Proseminar: „Computer Science“
Dozent: Prof. M. Hofmann
Referent: Mario Kaczmarek
14.01.2005

Kryptographische Protokolle

„Wer den kleinsten Teil seines Geheimnisses hingibt, hat den anderen nicht mehr in der Gewalt.“[J.P.F. Richter, 1763 - 1825, dt. Schriftsteller] [z]

1. Kryptographie im Altertum

Kryptographie, also die Wissenschaft von der Verschlüsselung von Informationen, existiert bereits seit Jahrhunderten und hatte besonders in Kriegszeiten einen gewichtigen Einfluss auf die Entscheidung über Sieger und Verlierer. Sie gehört, wie die Kryptoanalyse, d.h. die Wissenschaft der Entschlüsselung von Informationen, zur Kryptologie. Die Kryptographie hat im Wesentlichen 4 Ziele:

- Vertraulichkeit:

Nur dem gewünschten Adressaten sollte es möglich sein, die Information zu entschlüsseln.

- Authentizität:

Der Absender sollte vom Empfänger eindeutig identifiziert werden können.

- Integrität:

Sie gewährleistet die Unverfälschtheit der Information während der Informationsübertragung.

- Verbindlichkeit:

Der Absender sollte nicht bestreiten können, dass er die Nachricht gesendet hat.

Die einfachste Variante eine Nachricht relativ sicher zum Empfänger zu bringen, die häufig im Altertum eingesetzt wurde, ist die Steganographie. Dieses Verfahren, wo verborgen wird, dass eine Botschaft überhaupt existiert, zählt zwar nicht zur Kryptographie. Sie soll dennoch kurz erwähnt werden. Sie wurde schon vom „Vater der Geschichtsschreibung“ (nach Cicero, römischer Staatsmann, 106 - 43 v. Chr.) dem griechischen Weltreisenden und Historiker Herodot (485 – 425 v. Chr.) beschrieben. So beschreibt Herodot zum Beispiel folgende steganographische Vorgehensweise:
Einem Boten wurde der Kopf rasiert und die Nachricht auf seine Kopfhaut gebrannt. Nachdem das Haar genügend nachgewachsen war, konnte der Bote die Nachricht sicher überbringen, vorausgesetzt, ein möglicher Feind wusste nichts von diesem Verfahren und der Bote ließ nichts von seiner eigentlichen Aufgabe erkennen.
Ein weiteres Prinzip der Steganographie ist der Gebrauch der „unsichtbaren Tinte“:
Bereits vor zwei Tausend Jahren beschrieb der römische Schriftsteller Plinius der Ältere (23/24 – 79 n. Chr.), dass die Milch der Thithymallus-Pflanze als unsichtbare Tinte verwendet werden kann. Nach dem Trocknungsvorgang ist sie durchsichtig, doch durch leichte

Erwärmung bekommt sie eine, durch die Verbrennung von Kohlenstoff hervorgerufene, Braunfärbung.
Die Steganographie eignet sich nur dann, wenn der Feind keine Ahnung vom Einsatz des steganographischen Verfahrens hat bzw. es ihm nicht ersichtlich ist, dass ein solches Verfahren angewandt wurde.
Daher kommen wir nun zu den kryptographischen Verfahren:

1.1 Transposition (Permutation)

Dieses Verfahren ordnet die Buchstaben einer Nachricht anders an. Bei kurzen Botschaften ist dieses Verfahren unsicher, da die Anzahl der möglichen Kodierungen sehr beschränkt ist. Mit steigender Buchstabenanzahl explodieren die Möglichkeiten, die Buchstaben umzustellen.
Ein einfaches Beispiel ist die Gartenzaun-Variante:
Die Nachricht wird abwechselnd auf zwei oder mehr Zeilen geschrieben. Den Geheimtext erhält man, indem die Zeilen nacheinander angehängt werden.
Bsp.:

Klartext: computer science
Transposition: C M U E S I N E
O P T R C E C
Geheimtext: CMUESINE OPTRCEC

Zur Entschlüsselung der Nachricht wendet der Empfänger das Verfahren umgekehrt an. Für einen feindlichen Angreifer ist es schwierig, aber nicht unmöglich, ohne Kenntnis des Verfahrens einen Rückschluss auf die eigentliche Nachricht zu schließen.
Für militärische Zwecke war die Skytale geeignet:
Ein kantiger Holzstab wird mit Papierstreifen (früher Pergament) umwickelt. Will der Sender eine Nachricht verschlüsseln, so schreibt er diese auf den Stab. Nachdem er fertig ist, wird der Streifen abgewickelt und die Nachricht in eine unsinnige Buchstabenkombination transformiert.
Der Empfänger wickelt den Papierstreifen auf ein identisches Exemplar des Holzstabes und erhält somit die eigentliche Mitteilung.

1.2 Substitution

Bei der Substitution wird ein Buchstabe des Alphabetes durch einen beliebig anderen ersetzt. Kryptographen sprechen hier von einer Chiffrierung. Der umgangssprachlich oft verwendete Begriff der Kodierung wird in der Kryptographie nur für die Substitution von Wörtern durch andere Wörter oder Symbole verwendet. Mathematisch gesehen ist die Substitution eine bijektive Abbildung.

Bsp.:

Klartext: „kryptographie" a=D, e=H, g=A, h=Z, i=B, k=R, o=Y, p=E, r=W, t=G, y=U

Geheimtext: „RWUEGYAWDEZBH"

In der Kryptographie ist es üblich, den Klartext, d.h. die zu verschlüsselnde Botschaft, aus Kleinbuchstaben zusammenzusetzen und den Geheimtext, also die verschlüsselte Nachricht, aus Großbuchstaben aufzubauen.

Zur Dechiffrierung benötigt der Empfänger dieselbe Substitutionsliste, die den Schlüssel für die Chiffrierung und Dechiffrierung darstellt, wie der Sender.

Ein schematisches, substitutionelles Verfahren ist die Caesar-Verschiebung:

Caesar baute seine Substitutionsliste so auf, dass jeder Buchstabe des Klartextalphabetes im Geheimtextalphabet durch den Buchstaben ersetzt wurde, der 3 Stellen weiter folgt.

Klartextalphabet: abcdefghijkl...z

Geheimtextalphabet: DEFGHI...C

Mit der Cesar-Verschiebung (oder kurz Caesar) lassen sich somit 25 unterschiedliche Geheimtextalphabete erstellen, wenn Verschiebungen von 1 bis 25 Stellen angewendet werden.

Verwendet der Kryptograph eine allgemeine Substitutionsmethode, die es ihm gestattet, jeden Buchstaben des Klartextalphabetes durch jeden beliebigen Buchstaben im Geheimtextalphabet zu ersetzen, gibt es eine immense Anzahl von möglichen Schlüsseln.

Die Kryptographen hatten eine Methode entwickelt, die ihnen gegenüber den Kryptoanalytikern einen riesigen Vorteil verschaffte, da es bis zum Mittelalter nicht gelungen war, durch logische Schlussfolgerungen die Schlüsselanzahl zu reduzieren und somit das Verfahren angreifbar zu machen.

2. Kryptographie im Mittelalter

Bevor ich mich mit einer genialen kryptographischen Methode befasse, die in einer der dunkelsten geschichtlichen Epochen das Licht der Welt erblickte, streife ich kurz das Gebiet der Kryptoanalyse.

Wie bereits erwähnt, war es den Kryptographen mittels der Substitution gelungen, Nachrichten sicher zu verschlüsseln. Dies änderte sich, als im neunten Jahrhundert die Kryptoanalyse von den Arabern erfunden wurde. Arabische Gelehrte erkannten, dass die unterschiedliche Häufigkeit von Buchstaben in Nachrichten zur Entschlüsselung von Geheimschriften benutzt werden konnte. Das Verfahren der Häufigkeitsanalyse zur Decodierung von Geheimschriften ohne Kenntnis des Schlüssels wurde vom Gelehrten Al-Kindi beschrieben. Vorraussetzung zur Anwendung der Häufigkeitsanalyse ist die Kenntnis der Sprache, in der die Nachricht verfasst wurde, denn die Häufigkeit der Buchstaben ist von Sprache zu Sprache unterschiedlich. So ist im Arabischen „a“ bzw. „l“ am Häufigsten anzutreffen, während im Deutschen „e“ und „n“ und im englischen Sprachraum „e“ und „t“ die häufigsten Vertreter sind.

Buchstabe	**Deutsch**	**Englisch**
e	17,4 %	12,7 %
n	9,8 %	6,7 %
i	7,6 %	7,0 %
t	6,2 %	9,1 %
a	6,5 %	8,2 %

Ist die Sprache bekannt, in der die Nachricht verfasst wurde, so zählt man die Häufigkeit der einzelnen Buchstaben. Bei längeren Nachrichten ist es wahrscheinlich, dass der Buchstabe, der am Häufigsten im Geheimtext auftaucht, mit dem „e“ bzw. „a“, abhängig von der Sprache übereinstimmt. Man ersetzt nun den häufigsten „Geheimtextbuchstaben“ durch den vermuteten Klartextbuchstaben. Danach sucht man nach Buchstabenpaaren (Bigramme), die häufig auftreten („al“ im Arabischen, „ei“ im Deutschen). Damit ist es möglich weitere Geheimtextbuchstaben durch Klartextbuchstaben zu ersetzen. Schließlich bildet man Trigramme um weitere Buchstaben zu finden. Dieses Verfahren ist besonders für umfangreiche Nachrichten geeignet.

Durch diesen geschickten Schachzug war es den Kryptoanalytikern gelungen, die mittels Substitution verschlüsselten Texte zu entschlüsseln.
Jahrhundertelang wurde die monoalphabetische Verschlüsselung benutzt, d.h. es wurde nur ein Geheimtextalphabet verwendet. Durch die Häufigkeitsanalyse war diese Methode jedoch zunehmend unsicher. Die Rettung für die Kryptographen erfolgte im 15. Jahrhundert.

2.1 Vigenere-Verschlüsselung

Mitte des 15. Jahrhunderts kam dem Italiener Alberti die Idee, ein neues Substitutionsverfahren zu entwickeln. Statt wie bisher ein Geheimtextalphabet zu verwenden, wollte Alberti zwei oder mehr Geheimtextalphabete nutzen (polyalphabetische Verschlüsselung). Jedoch vollendete Alberti diese geniale Idee nicht. Im Zeitraum von hundert Jahren wurde Albertis Gedanke mehrmals aufgegriffen. Schließlich gelang Blaise de Vigenere durch die Vervollständigung von Albertis Idee der Schritt in die Unsterblichkeit. Die ihm zu Ehren genannte Vigenere-Verschlüsselung wird folgendermaßen verwendet:
Grundlage für den Einsatz der polyalphabetischen Substitution ist das Vigenere-Quadrat (siehe Seite 7). Kopf des Quadrates ist das Klartextalphabet. Darunter befinden sich 26 jeweils um einen Buchstaben verschobene Geheimtextalphabete.
Der Sender verschlüsselt jeden Buchstaben der Nachricht durch eine andere Zeile des Vigenere-Quadrates. Damit der Empfänger weiß, welcher Buchstabe mit welcher Zeile verschlüsselt wurde, wird ein Schlüsselwort verwendet. So gelingt die Synchronisation zwischen beiden Parteien.
Bsp.: Nachricht: ich kam, sah und siegte.
Schlüssel: BLITZ
Der Schlüssel wird dabei über die Nachricht geschrieben.

B	L	I	T	Z	B	L	I	T	Z	B	L	I	T	Z	B	L	I
i	c	h	k	a	m	s	a	h	u	n	d	s	i	e	g	t	e
J	N	P	D	Z	N	D	I	Z	T	O	O	A	B	D	H	E	M

Will man den Buchstaben „i“ unter Berücksichtigung des Schlüssels chiffrieren, so geht man in die Zeile B des Quadrates und sucht in der i-Spalte des Klartextalphabetes den Buchstaben, der in der B-Zeile des Quadrates sich befindet (J). Genauso chiffriert man die anderen Buchstaben. Die nachfolgende Tabelle veranschaulicht den Vorgang.

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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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
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

Abbildung 1: Vigenere-Quadrat mit Schlüsselwort „Blitz“

Geheimtext: JNP DZN, DIZ TOO ABDHEM.

Mehrfach auftauchende Buchstaben im Geheimtext lassen dabei nicht unbedingt auf ein und denselben Buchstaben schließen, da unterschiedliche Zeilen des Vigenere-Quadrates verwendet wurden.

Der Empfänger wendet das Verfahren in umgekehrter Reihenfolge an, um die Nachricht mit Hilfe des Schlüssels zu lesen.

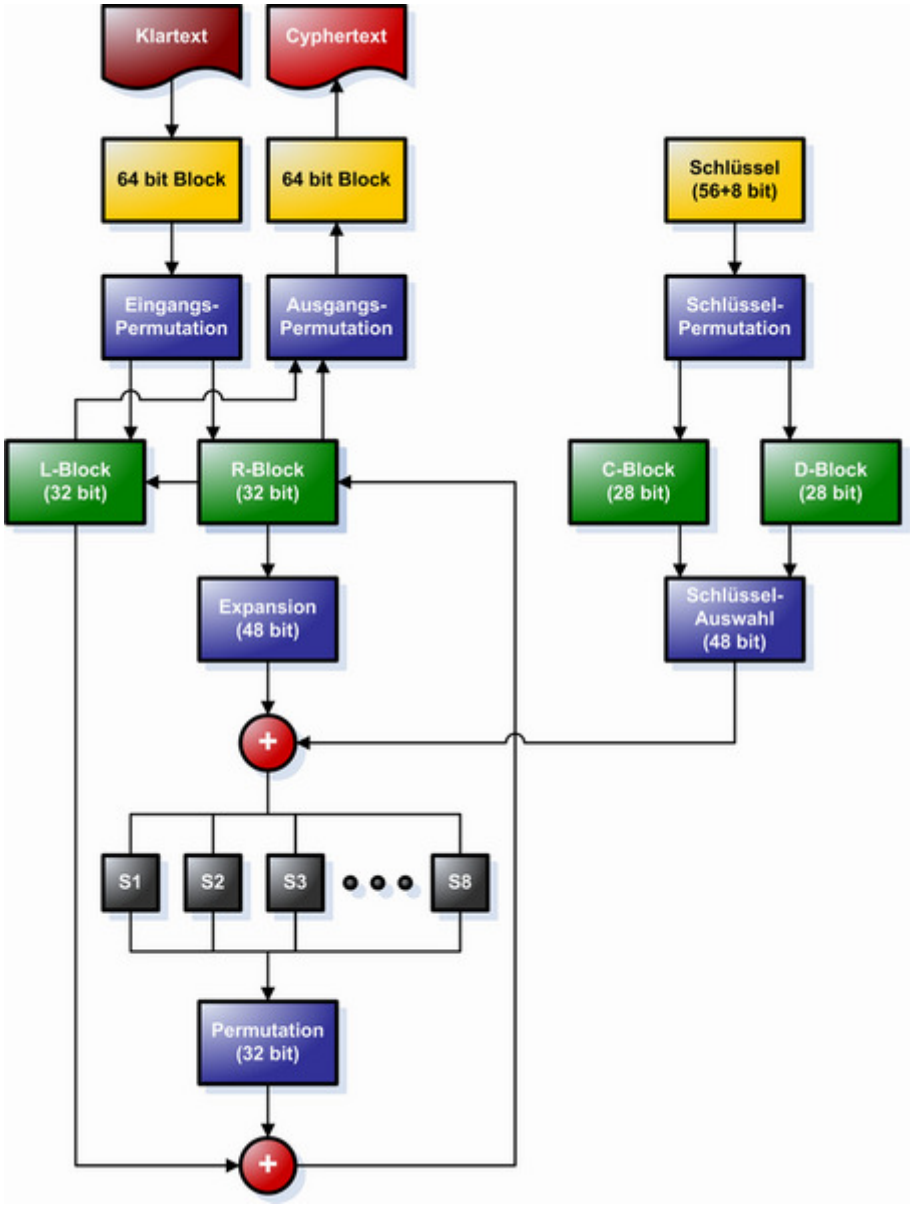
3. Kryptographie der Neuzeit

Über drei Jahrhunderte galt die Vigenere-Verschlüsselung als das Allheilmittel der Kryptographen. Es schien undenkbar, dass diese polyalphabetische Verschlüsselung jemals geknackt werden könnte.
Das britische Multitalent Charles Babbage, der unter anderem den ersten Computer der Welt, die Differenzmaschine No.2, erdachte, erkannte als Erster, dass bei einer geringen Länge des Schlüssels die Verschlüsselung angreifbar ist. Existiert im Klartext, d.h. in der eigentlichen Nachricht, mehrmals z.B. „Sonnenuntergang“, dann ist es bei einem kurzen Schlüssel sehr wahrscheinlich, dass gleiche Abschnitte des Wortes durch denselben Teil des Schlüssels verschlüsselt werden. Auf diese Weise entstehen im Geheimtext mehrere identische Zeichenketten. Die Entfernung, mit der die Zeichenketten im Geheimtext auftauchen, lässt dabei Rückschlüsse auf die Länge des Schlüssels zu. Ist die Länge des Schlüssels bekannt, ermöglicht die mehrfache Verwendung der Häufigkeitsanalyse die Entschlüsselung der Nachricht.
Eine ausführliche Darstellung des Verfahrens ist in [1] nachzulesen.
Obwohl Babbage als Erster die Vigenere-Verschlüsselung 1854 knackte, wird häufig Friedrich Kasiski als Entdecker des beschriebenen Verfahrens genannt. Kasiski entwickelte es 1863 unabhängig von Babbage. Man spricht daher auch vom Kasiski-Test.

3.1 DES

Mit dem Einsatz von Computern in wirtschaftlichen und militärischen Bereichen tauchte die Forderung nach einem Verschlüsselungsstandard auf. Durchgesetzt hat sich das Programm „Lucifer“, das vom deutschen Immigranten Horst Feistel in den siebziger Jahren bei IBM entwickelt wurde.
Lucifer verschlüsselt Texte nach dem folgenden Algorithmus:
Der binärcodierte Klartext wird in Blöcke K^1 bis K^n à 64 Zahlen aufgespaltet. Nach einer Eingangspermutation wird jeder der 64 Bit Blöcke in zwei Blöcke A^0 und B^0 geteilt. Der 56 Bit große Schlüssel wird in der Schlüsselpermutation umgestellt und 48 Bit werden für die weiteren Vorgänge ausgewählt. Der Block B^0 wird durch Duplizierung von bestimmten Bits

zu einem 48 Bit großen Block expandiert. Dieser wird mit dem Schlüssel addiert. Danach wird das Ergebnis in 8 Blöcke b_1 bis b_8 mit je 6 Bit geteilt. Acht S-Boxen (Substitutionsbox) wandeln jeden 6 Bit Block b_i in eine 4 Bit Zahl um. Die Substitutionsergebnisse bilden, nachdem diese wieder zusammengefügt wurden, einen 32 Bit Block, der nochmals permutiert wird. Anschließend wird dieser Block mit A^0 addiert und bildet den Block B^1.
Der ursprüngliche Block B^0 wird in $A^{(1)}$ umbenannt. Diese Schrittfolgen werden als Runde bezeichnet. Für den Algorithmus werden 16 Runden durchgeführt. In der letzten Runde werden die Blöcke A^{16} und B^{16} nicht vertauscht, sondern durchlaufen eine Abschlusspermutation. Danach ist der ursprüngliche Block K^i erfolgreich mit dem Lucifer-Algorithmus verschlüsselt worden.
Nach der Verschlüsselung kann der Geheimtext gesendet und beim Empfänger wieder durch Umkehrung des Verschlüsselungsverfahrens entschlüsselt werden.
Die nachfolgende Abbildung veranschaulicht die Vorgänge:



[WIKI]

1976 kam eine Lucifer-Version mit einem 64-Bit Schlüssel zum Einsatz, die unter dem Namen Data Encryption Standard (DES) bekannt wurde. Jeweils ein Bit pro Byte wird zum Paritäts-Check verwendet. Damit reduziert sich die Schlüssellänge auf 56-Bit.

DES wird heute unter anderem bei Bankautomaten eingesetzt. DES erzeugt mit einem Schlüssel und den Daten des Kunden, die über den Magnetstreifen eingelesen werden, eine PIN, die mit der Eingabe des Kunden verglichen wird.

In den 90er Jahren wurde bewiesen, dass DES nicht mehr die Sicherheit gewährleistet, die es 20 Jahre vorher noch bot, da die Hardware-Entwicklung rasant vorrangetrieben wurde. Alternativ zu DES wird 3DES eingesetzt, dass mit einem 112 Bit großen Schlüssel arbeitet und die Nachricht dreimal mit unterschiedlichen Schlüsseln chiffriert.

Im Jahre 2000 wurde ein neues Verfahren, AES (Advanced Encryption Standard) oder Rijndael-Algorithmus genannt, vorgestellt, dass DES bzw. 3DES in naher Zukunft ablösen könnte. AES verwendet größere Schlüssel (bis 256 Bit), verschlüsselt Blöcke, die unterschiedlich lang sind, mit verschieden Teilen des Schlüssels mehrmals nacheinander und hat eine variable Rundenanzahl.

3.2 Schlüsselaustausch-Problem

Seit Beginn der Kryptographie gab es, unabhängig vom Verschlüsselungssystem, ein gewaltiges Problem, das die Sicherheit der Verschlüsselung gefährdete. Damit Sender und Empfänger ihre Ver- und Entschlüsselungsvorgänge synchronisieren können, ist der Schlüssel notwendig. Doch dazu muss der Schlüssel zwischen beiden Parteien ausgetauscht werden. Wird der Schlüssel bei der Übertragung durch elektronische Schnüffelprogramme, durch Abhöraktionen oder in einer anderen Art und Weise abgefangen, ist die Verschlüsselung gefährdet. Dieses Problem wurde in den siebziger Jahren von einer amerikanischen Forschergruppe und einem britischen Wissenschaftler unabhängig voneinander gelöst.
Bis in die siebziger Jahre hinein galt der Schlüsselaustausch als Axiom der Kryptographie. Ein kleines Gedankenexperiment zeigt jedoch, dass ein Schlüsselaustausch nicht notwendigerweise stattfinden muss:
Man stelle sich vor, Sender und Empfänger kommunizieren miteinander und eine dritte Partei versucht diese Nachrichten abzufangen. In der Kryptographie werden die drei Parteien als Alice, Bob und Eve bezeichnet. Alice schreibt eine Nachricht und legt diese in eine Kiste, die durch ein Vorhängeschloss gesichert wird, zu dem nur Alice den passenden Schlüssel besitzt. Wird die Kiste von Eve geklaut, kann sie diese nicht öffnen, da sie den passenden Schlüssel nicht besitzt. Kommt die Kiste bei Bob an, fügt er der Kiste ein zusätzliches Schloss hinzu, zu dem nur er den Schlüssel besitzt und schickt die Kiste zu Alice zurück. Diese entfernt ihr Schloss und sendet die Kiste wieder an Bob, der die Kiste öffnet und die Nachricht lesen kann, da er den Schlüssel zu seinem Schloss besitzt. Es ist also kein Schlüsselaustausch zwischen Alice und Bob notwendig.
Dieses Gedankenexperiment wurde von den Amerikanern Whitfield Diffie, Martin Hellman und Ralph Merkle aufgegriffen. Beide versuchten mittels Einwegfunktionen die im Experiment geschilderten Vorgänge auf die Kryptographie zu übertragen. Einwegfunktionen sind in einer Richtung leicht durchführbar. Ihre Umkehrung jedoch ist umständlich. Beispiele für solche Funktionen finden sich in der Modul-Arithmetik.

Bsp.: 5 mod 9 = 5, 11 mod 9 = 2

Gesucht ist also der Rest, der bleibt, wenn eine Zahl durch den Modulus geteilt wird. Problematisch wird die Umkehrung von Modulfunktionen, da diese sich unregelmäßig verhalten.

Bsp.: Gesucht sei ein x, dass folgende Gleichung erfüllt: $4^x \pmod{11} = 1$. Man kann x nur bestimmen, indem man gut rät oder alle Werte von x=1 bis zur Lösung, x=10, berechnet.

Martin Hellman entwickelte 1976 auf Basis von Einwegfunktionen ein Verfahren, welches das Problem des Schlüsselaustausches löste. Mit diesem Algorithmus ist es Alice und Bob möglich einen Schlüssel zu vereinbaren, ohne den eigentlichen Schlüssel preiszugeben.

Grundlage dabei ist eine Einwegfunktion der Form $f(x) = R^X \pmod{Q}$ mit R<Q. Die eingesetzte Einwegfunktion muss nicht geheim gehalten werden und könnte Eve bekannt sein.

Alice und Bob suchen sich eine Zahl A bzw. B aus, die sie geheim halten (z.B. A=4, B=3). Sie einigen sich auf die Einwegfunktion $f(x) = 6^x \pmod{11}$. Beide setzen x=A bzw. x=B und erhalten ihr Ergebnis y=9 bzw. z=7, welches sie sich gegenseitig bekannt geben und das vor Eve nicht geheimgehalten werden muss. Alice setzt z von Bob für R in die Einwegfunktion ein (mit x=A) und Bob tut dies für y (mit x=B). Sie erhalten beide den vereinbarten Schlüssel 3, den sie z.B. für die DES-Verschlüsselung verwenden können.

Alice	Bob
Wählt geheime Zahl A=4	Wählt geheime Zahl B=3
$f(x) = 6^x \pmod{11}$	
$f(4) = 6^4 \pmod{11}=9=y$	$f(3) = 6^3 \pmod{11}=7=z$
$f'(4)= 7^4 \pmod{11}=3$	$f''(3)= 9^3 \pmod{11}=3$
Der gemeinsame Schlüssel ist 3.	

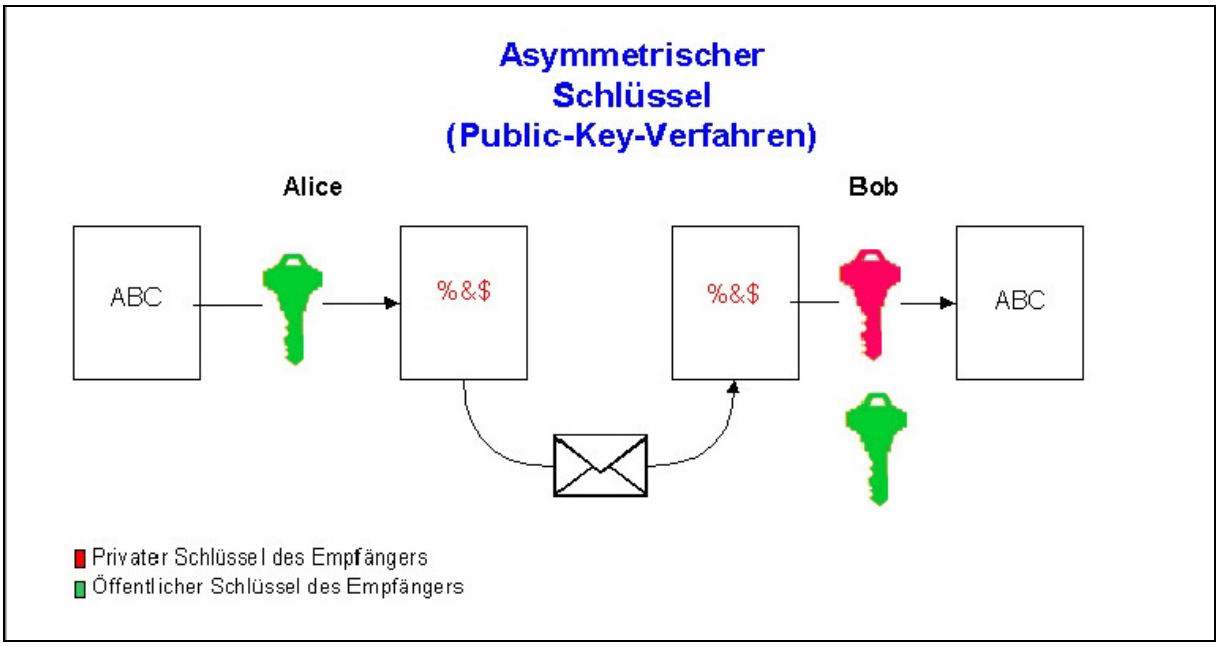
Alles was Eve bekannt ist, sind die Werte y, z und die Einwegfunktion. Doch um von y und z auf A und B zu schließen und somit den Schlüssel zu erfahren, muss Eve die Umkehrfunktion anwenden, d.h. sie muss entweder $6^x \pmod{11}=9$ (wenn z bekannt ist) oder $6^x \pmod{11}=7$ (wenn y bekannt ist) lösen. Dies ist bei großen Werten für A und B sehr aufwendig, da alle Werte der Reihe nach ausprobiert werden müssen. Eine Abkürzung dieser Sisyphus-Arbeit ist aufgrund der Unregelmäßigkeit von Einwegfunktionen nicht möglich.

Dieser Schlüsselaustausch nach dem Diffie-Hellman-Merkle-Verfahren gestattet, durch öffentlichen Austausch von Informationen (y, z, f), die Vereinbarung eines geheimen Schlüssels.

Malcolm Williamson, ein Kryptograph am britischen GCHQ (Government Communications Headquarters) entwickelte zur gleichen Zeit und unabhängig von seinen amerikanischen Kollegen dieses Schlüsselaustauschverfahren. Seine Entdeckung wurde erst 1997 von der britischen Regierung bekannt gegeben.

3.3 Public-Key-Kryptographie

Whitfield Diffie entwickelte 1975 das Konzept einer asymmetrischen Verschlüsselung. Vorher, z.B. bei DES oder bei der Vigenere-Verschlüsselung war der Schlüssel, den Sender und Empfänger vereinbarten, identisch. Die Asymmetrie kommt beim Verfahren von Diffie dadurch zu Stande, dass Chiffrier- und Dechiffrierschlüssel nicht identisch sind.
Will Alice an Bob eine Nachricht schicken, so verwendet sie den Chiffrierschlüssel von Bob, der als öffentlicher Schlüssel bezeichnet wird. Dieser ist Jedem, der Bob eine Nachricht schicken möchte, bekannt und verschlüsselt die an Bob adressierte Nachricht („ABC“). Die so chiffrierte Nachricht kann allerdings nicht mit dem Chiffrierschlüssel entschlüsselt werden. Dies ist nur mit dem Dechiffrierschlüssel möglich, der als privater Schlüssel bezeichnet wird, da er nur Bob bekannt sein sollte. Wenn Eve die chiffrierte Nachricht abfängt, ist es ihr mit dem öffentlichen Schlüssel unmöglich, diese Nachricht zu entschlüsseln.



[a]

Ein Schlüsselaustausch, z.B. mit dem Diffie-Hellman-Merkle-Verfahren, ist bei der asymmetrischen Verschlüsselung nicht notwendig, da der private Schlüssel nicht zwischen Sender und Empfänger ausgetauscht wird.

Diffie entwickelte dieses Konzept. Doch er scheiterte beim Versuch, eine geeignete Einwegfunktion zu finden.

Dies gelang den amerikanischen Wissenschaftlern Leonard Adleman, Ron Rivest und Adi Shamir. Die erforderliche Einwegfunktion wurde von Rivest 1977 gefunden. Das nach den Entwicklern RSA genannte Verfahren wird folgendermaßen angewendet:

a)

Alice wählt zwei große Primzahlen s und t ($s \neq t$). Zu Demonstrationszwecken wähle ich s=11 und t=17. In der Praxis werden Primzahlen mit mehr als 100 Stellen eingesetzt. Diese Zahlen sind für den privaten Schlüssel notwendig und sollten geheimgehalten werden. Das Produkt aus diesen Zahlen ist P=187. Zusätzlich wählt Alice eine Zahl z>1, z.B. z=7. Dabei sollten z und die Formel (s-1)(t-1) teilerfremd sein. Anschließend erstellt Alice ihren privaten Schlüssel u durch folgende Formel:

$$u*z = 1 \bmod((s-1)(t-1))$$

d.h. bei der Division des Produktes u*z durch (s-1)(t-1) soll ein Rest von 1 entstehen. Man kann die Gleichung

$$u*7 = 1 \bmod(160) \Rightarrow u*7 = 160*k+1$$

zu einer diophantischen Gleichung umschreiben:

$$160*k - 7*u + 1 = 0$$

und diese Gleichung mit dem Euklidischen Algorithmus lösen:

$160 = 22*7 + 6 \Rightarrow q_0 = 22$		
$7 = 1*6 + 1 \Rightarrow q_1 = 1$		
$1 = 1*1 + 0 \Rightarrow q_2 = 1$		
Rücklaufformeln : $y_{(n+1)} = q_n * y_n + y_{(n-1)}$ mit $y_{-1} = 0$ und $y_0 = 1$ $x_{(n+1)} = q_n * x_n + x_{(n-1)}$ mit $x_{-1} = 1$ und $x_0 = 0$		
$q_0 = 22$	$y_0 = 1$	$x_0 = 0$
$q_1 = 1$	$y_1 = 22$	$x_1 = 1$
$q_2 = 1$	$y_2 = 23$	$x_2 = 1$

Probe : $160* x_2 – 7*y_2 + 1 = 0$

Der private Schlüssel u von Alice ist y_2, d.h. u ist somit 23.

b)

Alice veröffentlicht z und P, da diese ihren öffentlichen Schlüssel bilden. Die binärcodierte Nachricht des Senders Bob ist N. Bob verschlüsselt N mithilfe des öffentlichen Schlüssels und erzeugt somit den Geheimtext Y nach folgender Einwegfunktion: $Y=N^z \pmod P$

Bob möchte z.B. eine Nachricht an Alice schicken, mit N=88 (ASCII Buchstabe X). Er verschlüsselt N und erhält den Geheimtext $Y=88^7 \pmod{187}=11$. Dabei wird die Kongruenzmathematik verwendet, d.h. man ersetzt 88^7 schrittweise durch eine kleinere Zahl, die kongruent ist.

$88^7 = 88^{(4+2+1)} \Rightarrow 88^7 \pmod{187} = (88^4 \pmod{187}*88^2 \pmod{187}*88^1(\text{ mod } 187))(\text{mod } 187)$

$= 11$

Bob verschickt Y=11 an Alice.

c)

Alice kann Y durch ihren privaten Schlüssel u und mit der Formel $N=Y^u \pmod P$ entschlüsseln. Zur Berechnung des Modulus wird wieder die Kongruenzmathematik angewendet.

$N=11^{23} \pmod{187}=88$

Eve kann die abgefangene Nachricht nicht mit dem öffentlichen Schlüssel von Alice entschlüsseln. Damit sie die Nachricht lesen kann, muss Eve den privaten Schlüssel ermitteln. Doch die einzige Möglichkeit besteht darin, die Primzahlen s und t von Alice mittels P zu ermitteln. Die Primfaktorzerlegung kann als Einwegfunktion bezeichnet werden, da es bisher kein einfaches und schnelles Verfahren für die Faktorzerlegung gibt. Daher gilt der RSA-Algorithmus bei der Verwendung von großen Primzahlen als relativ sicher.

6 Jahre vor Diffie gelangen dem Briten James Ellis die Entdeckungen, die Diffie Mitte der siebziger Jahre machte und sein Kollege Clifford Cocks entdeckte die Einwegfunktion 1973, die Rivest 4 Jahre später finden sollte. Doch erst 1997 kamen ihre Leistungen an die Öffentlichkeit, weil Ellis und Cocks, wie auch Williamson, für das GCHQ und damit für die britische Regierung arbeiteten. Das GCHQ hielt die Entdeckungen von Ellis, Williamson und Cocks unter Verschluss, da es keinen praktischen Nutzen sah.

3.4 Quantenkryptographie

Die Quantenkryptographie ermöglicht eine sichere Schlüsselübertragung zwischen Sender und Empfänger. Eine Möglichkeit ist die Polarisation (hier: die Ausrichtung des Spins, des Drehimpulses) von Photonen auszunutzen. Photonen können horizontal (h), vertikal (v) oder diagonal (d) polarisiert werden. H-Photonen gelangen nur durch einen h-Filter hindurch, v-Photonen nur durch einen v-Filter und d-Photonen zu 50% durch einen h- bzw. v-Filter (die als rektilinear bezeichnet werden) und zu 100% durch einen diagonalen Filter.
Wird zwischen Alice und Bob ein Photon ausgetauscht, so ist es Eve nicht möglich, dieses unbemerkt zu kopieren. Beim Versuch das Photon abzuhören, wird nach den Regeln der Quantenmechanik die Polarisation geändert. Für Eve ist es daher unmöglich, die Verbindung zwischen Alice und Bob unbemerkt abzuhören.
Für einen sicheren Schlüsselaustausch verschickt Alice zunächst eine Reihe von zufällig polarisierten Photonen. Bob misst diese Photonen mit zufällig eingestellten Filtern. Nach der Übertragung übermittelt Alice ihr Filterschema (rektilinear oder diagonal) an Bob und dieser teilt ihr mit, wo er das Schema korrekt angewendet hat. Beide streichen die abweichenden Filter von der Liste. Dabei hält Alice die eigentliche Polarisation der Photonen und Bob seinen Messaufbau geheim.
Eve kennt somit zwar das Polarisationsschema, aber nicht die eigentliche Polarisation. In der Hälfte der Fälle wählt sie den falschen Filter und verändert damit die Polarisation der Photonen. Alice und Bob bemerken somit, dass ihre Verbindung belauscht wird und können angemessen darauf reagieren.

Quellen

Simon Singh, „Geheime Botschaften“, 2000 [1]

Tim Bell, Ian H.Witten, Mike Fellows, „Computer Science Unplugged“, 1998 [2]

www.wikipedia.de [WIKI]

www.jorg.fruchbodt.bei.t-online.de [a]

www.zitate.de [z]