5.3 Asymmetrische Verschlüsselung

Die Arbeit von Diffie und Hellman zum Problem des Schlüsseltausches revolutionierte die Kryptographie. Aus ihr ging nicht nur die geniale Idee von Hellman zum Schlüsseltausch hervor, sondern auch eine sehr wichtige prinzipielle Überlegung von Diffie zur Kryptographie allgemein: die asymmetrische Verschlüsselung.
Das Schlüsseltauschverfahren hatte noch gewisse praktische Nachteile: so mussten Alice und Bob beide zum Zeitpunkt des Schlüsseltausches gemeinsam „online" sein, da die Zahlen α und β ausgetauscht werden mussten. Vor allem wenn Alice in Amerika und Bob in Europa oder Asien ansässig waren, war dies doch auf Grund der Zeitverschiebung recht kompliziert. Die von Diffie abstrakt formulierte asymmetrische Verschlüsselung sollte hier Abhilfe schaffen.

5.3.1 Symmetrische vs. asymmetrische Verschlüsselung

Symmetrische Verschlüsselungsverfahren

Die bisher betrachteten Verschlüsselungsverfahren waren alle *symmetrisch*: für die Verschlüsselung wird im Wesentlichen derselbe Schlüssel verwendet wie für die Entschlüsselung. Es ist deshalb unabdingbar, dass dieser Schlüssel nur Alice und Bob bekannt ist und dass Eve nicht die Möglichkeit erhält, den Schlüssel herauszufinden.
Es tritt hier das Problem auf, dass der Schlüssel sicher übermittelt werden muss (z.B. mit der Methode von Diffie/Hellman). Zudem ist man nie ganz sicher, ob die Meldung von Eve nicht abgefangen und verändert wurde, d.h. es stellt sich auch das Problem der Authentifizierung.

Asymmetrische Verschlüsselungsverfahren

Bei der asymmetrischen Verschlüsselung wird nicht mit *einem* geheimen Schlüssel gearbeitet, sondern mit *zwei* unabhängigen Schlüsseln: einem öffentlichen und einem privaten (geheimen) Schlüssel. Alice stellt ihren öffentlichen Schlüssel, der lediglich zum *Ver*schlüsseln von Nachrichten dient, allen frei zur Verfügung. Ähnlich wie in einem Telefonbuch kann also jedermann seinen Schlüssel, der für die Verschlüsselung zuständig ist, öffentlich publizieren. Dies setzt natürlich voraus, dass man mit Hilfe dieses öffentlichen Schlüssels eine Nachricht nicht entschlüsseln kann. Dafür hat Alice einen privaten (geheimen) zweiten Schlüssel, der für die Entschlüsselung verwendet wird.

5.3.2 Vorteile der asymmetrischen Verschlüsselung: Digitale Signatur

Die asymmetrische Verschlüsselung bringt den Vorteil, dass jedermann eine verschlüsselte Botschaft an Bob schicken kann. Dazu schlägt er den öffentlichen Schlüssel von Bob in einem Verzeichnis nach und verschlüsselt damit seine Meldung. Es ist also kein Schlüsseltausch notwendig.
Zudem wird durch das Konzept der asymmetrischen Verschlüsselung auch das Problem der Authentifizierung auf sehr elegante Weise gelöst: Will Alice eine Meldung an Bob schicken, so dass dieser sicher ist, dass die Meldung von Alice stammt und nicht bei der Übermittlung durch Eve verändert wurde (digitale Signatur), so kann sie ihre Meldung mit ihrem privaten Schlüssel verschlüsseln und das Ergebnis dann an Bob senden und dieser entschlüsselt die Botschaft mit dem öffentlichen Schlüssel von Alice. Erhält er einen konsistenten Text, dann ist er sicher, dass die Meldung nur von Alice stammen kann, denn nur Alice ist im Besitz des privaten Schlüssels und somit in der Lage einen Text so zu verschlüsseln, dass dieser mit ihrem öffentlichen Schlüssel dechiffriert wird. Bei der digitalen Signatur wird häufig die Nachricht selbst gar nicht verschlüsselt – man verschlüsselt nur einen kleinen Textteil am Schluss der Nachricht (oder als Anhang) um die Herkunft der Nachricht abzusichern (entsprechend einer normalen Unterschrift).

5.3.3 Voraussetzungen für eine asymmetrische Verschlüsselung

Wie kann aber ein konkretes asymmetrisches Verfahren in der Praxis realisiert werden? Ist es überhaupt möglich, zwei unabhängige Schlüssel für die Ver- bzw. Entschlüsselung einer Nachricht zu generieren? Wenn man den öffentlichen Schlüssel kennt und eine Nachricht damit verschlüsseln kann: kann man sie denn dann nicht automatisch auch entschlüsseln, weil man das konkrete Rezept kennt?
Auch hier glaubte man ähnlich wie beim Schlüsseltausch nach Diffie/Hellman, dass dies Fragen ohne befriedigende Antworten seien und dass die Idee der asymmetrischen Verschlüsselung in der Theorie von Diffie zwar wohl durchdacht war, dass es aber in der Praxis unmöglich sei, das Verfahren zu realisieren. Ein asymmetrisches Verfahren müsste folgende Voraussetzungen erfüllen:

- Es existiert eine Verschlüsselungsfunktion f (öffentlicher Schlüssel), mit welcher ein Text T verschlüsselt werden und ein Geheimtext G generiert werden kann: f(T) = G
- Kennt man die Funktion f, so ist es dennoch unmöglich, aus einem verschlüsselten Text G den Ursprungstext T zu gewinnen: d.h. die Funktion ist nicht ohne weiteres umkehrbar.

- Hat man aber eine bestimmte Zusatzinformation zur Funktion f (den geheimen Schlüssel), so ist man in der Lage, die Umkehrfunktion von f zu berechnen und dadurch den Text zu entschlüsseln.

Eine wie oben beschriebene Funktion f nennt man „Einwegfunktion mit Falltür“. Einwegfunktionen sind Funktionen, die unmöglich (oder sehr schwierig) umzukehren sind. Die Falltür ist die Zusatzinformation, die man benötigt, um die Funktion eben dennoch umkehren zu können.

White Diffie war auf seiner Suche nach einer geeigneten Funktion nicht erfolgreich und auch viele andere Mathematiker bissen sich die Zähne an diesem Problem aus. Im April 1977, etwa zwei Jahre nach der Idee von Diffie gelang es aber schliesslich Ron **R**ivest, Adi **S**hamir und Leonard **A**dleman eine geeignete Funktion zu finden und der Siegeszug des RSA-Verfahrens nahm seinen Lauf.

6. Konkrete Verschlüsselung im Internet: SSL/TLS

Was passiert nun konkret, wenn man sich im Internet bewegt und sensible Daten ausgetauscht werden sollen? Egal ob es sich um Kreditkartennummer, Passwörter, Persönliche Daten in einem Onlineshop, E-Banking etc. handelt, sollten die Daten unbedingt verschlüsselt werden, da sie durchaus von Dritten „angezapft“ und gelesen werden können.

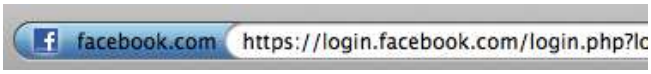

Abb. 16: Adresszeile beim Login auf Facebook

An der Internetadresse ist leicht zu erkennen, ob der Datenaustausch verschlüsselt oder unverschlüsselt passiert, denn die Internetadresse wechselt von http (Hypertext Transfer Protocol) auf https (Hypertext Transfer Protocol Secure). Abbildung 16 zeigt beispielsweise die Adresszeile des Browsers bei einem Login-Versuch auf „Facebook“.

Der Client (mein Browser „Firefox“) verbindet sich mit dem Facebook-Server und sendet ein so genanntes „Client Hello“. Dies ist eine Startmeldung, die dem Server zu verstehen gibt, dass sich jemand mit ihm verschlüsselt „unterhalten will“. Nun müssen sich Firefox und der Facebook-Server darauf verständigen, welche Verschlüsselungsmethode und welcher Schlüssel verwendet werden. Theoretisch könnte der Server einfach seinen öffentlichen Schlüssel senden und der Client verschlüsselt die gesamten Daten mit diesem öffentlichen Schlüssel und schickt sie dem Server, doch bei grösseren Datenmengen ist dies recht ineffizient da es ziemlich aufwändig ist, grössere Daten mit dem RSA-Verfahren auszutauschen.

Es wird daher von beiden Seiten ein symmetrisches Verfahren verwendet welches von den beiden Partien zunächst abgemacht wird (DES, 3DES, Idea und RC4). Welches Verfahren verwendet wird, hängt davon ab, welche Verschlüsselung der Client und der Server beherrschen. Nun muss jedoch ein Schlüssel (Session-Key) ausgetauscht werden, so dass diese Verschlüsselung sicher ist. Dies geschieht mit dem RSA- oder mit dem Diffie-Hellman Verfahren. Beide Partien haben dann den Schlüssel, welcher für das Symmetrische Verfahren verwendet wird, ohne dass eine Drittperson, die alles mithört, den Schlüssel knacken kann. Nun wird der gesamte Nachrichten-verkehr dieser Session mit diesem Schlüssel verschlüsselt und bei jeder Neuverbindung wird ein neuer Schlüssel gewählt.

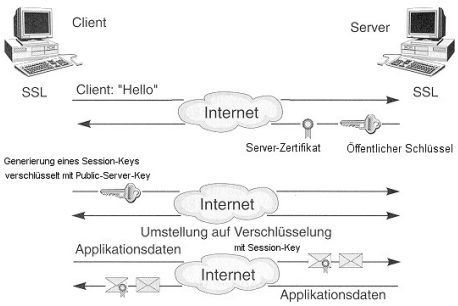

Abb. 17: grobe Übersicht SSL-Verschlüsselung

Damit der Client sicher ist, dass er tatsächlich mit Facebook verbunden ist, schickt der Server noch ein Server-Zertifikat, welches bei einer Zertifizierungsstelle registriert ist (vgl. Abb 17.) Dies ist eine Digitale Signatur, die mit dem privaten Schlüssel des Facebook-Servers verschlüsselt wurde und mit dem öffentlichen Schlüssel des Servers kann man die Digitale Signatur entschlüsseln. Man weiss also, dass der Kommunikationspartner tatsächlich den privaten Schlüssel zum gelieferten öffentlichen Schlüssel besitzt. Eine unabhängige Schlüsselzertifizierungsstelle garantiert, dass es sich dabei tatsächlich um Facebook handelt.

Links: http://nwn.de/hgm/krypto/mod-asym.htm

http://www.cdc.informatik.tu-darmstadt.de/TI/Lehre/WS99_00/Seminar/Kryptographie_im_Internet_und_Intranet/Ausarbeitungen/Ausarbeitung_Thomas_Rauch/Ausarbeitung/doc/thomas-rauch-3.htm

http://kuno-kohn.de/crypto/crypto/des.htm (Erklärung zur DES-Verschlüsselung)