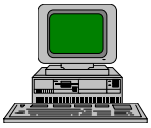


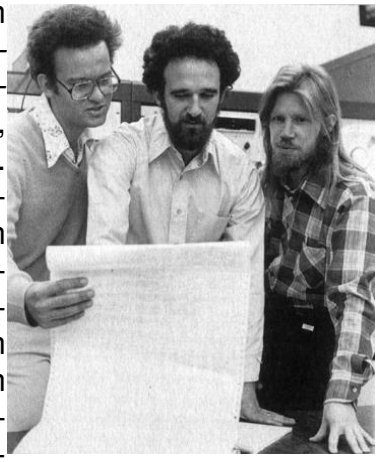
Public Key Verfahren

Im letzten Kapitel wurde die Funktionsweise der asymmetrischen Verschlüsselung, auch Public Key Verfahren, schematisch aufgezeigt. An dieser Stelle wollen wir zuerst kurz auf die Entdeckung dieses Verfahrens eingehen und anschliessen den historisch wohl wichtigsten Vertreter die RSA-Verschlüsselung anschauen.

Durch den zunehmenden Einsatz von Computern in der Kryptologie wurde das Problem des Schlüsseltausches sehr zentral. Zwei einfache Überlegungen zeigten, dass es theoretisch möglich sein musste ein konkretes Verfahren für die asymmetrische Verschlüsselung zu finden:

> **Überlegung 1:** Nehmen wir an, dass Alice an Bob einen verschlüsselte Nachricht per Post zukommen lassen will ohne das sie vorgängig miteinander einen geheimen Schlüssel abmachen müssen. Alice steckt die Nachricht in eine Kiste und verschliesst diese Kiste mit einem Vorhängeschloss, zu dem nur sie einen Schlüssel hat. Anschliessend schickt sie Bob das Paket per Post zu. Bob hängt nun seinerseits ein Vorhängeschloss an die Kiste, zu dem nur er den Schlüssel hat. Er schickt das Paket per Post an Alice zurück. Alice entfernt mit ihrem Schlüssel das von ihr hingefügte Schloss. Sie schickt das Paket per Post an Bob. Die Nachricht ist immer noch vor neugierigen Augen geschützt, denn Bob's Schloss hängt noch an der Kiste. Wenn Bob nun das Paket erhalten hat, entfernt er mit seinem Schlüssel sein Schloss und kann die Nachricht lesen. Alice und Bob haben somit eine Nachricht ausgetauscht, ohne einen gemeinsamen Schüssel abzumachen.
>
> **Überlegung 2:** Nehmen wir an, jedes Postamt in Land verfügt über (offene!) Vorhängeschlösser vom Typ 'Bob' (= public key). Alle diese 'Bob'-Schlösser lassen sich mit einem Schlüssel öffenen von dem es nur ein Exemplar gibt und diesen Schlüssel (= privat key)hat Bob. Wenn nun Alice an Bob eine sichere Nachricht übermitteln will, so sendet holt sie sich auf dem Postamt ein 'Bob'-Schloss. Sie versorgt die Nachricht in einer Kiste und verschliesst diese mit dem 'Bob'-Schloss. Niemand ausser Bob, auch nicht die Versenderin Alice (!), kann nun die Kiste wieder öffnen. Sie kann getrost über das (korrupte?) Postnetz versendet werden.

In der Geschichte der Kryptologie gelten Whitfield Diffie[1], Martin Hellman[2] und Ralph Merkle[3] (vgl. Abbildung) als Erfinder der asymmetrischen Verschlüsselung. Sie prägten 1975 als erste die Begriffe *öffentlicher Schlüssel (public key)* und *privater Schlüssel (privat key).* Die oben erwähnten Überlegungen zeigten ihnen, dass ein solches Verfahren grundsätzlich existieren konnte. Allerdingst reichte es natürlich nicht aus, von Vorhängeschlössern und 'normaler' Post zu sprechen. Es mussten mathematische Verfahren gefunden werden, die diese Überlegungen auf die computergestützte Kommunikation übertragen lassen. Das wichtigste an den zu findenden Verfahren war, dass es sich um sogenannte Einwegfunktionen handeln musste. Man stelle sich dazu nochmals das Vorhängeschloss vor. Jedermann kann ohne Probleme und in kürzester Zeit ein solches Schloss einschnappen lassen. Öffnen lässt es sich aber nur durch den passenden Schlüssel, resp. mit nicht zu unterschätzender Gewaltanwendung.



Merkle, Hellman, Diffie

[1] Whitfield Diffie, geboren 1944, aus New York. Er studierte am MIT (Massachusetts Institute of Technology) und macht 1965 seinen Abschluss. Nach einem Zusammentreffen mit Hellman schrieb er sich als Doktorand an der Standford University in Kalifornien.

[2] Martin Hellman, geboren 1946, aus der Bronx. Professor an der Standford University in Kalifornien.

[3] Ralph Merkle, Mitarbeiter in der Forschungsgruppe von Professor Hellman.

Auf zwei mathematische Operationen wurde ein besonderes Augenmerk gerichtet. Erstens auf die Faktorisierung. Zwei Zahlen (insbesondere grosse Primzahlen) lassen sich mit geringem Aufwand miteinander multiplizieren. Muss aber jemand der nur das Produkt kennt eine Faktorzerlegung durchführen, so ist das mit einem grossen zeitlichen Aufwand verbunden. Die zweite interessante Funktion ist die Modulo-Funktion, auch Rest-Funktion genannt. Sie berechnet aus einer Division den verbleibenden Rest. Bsp. 26 mod 5 ergibt 1 oder 32 mod 9 ist 5. Die Modulo-Funktion ist nicht umkehrbar. Aus dem Resultat kann nicht (eindeutig) auf die ursprüngliche Zahl geschlossen werden.

Ronald Rivest. Adi Shamir. Leonard Adleman

Obwohl Diffie, Hellman und Merkle angestrengt forschten waren nicht sie es, die das erste vollständige mathematische Verfahren entwickeln konnten, das den Anforderungen der asymmetrischen Verschlüsselung genügte. Sie hatten neuen Wind in die Forschung der Kryptologie gebracht und die grundsätzlichen Ideen zur Public Key Verschlüsselung aufgestellt. Die Lorbeeren für das erste einsetzbare Verfahren gehört aber dem Trio Ronald Rivest, Adi Shamir und Leonard Adleman vom MIT (Massachusets Institute of Technology). Das von ihnen 1977 aufgezeigte RSA-Verfahren gilt als das ursprüngliche asymmetrische Verschlüsselungsverfahren. Die Buchstaben RSA stehen für Rivest, Shamir und Adleman. Im zweiten Teil dieses Kapitels werden wir das RSA-Verfahren an einem einfachen Beispiel anschauen.

Am 18. Dezember 1997 (!) zeigte es sich, dass die oben beschriebene Geschichte der Public Key Kryptologie nicht die ganze Wahrheit ist. An besagtem Tag hielt ein gewisser Clifford Cocks in Cirencester einen vielbeachteten Vortrag an der Konferenz für Mathematik und ihre Anwendungen. Cocks war ein Mitarbeiter des GCHQ des Government Communications Headquarter der britischen Regierung. Es handelt sich dabei um eine Abteilung, die aus dem legendären Blechley-Park-Zeitalter hervorgegangen war. Alle Mitarbeiter des GCHQ waren ihr Leben lang zu Verschwiedenheit über ihre Arbeit verpflichtet.

Am GCHQ entwickelten James Ellis, Clifford Cocks und Malcolm Williamson bereits 1975 die wesentliche Elemente für ein Verschlüsselungsverfahren, das ebenfalls den Public Key Anforderungen genügte. Die Briten mussten stumm mit ansehen, wie drei Jahre später Diffie, Hellman, Merkle, Shamir und Adleman ihre Entdeckungen erneut machten. Erst am erwähnten Vortrag von Cocks 1997 wurde es ihm gestattet kurz über die bis anhin geheimen Entdeckungen des GCHQ zu berichten.

Weiterführende Links (7.12.03)

http://www.pro-privacy.de/pgp/tb/de/rsa.htm

http://www.gnupg.org/gph/de/manual/x96.html

http://www.ifi.unizh.ch/ikm/Vorlesungen/sec/rsa.pdf

http://www.hh.schule.de/julius-leber-schule/melatob/historyrsa.html