Facharbeit

Public-Key-Verfahren(PGP)

Stephan Larws

Informatik 02

Inhaltsverzeichnis

1.) DES
2.) Das Problem der Schlüsselverteilung
    - Lösung von Diffie, Hellman und Merkle
3.) Die Idee der asymmetrischen Verschlüsselung
4.) RSA
5.) PGP – Pretty Good Privacy
    - Das Projekt PGPi

1.) DES – Data Encryption Standard

Durch die Einführung des ASCII-Codes (American Standard Code for Informaiton Interchange) konnten Textnachrichten auf recht einfache aber doch effiziente Weise verschlüsselt werden. Jedem Buchstaben im Alphabet wird eine Binärzahl zugeordnet, damit der Computer die Zeichen verarbeiten kann. So würde zum Beispiel das Wort HALLO wie folgt in ASCII ausssehen:

1001000 1000001 1001100 1001100 1001111

Nun kann man durch Vereinbarung eines Schlüsselwortes diese Zahlenfolge einfach durch Addition des Schlüsselwortes verschlüsseln. (Die Addition von Binärzahlen erfolgt nach zwei Regeln: unterschiedliche Zahlen ergeben 1, gleiche Zahlen Null)

Botschaft = HALLO	1001000 1000001 1001100 1001100 1001111
Schlüssel = DAVID	1000100 1000001 1010110 1001001 1000100
Geheimtext	0001100 0000000 0011010 0000101 0001011

Der Geheimtext kann nun durch Addition des Schlüssels wieder in die ursprüngliche Botschaft verwandelt werden. Dieses Verfahren fand aber nur in den Anfängen des Computers seine Einsätze

Als Mitte der siebziger Jahre der Computer immer mehr Menschen zugänglich wurde, musste ein neues Verschlüsselungsverfahren her. Horst Feistel, ein Mitarbeiter von IBM, hatte das damals weit verbreitete Verschlüsselungsverfahren Luzifer entwickelt. Hierbei wird die Botschaft zuerst in eine ASCII-Zahlenfolge verwandelt, diese wird dann in Blöcke zu je 64 Zahlen aufgeteilt. Diese Blöcke werden aufgeteilt in Rechts^0 und Links^0, Rechts^0 und Links^0 werden addiert und bilden den neuen Block Rechts^1. Rechts^0 wird umbenannt in Links^1. Dies ist eine Runde, das Verfahren wird etwa 16 Runden lang angewandt. Durch den vom Sender und Empfänger vereinbarten Schlüssel können sich die genauen Einzelheiten der Verwirbelungsfunktion ändern. Da der Computer nur mit Zahlen arbeitet gibt es eine Unzahl von möglichen Schlüsseln. Dies machte Luzifer zu einem sehr starken Verschlüsselungsverfahren, und um es für die amerikanischen Geheimdienste noch möglich zu machen, dass abgehörte Nachrichten entschlüsselt werden können, führte die NSA eine Begrenzung von etwa 100 000 000 000 000 000 (56 Bits) Schlüsseln ein. Dieser neu geschaffene Standard wurde 1976 als DES (Data Encryption Stardard) bekannt. DES ist heute immer noch der offizielle amerikanische Verschlüsselungsstandard.

2.) Das Problem der Schlüsselverteilung

Seit dem Beginn der Verschlüsselung bei den alten Griechen gab es das Problem der Schlüsselverteilung. Wie konnten Sender und Empfänger einen gemeinsamen Schlüssel vereinbaren, ohne dass ein Dritter ihn in die Hände bekam? Es sollte bis in die 70er Jahre des 20. Jahrhunderts dauern, bis dieses Problem gelöst wurde.

Lösung von Diffie, Hellman und Merkle

Die drei Kryptographiebegeisterten Whitfield Diffie, Martin Hellman und Ralph Merkle gingen das Problem wie folgt an. Sie stellten sich vor, Alice und Bob wollten sich eine Nachricht schicken, doch Eve sei versucht, die Nachricht abzufangen und zu lesen. Nun könnten Alice und Bob sich jedes Mal treffen, wenn sie sich eine Nachricht schicken wollten, um den Schlüssel zu vereinbaren, doch das wäre sehr

umständlich und mit viel Zeitaufwand verbunden. Eine Alternative wäre, dass Alice ihre Nachricht in eine eiserne Kiste packte, sie mit einem Vorhängeschloss verriegelte und dann an Bob schickte. Bob wiederum könnte die Kiste nicht öffnen, aber er könnte auch ein Vorhängeschloss anhängen und sie wieder an Alice zurück schicken. Alice nähme nun ihr Schloss ab und schickte die Kiste mit der Nachricht wieder an Bob, der die Kiste nun öffnen könne, da nur noch sein Schloss davorhinge. Diese Idee war revolutionär, da sich Sender und Empfänger nicht mehr auf einen einzigen Schlüssel einigen mussten. Jetzt brauchte man nur noch ein Verfahren, das diese Methode umsetzen konnte: nähme man z. B. das Caesar-Verfahren, verschlüsselte mit zwei Schlüsseln und entfernte sie in umgekehrter Reihenfolge, so bekäme man nicht den originalen Klartext, sondern ein Wirrwarr an Buchstaben.
Es war schließlich Martin Hellman aus dem Trio, dem es gelang, ein Verfahren zu finden, das diese Methode des Schlüsselaustauschs umsetzen konnte. Einen Nachteil hat dieses Verfahren allerdings, der Sender muss immer auf den Empfänger warten, bis dieser antwortet, damit ein Schlüssel vereinbart werden kann, und dann kann die eigentliche Nachricht erst geschickt werden.

3.) Die Idee der asymmetrischen Verschlüsselung

Das Problem der Schlüsselverteilung war nun gelöst, doch das Trio Diffie, Hellman, Merkle setzte sich nicht zur Ruhe. Eines Tages hatte Diffie wieder eine revolutionäre Idee. Was wäre, wenn Alice einen Schlüssel hätte, mit dem sie die Nachricht verschlüsselte, sie aber einen anderen Schlüssel bräuchte um den Geheimtext wieder zu entschlüsseln. Dann könnte Bob einen Schlüssel, den öffentlichen Schlüssel, in eine Liste stellen, die jedem zugänglich wäre und Alice könnte mit diesem Schlüssel dann ihre Nachricht verschlüsseln und an Bob schicken. Eve könnte die Nachricht abfangen, aber um sie zu entschlüsseln bräuchte sie Bobs privaten Schlüssel. Da dieser aber geheim ist, hat Eve keine Chance an den Inhalt der Nachricht zu gelangen. Damit wäre es dann auch möglich eine verschlüsselte Nachricht zu senden, ohne dass vorher der Nachrichtenverkehr zwischen den einzelnen Personen erfolgt, um einen Schlüssel auszutauschen. Diffie hatte zwar noch kein spezielles Verfahren, aber die Idee war genial. Also machten sich die drei an die Arbeit, ein Verfahren zu entwickeln, mit dem man diese Idee umsetzen

konnte. Doch sollten es diesmal nicht Diffie, Hellman und Merkle sein, die als erstes zur Lösung dieses Problems gelangten.

4.) RSA

Drei Wissenschaftlern vom MIT, Ronald Rivest, Adi Shamir und Leonard Adleman, fanden im April 1977, nach anderthalb Jahren Arbeit, endlich eine Einwegfunktion, die nur mit besonderen Informationen umkehrbar ist. Die Funktion musste folgende Kriterien erfüllen.

1.) Alice muss einen öffentlichen Schlüssel haben, mit dem Bob und andere verschlüsseln können, es ihnen aber nicht möglich ist, die Nachricht damit zu entschlüsseln.
2.) Alice besitzt einen privaten Schlüssel, der es ihr erlaubt, die Verschlüsselung rückgängig zu machen.

Die gefundene Funktion benutzt Primzahlen als Schlüssel. Die beiden Zahlen *p* und *q* bilden den privaten Schlüssel. Es wird das Produkt aus *p* und *q* als öffentlicher Schlüssel verwendet. Dies klingt zunächst sehr primitiv und anfällig, wenn aber *p* und *q* im Bereich von 10^{150}, so liegt das Produkt aus beiden im Bereich von 10^{300}, und eine solche große Zahl ist mit heutigen Mitteln nicht in ihre Primfaktoren zerlegbar.

Dieses Verfahren, benannt nach seinen Erfindern (Rivest, Shamir, Adleman) RSA, hat die Kryptographie vor 20 Jahren komplett umgekrempelt. Seitdem ist es Menschen möglich, ohne sich vorher gesprochen zu haben, sicher Nachrichten auszutauschen. Da man hierbei mit öffentlichen Schlüsseln arbeitet, wird es Public-Key-Verfahren genannt. Viele moderne Programme für den PC benutzen den RSA Algorithmus für die Verschlüsselung der Nachrichten des Benutzers. Eines auf das ich näher eingehen möchte, ist PGP.

5.) PGP – Pretty Good Privacy

Phil Zimmermann hatte sich zum Ziel gesetzt, einem breiten Publikum hochgradige sichere Verschlüsselung zugänglich zu machen. Er machte sich sowohl RSA als auch IDEA zu Nutzen. IDEA ist ein Verfahren ähnlich DES und hat den entscheidenden Vorteil gegenüber RSA, dass es sehr viel schneller ausführbar ist. Zimmermann baute in den späten 80er Jahren bei sich zu Hause an seinem Computer Stück für Stück seine Software zusammen. Sein Ziel war es, RSA zu beschleunigen.

Da der Rechenaufwand sehr hoch ist, eine lange Nachricht mit RSA zu verschlüsseln und zu entschlüsseln, benutzte Zimmermann zur Verschlüsselung der Nachricht nur IDEA (International Data Encryption Algorithm – ein Nachfolger von DES). Da IDEA ein symmetrisches Verschlüsselungsverfahren ist, muss nun noch ein Schlüssel ausgetauscht werden. Dies macht Zimmermann mit RSA. Die recht „kleinen“ Schlüssel können so auf sehr sicherem und effizientem Wege zum Empfänger gebracht werden, der dann die Nachricht schnell entschlüsseln kann. Zimmermann wagte im Juli 1991 den entscheidenden Schritt und stellte PGP auf einem Bulletin Board System im Internet als Download zur Verfügung. Schnell verbreitete sich PGP und Zimmermann erhielt Lobes-Emails aus der ganzen Welt.

Doch in den USA wurde Zimmermann zur Zielscheibe der Kritik. Die RSA Data Security Inc. versuchte Zimmermann zu verklagen, da er den von ihnen patentierten Algorithmus in seinem Produkt ohne Erlaubnis benutzt hatte. Man versuchte ihn nicht nur wegen Verletzung von Patentrechten zu verklagen, sondern auch wegen illegalem Export von Waffen. Da damals in den USA Verschlüsselungsprodukte zu Waffen zählten und Zimmermann keinen Genehmigung für die Verbreitung eines solchen Produktes hatte, begann das FBI gegen ihn zu ermitteln. Doch war es nicht möglich Zimmermann vor Gericht zu bringen, da er das Programm eigentlich nicht exportiert hatte. 1996 wurde die Anklage fallen gelassen und er erhielt auch von RSA Data Security Inc. eine Genehmigung RSA zu benutzen. PGP wurde endlich zu einem legalen Produkt und es entstand ein Projekt, PGP für den nicht kommerziellen Gebrauch zu erhalten und zu verbessern.

Das Projekt PGPi

Dieses Projekt heisst PGPi, Freiwillige haben es gegründet, da PGP an kommerzielle Anwender verkauft und für diese auch weiterentwickelt wird. Ihr Ziel ist, PGP für alle zum privaten Gebrauch zur Verfügung zu stellen und es vor allen Dingen weiterzuentwickeln. Der Quelltext für PGP steht allen zum Download zur Verfügung und wird daher von Hunderten von Programmierern auf Fehler geprüft und verbessert. Genaue Informationen zu Weiterentwicklung von PGP gibt es unter http://www.pgpi.com. Abschließend lässt sich sagen, dass PGP ein sehr hochwertiges Produkt ist, das einem sehr viel Privatssphäre in der offene Welt des Internet gibt, doch leider kann es auch zur Planung illegaler Aktivitäten missbraucht werden, die durch die hochgradige Verschlüsselung auch nicht von den ermittelnden Behörden bemerkt werden.

Benutzte Quellen:

Simon Singh – Geheime Botschaften
http://www.pgpi.com