

Sicher Surfen IV: Verschlüsselung & Kryptographie

Georg Wagner

25. Mai 2001

1 Was ist Kryptographie?

Kryptographie ist aus den griechischen Wörtern für *Verstecken* und *Schreiben* zusammengesetzt und kann somit mit *Versteckt Schreiben* übersetzt werden. Heute ist Kryptographie ein eigener Forschungsbereich, der spätestens seit der Entstehung des Internets auch für die breite Öffentlichkeit interessant ist.

1.1 Verschlüsselung ganz einfach!

Worum geht's? Sie möchten jemanden eine vertrauliche Nachricht per Email senden. Ihnen ist bekannt, dass eine normal versendete Email dem Versand einer offenen Postkarte entspricht. Daher entschliessen Sie sich, Ihre Nachricht verschlüsselt zu senden. Dabei gehen Sie wie folgt vor:

- Sie schreiben wie gewohnt Ihre Nachricht, diese liegt dann im sogenannten Klartext¹ vor.
- Sie lassen ihre Nachricht von einem Verschlüsselungsverfahren² bearbeiten. Damit ein solches Verfahren arbeiten kann, benötigt es einen geheimen Wert, den sogenannten Schlüssel³.
- Nach der Bearbeitung Ihrer Nachricht mit dem Verschlüsselungsverfahren - dem Verschlüsseln - liegt ihre Nachricht in kodierter Form⁴ vor.
- Diese senden Sie nun dem Empfänger zu.

Der Empfänger muss Ihr Vorgehen rückgängig machen, er muss Ihre Nachricht entschlüsseln. Also:

- Der Empfänger nimmt Ihre Nachricht entgegen und wendet ein passendes Entschlüsselungsverfahren - meist die Umkehrung des Verschlüsselungsverfahrens - mit dem gleichen Schlüssel auf Ihre verschlüsselte Nachricht an.
- Danach liegt die Nachricht wieder im Klartext vor.

¹english:cleartext

²englisch: DEA - Data Encryption Algorithm

³Dies kann eine PIN sein wie bei ihrer Kreditkarte oder ein Passwort, oder speziell generierte Datenblöcke.

⁴englisch: cyphertext

1.2 Verschlüsselung nicht ganz so einfach?

Bei dem oben skizzierten Verfahren sind Ihnen sicher einige Probleme aufgefallen:

- Sender und Empfänger müssen im Besitz des gleichen geheimen Schlüssels sein.
- Sender und Empfänger müssen sich über das zu verwendende Verfahren einig sein.

Das Hauptproblem ist hier: Wie übergebe ich den Schlüssel an den Empfänger, ohne dass jemand anderes in den Besitz dieses Schlüssels kommt. Dies ist bei weltweiter Kommunikation ein echtes Hindernis, da die sichere Uebergabe eines Schlüssels nur bei einem persönlichen Treffen mit dem Empfänger möglich ist.

2 Verschlüsselungsverfahren

2.1 Einfache Verschlüsselungsverfahren

Ein sehr einfaches Verschlüsselungsverfahren ist Ihnen sicher noch aus der Kindheit bekannt: die Hühnersprache. Der Satz *Das Internet ist toll* verwandelt sich in der Hühnersprache zu *Dahadefas Ihidefintehedefernhedefet ihidefist tohodefoll*. Ein weiteres einfaches Verfahren ist das Verschieben von Buchstaben um mehrere Positionen. Verschieben Sie z.B. alle Buchstaben um 5 Positionen, wird aus einem A ein F, einem B ein G usw. Also:

ABCDEF GHIJKL MNOPQR STUVWXYZ ABCDE
 ABCDEF GHIJKL NNOPQR STUVWXYZ

Sie könnten in diesem Fall das *Verschieben um n Positionen* als das verwendete Verschlüsselungsverfahren bezeichnen, bei dem der geheime Wert n der Schlüssel wäre. Verwenden Sie für den geheimen Wert n die Zahl 13, erhalten Sie das Verschlüsselungsverfahren ROT13. Dieses Verfahren ist speziell bekannt, weil es bei 26 Buchstaben im Alphabet absolut symmetrisch ist: Wenden Sie dieses Verfahren noch einmal auf einen zuvor mit diesem Verfahren verschlüsselten Text an, erhalten Sie wieder den ursprünglichen Klartext. Angeblich hat bereits Cäsar diese Verfahren verwendet.

Wie Sie sich sicher denken können, sind die bisher vorgestellten Verfahren alle nicht sicher. Sie würden einer sogenannten Kryptanalyse nicht lange widerstehen. In jeder Sprache treten bestimmte Buchstaben und Buchstabenkombinationen häufiger auf als andere. Mit diesem Wissen und einem Computer lassen sich solche verschlüsselten Texte leicht wieder in Klartext umwandeln. Dennoch wird ROT13 von einigen Emailprogrammen zur Verschlüsselung der Betreffzeile verwendet. Dies soll das automatische Suchen nach bestimmten Reizwörtern erschweren.

2.2 Symmetrische Verschlüsselungsverfahren

Die oben beschriebenen Verfahren gehören zu einer bestimmten Klasse von Verschlüsselungsverfahren: den symmetrischen Verschlüsselungsverfahren. Bei

den symmetrischen Verschlüsselungsverfahren wird nur ein einziger Schlüssel zur Verschlüsselung und Entschlüsselung einer Nachricht verwendet⁵. Aus diesem Grund müssen sowohl der Sender als auch der Empfänger den gleichen Schlüssel besitzen und geheim halten.

Es gibt zwar sehr sichere symmetrische Verschlüsselungsverfahren, aber sie haben für die Verwendung im Internet einen erheblichen Nachteil. Stellen Sie sich vor, dass eine grosse Bank mit tausenden von Kunden mit diesen symmetrischen Verfahren arbeiten würde. Die Bank müsste dann:

- für jeden Kunden einen geheimen Schlüssel aufbewahren
- diese Schlüssel jedem Kunden auf einem sicherem Vertriebsweg zukommen lassen

Das bekannteste symmetrische Verschlüsselungsverfahren ist der Data Encryption Standard (DES).

2.3 Asymmetrische Verschlüsselungsverfahren

Im Gegensatz zu den symmetrischen Verschlüsselungsverfahren arbeiten die asymmetrischen Verschlüsselungsverfahren mit einem Schlüsselpaar:

- einem privaten/geheimen Schlüssel⁶
- und einem dazugehörenden öffentlichen Schlüssel⁷

Die Schlüssel eines Schlüsselpaars stehen miteinander in folgender Beziehung: eine mit dem öffentlichen Schlüssel eines Schlüsselpaars verschlüsselte Nachricht kann nur mit dem dazugehörendem privaten Schlüssel wieder entschlüsselt werden.

Nun werden Sie sich fragen "Was nützt mir das? Ich verschlüssele eine Nachricht mit meinem öffentlichen Schlüssel und entschlüsseln kann ich sie wieder mit meinem privaten Schlüssel. Damit komme ich nicht weiter!" Richtig, Sie brauchen die öffentlichen Schlüssel aller Personen, mit denen Sie verschlüsselte Nachrichten austauschen wollen. Sie sammeln gewissermassen alle öffentlichen Schlüssel der Personen, mit denen Sie Nachrichten austauschen wollen, in einem Schlüsselbund. Öffentliche Schlüssel können und sollen frei verteilt werden. Sie sind nicht auf einen sicheren Vertriebsweg angewiesen, da sie nur zum Verschlüsseln, nicht aber zum Entschlüsseln verwendet werden. Ausserdem werden bei diesem Verfahren deutlich weniger Schlüssel benötigt. Wenn 1000 Menschen miteinander verschlüsselt kommunizieren wollen, müssen bei dem asymmetrischen Verfahren 1000 öffentliche Schlüssel verteilt werden. Bei dem symmetrischen Verfahren müssten $\frac{n*(n-1)}{2} = 499500$ geheimzuhaltende Schlüssel verteilt werden, wenn jeder mit jedem Nachrichten austauschen möchte.

⁵Sie werden daher auch als Private-Key-Verfahren bezeichnet.

⁶englisch: private/secret key

⁷englisch: public key; wegen der Verwendung eines public keys werden diese Verfahren auch als Public-Key-Verfahren bezeichnet.

2.3.1 Ablauf des verschlüsselten Nachrichtenaustauschs

Nehmen wir an, Sie wollen eine verschlüsselte Nachricht an Fritz Meier senden. Dann gehen Sie wie folgt vor:

1. Sie schreiben Ihre Nachricht.
2. Sie verschlüsseln diese Nachricht mit dem öffentlichen Schlüssel von Fritz Meier.
3. Sie senden die Nachricht an Fritz Meier.
4. Fritz Meier entschlüsselt die Nachricht mit seinem privaten Schlüssel und erhält so den lesbaren Klartext Ihrer Nachricht.

Das ist nicht viel schwieriger wie bei dem symmetrischen Verfahren. Was Sie nie tun sollten:

- Versenden Sie nie eine Nachricht, die Sie mit Ihrem privaten Schlüssel verschlüsselt haben. Denn jeder, der Ihren öffentlichen Schlüssel hat, kann diese Nachricht entschlüsseln.
- Geben Sie niemand Ihren geheimen Schlüssel!
- Verlieren Sie nie Ihren geheimen Schlüssel!

Sind nun alle Probleme gelöst? Es sieht so aus, denn die öffentlichen Schlüssel sind nicht auf einen sicheren Vertriebsweg angewiesen. Sie können Ihren öffentlichen Schlüssel also auch per Email verteilen. Aber halt! Ein Problem bleibt. Woher wissen Sie, dass der Schlüssel, den Sie per Email erhalten, wirklich der öffentliche Schlüssel von Fritz Meier ist?

2.3.2 Wann ist ein Schlüssel echt?

Zu jedem öffentlichen Schlüssel lässt sich ein sogenannter Fingerprint erzeugen. Das ist eine Art Seriennummer, die einmalig ist. Wenn Sie die Stimme einer Person gut kennen, können Sie sie anrufen und sich den Fingerprint ihres öffentlichen Schlüssels vorlesen lassen. Stimmt dieser mit dem überein, den Sie haben, haben Sie die Echtheit des Schlüssels verifiziert. Falls Sie die Person nicht kennen, bestehen folgende Möglichkeiten:

1. Sie wenden sich an eine Zertifizierungsstelle. Dies ist eine vertrauenswürdige Organisation, bei der man seinen öffentlichen Schlüssel hinterlegen kann. Bei der Hinterlegung des Schlüssels muss man sich ausweisen. Die Zertifizierungsstelle sagt Ihnen auf Anfrage also: "Ja, der öffentliche Schlüssel mit diesem Fingerprint gehört einer Person, die sich als Fritz Meier ausweisen konnte."
2. Sie vereinbaren ein Treffen mit Fritz Meier. Bei diesem Treffen lassen sie sich den Reisepass von Fritz Meier und den Fingerprint seines öffentlichen Schlüssels zeigen. Falls Sie einen Bekannten haben, der auch Fritz Meier kennt, können Sie auch diesen Bekannten zu dem Treffen mitnehmen. Wenn der Bekannte Ihnen dann glaubhaft versichern kann, dass es sich wirklich Fritz Meier ist, der vor Ihnen steht, müssen Sie nur noch den Fingerprint des öffentlichen Schlüssels von Fritz Meier zeigen lassen.

So, damit haben Sie auch das Problem der Echtheit eines öffentlichen Schlüssels gelöst.

3 Sicherheit der Verschlüsselungsverfahren

Bevor die Kryptographie als Wissenschaft betrieben wurde, lag die Sicherheit bei der Verschlüsselung in der Kenntnis der Verfahren. Diese wurden eifersüchtig behütet. Kannte jemand anderes das Verfahren, konnte er eine verschlüsselte Nachricht leicht entschlüsseln. Diese Denkweise entspricht ungefähr dem Verstecken des Haustürschlüssels unter der Fussmatte.

Bei den modernen Verschlüsselungsverfahren ist der verwendete Algorithmus allgemein bekannt. Man versucht solche Algorithmen zu finden, bei denen die Verschlüsselung sehr schnell geht, während die Entschlüsselung - ohne Kenntnis des Schlüssels - sehr lange dauert. Um Ihnen eine Idee von den Rechenzeiten zu geben:

Bei dem Verfahren RSA, einem Vertreter der asymmetrischen Verschlüsselungsverfahren, würde das Knacken⁸ einer Nachricht, die mit einem Schlüssel von 665 Bit⁹ verschlüsselt wurde, 380267 Jahre benötigen. Ist Ihnen das nicht sicher genug, können Sie einen Schlüssel von 1330 Bits verwenden. Dann werden $8,6 \cdot 10^{15}$ Jahre benötigt. Das ist vermutlich lang genug, denn das Universum ist nach den Berechnungen von Stephen Hawkins¹⁰ $2 \cdot 10^{10}$ Jahre¹¹ alt.

Oder um es etwas anders zu illustrieren: Wenn Sie alle Zwischenergebnisse beim Faktorisieren eines 665-Bit-Schlüssels auf Festplatten von 100 GB zwischenspeichern würden, würden Sie $6,12 \cdot 10^{189}$ Festplatten benötigen; was bei einem Gewicht von nur einem Millionstel Gramm pro Platte einer Gesamtmasse von $6,12 \cdot 10^{180}$ kg entspräche, also ungefähr dem $3,06 \cdot 10^{150}$ fachen der Sonnenmasse¹². Diese Masse liegt weit oberhalb der Chandrasekhar-Grenze¹³, bei deren Ueberschreiten ein Stern zu einem schwarzen Loch kollabiert.

Nach heutigem Ermessen und ohne einen gewaltigen Durchbruch in der Algorithmik sind diese Verfahren also als sicher anzusehen.

3.1 Einfluss der Schlüssellänge auf die Sicherheit

Das entscheidende Kriterium bei der Sicherheit der modernen Verschlüsselungsverfahren ist die Länge des Schlüssels. Ein Schlüssel der Länge 128 Bit¹⁴ ist sicherer als einer, der 64 Bit lang ist. Die Abhängigkeit ist exponentiell¹⁵. Bei einem 64-Bit-Schlüssel gibt es $2^{64} = 1,8 \cdot 10^{19}$ mögliche Kombinationen, während es bei einem 128-Bit-Schlüssel bereits $2^{128} = 3,4 \cdot 10^{38}$ Kombinationen sind.

⁸englisch:crack(ing); dieses Vorgehen, das Durchprobieren aller möglichen Kombinationen mit geballter Rechenkraft von Computern wird auch als *Brute Force Attack* bezeichnet.

⁹Das entspricht einer Zahl mit 200 Stellen im Dezimalsystem.

¹⁰Stephen W. Hawkins: A Brief History of Time

¹¹20 Milliarden

¹²Die Sonnenmasse beträgt: $2 \cdot 10^{30}$ kg

¹³Die Chandrasekhar-Grenze liegt bei dem anderthalbfachen der Sonnenmasse.

¹⁴Ein Bit entspricht einer Stelle im binären Zahlensystem.

¹⁵Denken Sie hier an das bekannte Reiskorn auf dem Schachbrett: Auf das erste Feld legen Sie ein Korn, auf das zweite zwei Körner, auf das dritte 4 Körner usw. Wie gross muss der Speicher sein, um alle Reiskörner zu lagern?

4 Verschlüsselung in der Praxis

4.1 Was können Sie alles verschlüsseln?

Sie können Verschlüsselung verwenden, um:

- die Dateien auf Ihrem Computer gegen unberechtigte Zugriffe zu schützen.
- Daten während der Uebertragung von einem zum anderem Computer zu schützen, also z.B. bei Email und den Internetbrowsern.
- absichtliche oder unabsichtliche Veränderungen Ihrer Daten zu verhindern oder festzustellen.
- festzustellen, wer wirklich der Urheber eines Dokuments ist.

Bei den Browsern wird normalerweise unverschlüsselt gearbeitet. Besuchen Sie aber eine sogenannt sichere Webseite, werden die Daten zwischen dem Browser und dieser Seite verschlüsselt übertragen. Leider fallen kryptographische Verfahren in den USA unter das Waffengesetz. Daher werden bei den Exportversionen von Netscape die Schlüssellängen auf 40 Bit beschränkt. Vermutlich ist dies eine Schlüssellänge, bei der die National Security Agency (NSA) eine mit einem solchen Schlüssel verschlüsselte Nachricht in Sekundenbruchteilen entschlüsseln kann. In den USA wird bei den Browsern normalerweise mit einer Schlüssellänge von 128 Bit gearbeitet.

4.2 Handhabung

In der Praxis nehmen Ihnen die unterschiedlichsten Kryptoprogramme - das bekannteste ist wohl *Pretty Good Privacy* (PGP) - das Ver- und Entschlüsseln ab. Sie müssen sich nur am Anfang Ihr Schlüsselpaar erzeugen lassen und die öffentlichen Schlüssel Ihrer Kommunikationspartner besorgen. Die meisten Programme sind so gut auf die Emailprogramme abgestimmt, dass die Ver- und Entschlüsselung nahezu automatisch abläuft.

4.3 Praktische Sicherheitshinweise

Wenn Sie die Verschlüsselung Ihres Browsers testen wollen, gehen Sie doch auf folgende Webseite: Fortify <http://www.fortify.net/sslcheck.html>. Der Unterschied zwischen der 40-Bit- und der 128-Bit-Verschlüsselung wird auf dieser Webseite als der Unterschied zwischen einem normalen Briefumschlag und einem Qualitätstresor beschrieben. *Fortify* ist übrigens ein Programm, um die Verkrüppelung der Schlüssellänge in Netscape rückgängig zu machen.

Deutschsprachige Informationen finden Sie beim Security Server der Universität-Gesamthochschule Siegen <http://www.uni-siegen.de/security>.