschen kommen die Buchstaben „e“ und „n“ am häufigsten vor. Im Englischen sind es „e“ und „t“ (siehe Abbildung 3).
- •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.

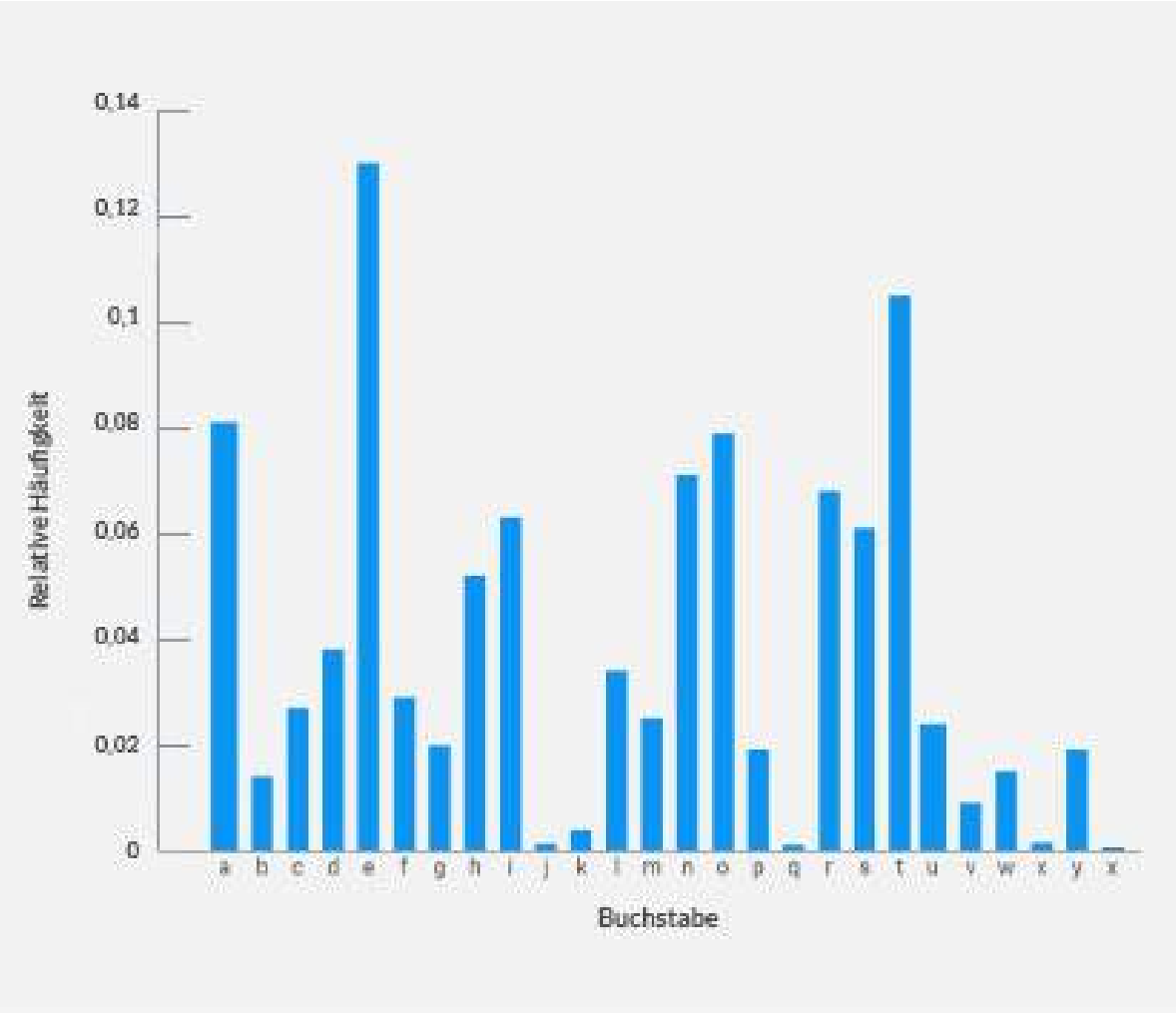

Abbildung 3

Eine Renaissance der Kryptologie

Im Mittelalter kam es im Zuge stark zunehmender diplomatischer Aktivitäten zu einer erheblichen Verfeinerung kryptografischer Verfahren, da die klassischen Chiffren entschlüsselt worden waren und neue erfunden werden mussten, um ein wachsendes Volumen vertraulicher Informationen zu schützen.

Die Chiffre der Maria Stuart

Die von der schottischen Königin Maria Stuart und ihren Mitverschwörern im 16. Jahrhundert benutzte Chiffre war ein sogenannter Nomenklator. Neben dem Austauschen einzelner Buchstaben wurden dabei für häufig verwendete ganze Wörter und Sätze auch Symbole genutzt, die in einem Codebuch festgehalten waren. Allerdings konnte die Schwäche dieser Chiffre, Buchstaben des Klartextes eins zu eins gegen andere Buchstaben auszutauschen, zu ihrer Entschlüsselung ausgenutzt werden. Maria Stuart zahlte einen hohen Preis dafür, als sie des Hochverrats für schuldig befunden und in Fotheringhay Castle hingerichtet wurde, weil sie die Ermordung der Königin Elizabeth I. von England geplant hatte.

Klartext	GOLDMEDAILLE
Schlüssel	OLYMPIAOLYMP
Verschlüsselte Nachricht	UZJPBMDOTJXT

Die Vigenère-Chiffre

Um die Schwächen der Substitutionschiffren zu überwinden und auch auf umfangreiche Codebücher verzichten zu können, entwickelte Leon Battista Alberti im 15. Jahrhundert erstmals ein polyalphabetisches Substitutionsverfahren, bei dem mehrere Substitutionsalphabete benutzt wurden. Damit war der Grundstein für weitere Entwicklungen gelegt, darunter auch die Blaise de Vigenère zugeschriebene endgültige Form der polyalphabetischen Substitutionschiffren, die relativ sichere Vigenère-Chiffre.

Dabei wird ein sogenanntes Vigenère-Quadrat (siehe Abbildung 4) verwendet, um den Klartext, z. B. das Wort „Goldmedaille“, mithilfe eines Schlüsselworts, z. B. „Olympia“, zu verschlüsseln. Ohne das Schlüsselwort ist die Entschlüsselung extrem schwierig, auch wenn die Tabelle in die Hände Dritter fällt.

	AB	CD	EF	GH	IJ	KL	MN	OP	QR	ST	UV	WX	YZ
A	AB	CD	EF	GH	IJ	KL	MN	OP	QR	ST	UV	WX	YZ
B	BC	DE	FG	HI	JK	LM	NO	PQ	RS	TU	VW	XY	ZA
C	CD	EF	GH	IJ	KL	MN	OP	QR	ST	UV	WX	YZ	AB
D	DE	FG	HI	JK	LM	NO	PQ	RS	TU	VW	XY	ZA	BC
E	EF	GH	IJ	KL	MN	OP	QR	ST	UV	WX	YZ	AB	CD
F	FG	HI	JK	LM	NO	PQ	RS	TU	VW	XY	ZA	BC	DE
G	GH	IJ	KL	MN	OP	QR	ST	UV	WX	YZ	AB	CD	EF
H	HI	JK	LM	NO	PQ	RS	TU	VW	XY	ZA	BC	DE	FG
I	IJ	KL	MN	OP	QR	ST	UV	WX	YZ	AB	CD	EF	GH
J	JK	LM	NO	PQ	RS	TU	VW	XY	ZA	BC	DE	FG	HI
K	KL	MN	OP	QR	ST	UV	WX	YZ	AB	CD	EF	GH	IJ
L	LM	NO	PQ	RS	TU	VW	XY	ZA	BC	DE	FG	HI	JK
M	MN	OP	QR	ST	UV	WX	YZ	AB	CD	EF	GH	IJ	KL
N	NO	PQ	RS	TU	VW	XY	ZA	BC	DE	FG	HI	JK	LM
O	OP	QR	ST	UV	WX	YZ	AB	CD	EF	GH	IJ	KL	MN
P	PQ	RS	TU	VW	XY	ZA	BC	DE	FG	HI	JK	LM	NO
Q	QR	ST	UV	WX	YZ	AB	CD	EF	GH	IJ	KL	MN	OP
R	RS	TU	VW	XY	ZA	BC	DE	FG	HI	JK	LM	NO	PQ
S	ST	UV	WX	YZ	AB	CD	EF	GH	IJ	KL	MN	OP	QR
T	TU	VW	XY	ZA	BC	DE	FG	HI	JK	LM	NO	PQ	RS
U	UV	WX	YZ	AB	CD	EF	GH	IJ	KL	MN	OP	QR	ST
V	VW	XY	ZA	BC	DE	FG	HI	JK	LM	NO	PQ	RS	TU
W	WX	YZ	AB	CD	EF	GH	IJ	KL	MN	OP	QR	ST	UV
X	XY	ZA	BC	DE	FG	HI	JK	LM	NO	PQ	RS	TU	VW
Y	YZ	AB	CD	EF	GH	IJ	KL	MN	OP	QR	ST	UV	WX
Z	ZA	BC	DE	FG	HI	JK	LM	NO	PQ	RS	TU	VW	XY

Abbildung 4

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 5).

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 5

Krieg der Chiffren

Aufgrund der Fortschritte in der Kommunikationstechnik gewannen die Kryptografie und Kryptoanalyse im Ersten Weltkrieg an Bedeutung.

Kappung der deutschen Seekabel

Als Großbritannien 1914 in den Krieg eintrat, durchschnitt die britische Marine die deutschen Kommunikationsseekabel im Ärmelkanal, sodass das deutsche Militär Nachrichten nach Übersee nur über internationale Seekabel, und damit über Großbritannien, oder per Funkübertragung senden konnte. Danach wurden alle abgefangenen Nachrichten an eine eigens geschaffene kryptoanalytische Abteilung im britischen Marineministerium, den sogenannten Room 40 (Zimmer 40), weitergeleitet. Dort wurde die deutsche Chiffre entschlüsselt.

Die Zimmermann-Depesche

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. Ein Telegramm von Zimmermann mit entsprechenden Anweisungen an den deutschen Botschafter in Mexiko wurde im „Room 40“ entschlüsselt. Die Briten veröffentlichten die entschlüsselte Nachricht jedoch nicht, um zu vermeiden, dass Deutschland eine neue, sicherere Chiffre entwickeln würde. Erst nachdem sie eine Klartextversion des Telegramms beschaffen konnten, veröffentlichten sie dieses und lösten damit die amerikanische Kriegserklärung an Deutschland aus.

Die ADFGVX-Chiffre

Die von Fritz Nebel, einem Oberst der deutschen Armee, entwickelte ADFGX-Chiffre wurde ab 1918 verwendet. Ähnlich wie die Uesugi-Chiffre basierte sie auf einem Polybios-Quadrat, dessen Zeilen und Spalten mit den Buchstaben ADFGX beschriftet sind. Jeder Buchstabe wurde als das Buchstabenpaar verschlüsselt, das seine Zeilen- und Spaltenposition in

der Tabelle angibt. Dann wurde das Ergebnis jedoch mithilfe eines Transpositionsverfahren nochmals verschlüsselt. Im Laufe der Zeit wurde die ADFGX-Chiffre durch die ADFGVX-Chiffre abgelöst, die auf einer Tabelle mit je sechs Zeilen und Spalten basierte (siehe Abbildung 6).

	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 6

Wenn die als Schlüssel dienenden Tabellen jeweils nur einmal verwendet werden, ist es praktisch unmöglich, diese Chiffre zu knacken. Dazu müsste allerdings eine große Anzahl dieser Schlüssel weitergeleitet werden, was insbesondere in Gefechtssituationen an der Front kaum umsetzbar ist.

Das Zeitalter der Enigma

Die Einführung mechanischer Chiffriermaschinen Anfang des 20. Jahrhunderts machte es möglich, selbst extrem komplexe Chiffren zu entschlüsseln, begünstigte aber gleichzeitig auch die Entwicklung neuer ausgefeilterer Verschlüsselungsmethoden.

1918 entwickelte der deutsche Ingenieur Arthur Scherbius die als Enigma vermarktete Produktreihe tragbarer und besonders sicherer mechanischer Chiffriermaschinen. Da der deutschen Armee noch nicht bekannt war, dass ihre im Ersten Weltkrieg benutzte Chiffre geknackt worden war, bestand wenig Interesse an einer teuren Aufrüstung ihrer Verschlüsselungstechnologie, und die Enigma wurde zunächst nicht eingeführt. Dies änderte sich jedoch, als die Erkenntnis durchdrang, dass die Entschlüsselung der deutschen Chiffren durch die Briten maßgeblich zur Niederlage beigetragen hatte.

Die Enigma nutzte ein polyalphabetisches Substitutionsverfahren. Das Gerät bestand aus einer als „Zerhacker" bezeichneten Anordnung mehrerer Rotoren, die mit den 26 Buchstaben des Alphabets beschriftet waren, und einem Steckfeld, mit dem einzelne Buchstabenpaare miteinander vertauscht werden konnten. Der Text wurde über eine Tastatur eingegeben, was die Ver- und Entschlüsselung vereinfachte. Nach jeder Eingabe eines Buchstaben drehte sich die Rotorenanordnung des Zerhackers um eine Position weiter, sodass sich der Schlüssel mit jedem eingegebenen Buchstaben änderte.

Angesichts der aus Deutschland drohenden Invasionsgefahr arbeitete Polen zeitgleich an der Entwicklung einer „Bomba" genannten Entschlüsselungsmaschine. Verbesserungen an der Enigma erhöhten jedoch die Anzahl der möglichen Verschlüsselungsmuster und Polen stellte aus wirtschaftlichen Gründen seine Kryptoanalyseforschung ein. Seine Forschungsergebnisse und Entwicklungsarbeit übergab Polen 1939, zwei Wochen vor dem Ausbruch des Zweiten Weltkriegs, an Großbritannien. Auf dieser Grundlage war es Großbritannien schließlich möglich, die von der deutschen Wehrmacht verwendeten Enigma-Codes zu knacken.

Die dadurch ermöglichte Entschlüsselung der deutschen Kommunikation durch die Spezialgruppe „Ultra" war bis zum Kriegsende eine wichtige Informationsquelle der Alliierten. Dieser Durchbruch blieb jedoch streng geheim, damit sich die deutsche Wehrmacht in Sicherheit wiegen und die Enigma weiterhin verwenden würde. Erst 1974 wurde öffentlich bekannt, dass die Enigma geknackt worden war.

Die Anfänge des Computerzeitalters

Ab dem Zweiten Weltkrieg wurden Maschinen für die Ver- und Entschlüsselung durch Computer ersetzt. Auch durch die rasche Verbreitung von Computern in der freien Wirtschaft hat die Kryptografie für geschäftliche Transaktionen, andere zivile Anwendungen und das Militär an Bedeutung gewonnen.

Die DES-Chiffre

Im Jahr 1973 schrieb das Normenbüro des US-amerikanischen Wirtschaftsministeriums (NBS), das später in National Institute of Standards and Technology (NIST) umbenannt wurde, die Entwicklung eines kryptografischen Verfahrens für den Standardgebrauch aus, bei dem der Verschlüsselungsalgorithmus offengelegt wird. Mit dem DES-Algorithmus (Data Encryption Standard), der 1976 durch das NBS angenommen wurde, war ein Verschlüsselungsverfahren geboren, das sich rasch zum weltweiten Standard entwickelte.

Dies war der Wendepunkt in der Geschichte der Kryptografie und insbesondere ihrer zivilen Nutzung. Unternehmen bot DES eine kostengünstige und praktikable Methode zur Ver- und Entschlüsselung vertraulicher Informationen mit symmetrischen Schlüsseln – nicht wesentlich anders als mit der Cäsar-Chiffre.

Public-Key-Verschlüsselung

Die Entwicklung der Public-Key-Verschlüsselung löste schließlich auch das zentrale Problem, das schon seit der Cäsar-Chiffre bekannt war: Wie kann der Schlüssel weitergegeben werden? Die 1976 von Bailey Whitfield Diffie, Martin Hellman und Ralph Merkle vorgestellte Public-Key-Verschlüsselung macht die Überlieferung von Schlüsseln per Bote oder Briefpost überflüssig und erleichtert somit die verschlüsselte Kommunikation. Dazu nutzt sie einen öffentlich zugänglichen Schlüssel zur Verschlüsselung und einen privaten Schlüssel, der nur dem Empfänger bekannt ist, zur Entschlüsselung.

Der Diffie-Hellman-Merkle-Schlüsselaustausch nutzt eine Funktion aus der modularen Arithmetik, die es ermöglicht, die Vertraulichkeit einer über das Internet übertragenen Mitteilung zu sichern. 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 jedoch noch keine Einwegfunktion, die die asymmetrische Ver- und Entschlüsselung mit verschiedenen Schlüsseln ermöglichte. 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. Die Bezeichnung RSA-Verschlüsselung leitet sich von den Anfangsbuchstaben der Nachnamen der drei Forscher ab.

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 Verfahren bis 1997 streng geheim.

Die RSA-Verschlüsselung beruht auf der Zerlegung großer Zahlen in Primfaktoren, die als öffentlicher Schlüssel und Teil des privaten Schlüssels verwendet werden, wie in diesem Beispiel:

95=5 × 19

851=23 × 37

176653=241 × 733

9831779=2011 × 4889

Aufgrund der Besonderheiten der Primfaktorzerlegung ist die Ermittlung des privaten Schlüssels anhand des öffentlichen Schlüssels innerhalb eines realistischen Zeitrahmens schwierig. Damit bleibt die Entschlüsselung auch beim offenen Austausch des öffentlichen Schlüssels nur dem beabsichtigten Empfänger möglich.

Transport Layer Security und Secure Sockets Layer (TLS/SSL) sind zum Beispiel Protokolle für die sichere Kommunikation zwischen Webserver und -client, die von Netscape Communications eingeführt und in Netscape Navigator eingebunden wurden. TLS/SSL zeichnet sich durch die Ausgabe eines elektronischen Zertifikats aus, das die Identität eines Web-, Mail- o. ä. Servers ausdrücklich bestätigt. Danach werden Zugriffe durch Dritte, Datenlecks und andere Verletzungen der Sicherheit der über das Internet ausgetauschten Daten durch die Verschlüsselung der Nachrichten mit einem symmetrischen Schlüssel verhindert, der mittels Public-Key-Verschlüsselung sicher ausgetauscht wurde.

Alternativen zu RSA

1. **Digital Signature Algorithm**
   Der Digital Signature Algorithm (DSA) ist ein von der US-Regierung genehmigter und zertifizierter Verschlüsselungsalgorithmus, der 1991 von der nationalen Sicherheitsbehörde NSA als Alternative zum derzeitigen Standard RSA entwickelt wurde. Er bietet das gleiche Sicherheits- und Leistungsniveau wie RSA, verwendet zur Signierung und Verschlüsselung jedoch einen anderen, seltener verwendeten mathematischen Algorithmus. Ein DSA-Schlüsselpaar hat dieselbe Größe wie ein äquivalenter RSA-Schlüssel, dennoch sind die Schlüsselerzeugung und digitale Signierung mit DSA schneller. Der Nachteil ist, dass die Schlüsselverifizierung etwas langsamer erfolgt.

2. **Elliptische-Kurven-Kryptografie**
   Die Elliptische-Kurven-Kryptografie (ECC) basiert auf einer algebraischen Struktur elliptischer Kurven über endlichen Feldern. Während RSA ausnutzt, dass es mathematisch äußerst schwierig ist, eine große ganze Zahl aus zwei oder mehr Primfaktoren in diese zu zerlegen, liegt ECC die Unmöglichkeit zugrunde, anhand eines öffentlich bekannten Basispunktes den diskreten Logarithmus eines zufälligen Elements einer elliptischen Kurve zu ermitteln. In der aktuellen Kryptografie ist eine elliptische Kurve eine ebene Kurve aus Punkten, die die Gleichung $y^2 = x^3 + ax + n$ erfüllen, zusammen mit einem konkreten Punkt im Unendlichen (∞). Die Koordinaten sind hier aus einem feststehenden, endlichen Feld der Charakteristik ungleich 2 oder 3 zu wählen, sonst wird die Kurvengleichung etwas komplexer. Diese Menge in Kombination mit der Gruppenoperation der elliptischen Gruppentheorie bildet eine Abelsche Gruppe, wobei der Punkt im Unendlichen als neutrales Element dient. Die Struktur der Gruppe ergibt sich aus der Teilergruppe der zugrunde liegenden algebraischen Varietät.

   Auf der RSA Conference 2005 stellte die nationale Sicherheitsbehörde NSA die Suite B vor, die zur Erzeugung digitaler Signaturen und für den Schlüsselaustausch ausschließlich ECC verwendet. Mit der Suite sollen sowohl als geheim eingestufte als auch nicht als geheim eingestufte nationale Sicherheitssysteme und Informationen geschützt werden.

3. **NIST-Empfehlung zur Schlüssellänge**
   NIST steht für „National Institute of Standards and Technology“, eine US-Bundesbehörde, die im technischen Bereich mit der Industrie zusammenarbeitet, um Technologien, Maße und Normen zu entwickeln und durchzusetzen. NIST-Empfehlungen sind ein Teil des Rahmenwerks von Standards und Normen, die Webbrowser und Zertifizierungsstellen (CA) einhalten.

Minimum size (bits) of Public Keys				Key Size Ratio
Security (bits)	DSA	RSA	ECC	RSA/DSA to ECC
112	2048	2048	N/A	1:09
128	3072	3072	256-383	1:12
192	7680	7680	384-511	1:20

Die praktischen Vorteile kürzerer Schlüssel gegenüber längeren Schlüsseln mit dem gleichen Sicherheitsniveau sind eine Verbesserung der Serverleistung und eine größere Zahl gleichzeitig möglicher Verbindungen bei gleichzeitiger Verringerung der CPU-Belastung.

Eine nie endende Herausforderung

DES-Schlüssel sind 56 Bit lang, d. h. es gibt 256 oder ungefähr 70 Billiarden (7×10^{16}) mögliche Kombinationen. Eine Entschlüsselung war damit zunächst praktisch unmöglich, gelang 1994 aber dennoch infolge des enormen Anstiegs der Rechenleistung von Computern.

In ganz ähnlicher Weise ist es auch nicht unmöglich, den kryptografischen Algorithmus von TLS/SSL zu knacken – nur wäre dies mit der Rechenleistung heutiger Computer so zeitaufwendig und teuer, dass die Entschlüsselung faktisch unmöglich ist. Um TLS/SSL ein ähnliches Schicksal wie DES zu ersparen, wurde die Spezifikation für die Länge des öffentlichen Schlüssels von 1024 Bit auf 2048 Bit erhöht. Ein neuer Trend hin zu einer digitalen SHA-2-Signatur für öffentliche TLS/SSL-Schlüssel hat in jüngerer Zeit ebenfalls Fahrt aufgenommen, da Unternehmen sich an die Anforderungen des Datenschutzstandards für Zahlungskarten (Payment Card Industry Data Security Standard; PCI DSS) anpassen.

Nutzer von TLS/SSL-Verschlüsselung haben ihre PC-Browser, Webbrowser, Mobilgeräte und anderen Clientgeräte auf den neuesten Stand gebracht, um neue Hashfunktionen und Schlüssellängen schneller nutzen zu können. Die Aufrechterhaltung einer starken Verschlüsselung hat jedoch Priorität.

Das NIST erkannte die Grenzen der für TLS/SSL verwendeten Zertifikate mit einem 1024 Bit langen RSA-Schlüssel und setzte Januar 2014 als Frist für die Umstellung auf Zertifikate mit 2048 Bit.

Leistungsfähigere Computer und neue Techniken machen Schlüssel einer bestimmten Länge immer angreifbarer. Mit der Umstellung auf Zertifikate mit 2048 Bit konnte vielen dieser Risiken begegnet werden. Allerdings kann sich die Erhöhung der RSA-Schlüssellänge auch negativ auf die Serverbelastung und die Zahl der gleichzeitig möglichen Verbindungen auswirken. Eine Alternative bietet die Elliptische-Kurven-Kryptografie (ECC), bei der öffentliche und private Schlüssel anhand von Punkten auf einer Kurve erstellt werden. ECC ist kaum mit Brute-Force-Angriffen zu knacken und potenziell trotz eines geringeren Ressourcenbedarfs schneller als RSA-Verschlüsselung.

Wie alle Chiffren können die für TLS/SSL genutzten Algorithmen nur dann weiterhin Schutz bieten, wenn Browser, Server und TLS/SSL-Serverzertifikate mit der wachsenden Verschlüsselungsleistung Schritt halten. Daher ist es wichtig, dass sich Nutzer und Anbieter gleichermaßen bewusst sind, dass diese Chiffren entschlüsselt werden können, wenn nicht Sorge getragen wird, dass die geeigneten Schutzmaßnahmen zuverlässig umgesetzt werden. Denn das hätte ernsthafte Folgen für die Nutzung des Internets an und für sich.

Gute Aussichten

Wie dargelegt wurde, ist die Geschichte der Kryptografie ein Kreis der Erfindung neuer Verschlüsselungsalgorithmen, gefolgt von der Erfindung neuer Entschlüsselungsmethoden. Ein bemerkenswerter Meilenstein in diesem Prozess ist die Quantenkryptografie, bei der Daten als Drehwinkel von Photonen verschlüsselt werden.

Während bei herkömmlichen Verschlüsselungsmethoden der Zeitfaktor entscheidend war, um sie praktisch nicht entschlüsselbar zu machen, gilt die Quantenkryptografie als nicht entschlüsselbar, weil beim Abfangen der Daten der Drehwinkel der Photonen verändert wird, was leicht festzustellen ist.

Verweise

Simon Singh: The Code Book; Shinchosha Publishing Co., Ltd. 2001 (deutsche Übersetzung: Geheime Botschaften; dtv 2014)

http://freemasonry.bcy.ca/texts/templars_cipher.html
http://www.nsa.gov/ia/programs/suiteb_cryptography/
http://www.nsa.gov/public_info/_files/cryptologic_spectrum/early_history_nsa.pdf

Wenn Sie weitere Informationen wünschen, schreiben Sie unseren Sicherheitsexperten unter contactus@digicert.com

Nord- und Südamerika

Lehi, Utah, USA
2801 North Thanksgiving Way, Lehi, Utah 84043, USA

Mountain View, Kalifornien, USA
485 Clyde Ave., Mountain View, California 94043, USA

Asien-Pazifik und Japan

Bangalore, Indien
RMZ Eco World, 10th Floor, 8B Campus,
Marathalli Outer Ring Road, Bangalore - 560103, Indien

Melbourne, Australien
437 St Kilda Road, Melbourne, 3004, Australien

Tokio, Japan
Ginza Six 8F, 6-10-1 Ginza Chuo-Ku, Tokio,
104-0061, Japan

Europa, Naher Osten und Afrika (EMEA)

Nieuwegein, Niederlande
Nevelgaarde 56 Noord, 3436 ZZ Nieuwegein, Niederlande

Kapstadt, Südafrika
Gateway Building, Century Blvd & Century Way 1,
Century City, 7441, Kapstadt, Südafrika

Dublin, Irland
Block 21 Beckett Way, Park West Business Park,
Dublin 12, D12 C9YE, Irland

St. Gallen, Schweiz
Poststrasse 17, St. Gallen, Schweiz, 9000

London, GB
7th Floor, Exchange Tower, 2 Harbour Exchange Square,
London, E14 9GE, Großbritannien

Mechelen, Belgien
Schaliënhoevedreef 20T, 2800 Mechelen, Belgien

München, Deutschland
Ismaninger Straße 52, 81675 München, Deutschland

digicert®

© 2019 DigiCert, Inc. Alle Rechte vorbehalten. DigiCert ist eine eingetragene Marke von DigiCert, Inc. in den USA und in anderen Ländern. Alle anderen Marken und eingetragenen Marken sind das Eigentum ihrer jeweiligen Inhaber.