Kryptographie in Geschichte und Politik

Martin Weissenböck

Das Bedürfnis, zu übertragende Mitteilungen vor dem Zugriff durch Unberufene zu Verbergen, ist sicher so alt wie jede Art der Kommunikation selbst.

Kryptographie war immer eine Domäne der Politik und ein zentraler Teil der Kriegsführung. Im 20. Jahrhundert *führte die Entwicklung des Telegraphen und die Entdeckung der Radiowellen dazu, daß Forderungen nach effektiven Kodierverfahren wieder stärker in den Vordergrund traten. Mit Hilfe des Telegraphen und des Funkverkehrs war es erstmals möglich, eine übergreifende Kommunikation zwischen Teilstreitkräften einer Armee und den Befehlshabern aufzubauen. Ohne den Einsatz der Kryptographie ist der Austausch von Nachrichten jedoch den Angriffen feindlicher Spione ausgesetzt. Erst mit der Entwicklung von kryptographischen Methoden wurde die elektronische Kommunikation für das Militär interessant.*

Ihre Blütezeit erlebte die Kryptographie während des zweiten Weltkrieges, als aus gegebenen Anlaß die wissenschaftliche Forschung auf vielen Gebieten vorangetrieben wurde. Die ersten Digitalrechner der Welt wurden einzig und allein gebaut, um mit ihrer Hilfe die Chiffrierung des Feindes zu dekodieren. Die alliierten Streitkräfte setzten damals alles daran, die von den Deutschen eingesetzte Enigma-Chiffre zu knacken. Das Projekt wurde in England unter der Leitung von Alan Turing ins Leben gerufen.

Nach dem zweiten Weltkrieg nahm die NSA (National Security Agency) die weltweit führende Rolle auf dem Gebiet der Kryptographie ein. Die NSA ist eine Abteilung des Verteidigungsministeriums der USA mit Sitz in Fort Meade, Bundesstaat Maryland, etwa eine halbe Autostunde von Washigton D.C. entfernt. Innerhalb der amerikanischen Regierung mit allen ihren Ministerien ist die NSA die wohl geheimste Institution. Die Geheimhaltung ging sogar soweit, daß eine Zeit lang *die Existenz der NSA von der Regierung bestritten wurde. Das von der Regierung vorgesehene Budget unterliegt ebenfalls strengster Geheimhaltung.* Warum? Die NSA ist der weltweit größte Abnehmer von Computern und Computerzubehör. Wäre das Budget bekannt, wäre auch eine grobe Abschätzung der installierten Rechnerleistung möglich.

(Kursiv geschriebener Text zitiert aus dem Buch „PGP - Pretty Good Privacy“)

Die Anwendung mathematischer Prinzipien auf die elektronische Post gehört gegenwärtig zu den spannendsten Entwicklungen im Bereich der Telekommunikation. Technische und mathematische Aufgaben und Lösungen stehen auf der einen Seite, rechtliche und gesellschaftspolitische Fragen auf der anderen. Hier einige Diskussionpunkte:

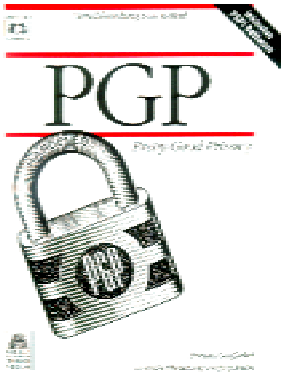
- Wenn ich im Zuge einer Bestellung per E-Mail meine Kreditkartennummer bekanntgebe - wie ist sichergestellt, daß nur der berechtigte Empfänger sie erhält?
- Würden Sie Ihre Briefe lieber in einem (undurchsichtigen) Kuvert oder in einem (durchsichtigen) Plastiksackerl versenden?
- Welche kryptographischen Verfahren und welche mathematischen Grundlagen gibt es, um Nachrichten aller Art vor unberechtigten Lesern zu schützen? (Hier spielen sehr große Primzahlen und deren Produkte eine wesentliche Rolle)
- Welche Verfahren sind praktisch handhabbar, technisch leicht zu implementieren und gleichzeitig sicher genug?
- Darf der Staat unter bestimmten Umständen Zugriff auf die private Korrespondenz seiner Bürger haben? Ist es zur Aufrechterhaltung der öffentlichen Sicherheit und Ordnung notwendig, daß - gegebenenfalls mit mehrfacher Sicherung durch unabhängige (richterliche) Instanzen - Schlüssel zum Öffnen geheimer Informationen bereitgestellt werden müssen? Eine Aufgabe, die beispielsweise den beiden GSM-Anbietern in Österreich Kosten in in dreistelliger Millionenhöhe bereiten würde, Kosten, die natürlich dann wieder von jenen Kunden zu tragen sind, deren Gespräche der Große Bruder gerne abhören möchte.
- Ist das Vertrauen der Bürger in den Staat groß genung, um diesen Teil der Privatsphäre preiszugeben?
- Würden bei entsprechender gesetzlicher Verpflichtung nicht wieder nur „die Guten“ die Dummen sein, da sie beim Einhalten der Regeln ihre Privatsphäre preisgeben, „die Bösen“ aber sowieso solche Verfahren einsetzen würden, deren Öffnung praktisch unmöglich ist?
- Was ist alles im Dienste der nationale Sicherheit möglich? Der Begriff wird in den USA groß geschrieben, daher kann damit (fast) alles legitimiert werden.

PGP - Pretty Good Privacy

Das Buch „PGP - Pretty Good Privacy“ gibt einen ausgezeichneten Überblick über

- die Verwendung des Programms PGP (das Programm liegt auf Diskette bei!),
- die Grundlagen der Kryptographie,
- Geschichte und Politik der Kryptographie (der obenstehende Beitrag ist diesem Kapitel entnommen),
- die Frage „Privatsphäre als öffentliches Gut“,
- Patente und (amerikanische) Exportbestimmungen,
- die Rolle des Phil Zimmermann, der zur weltweiten Verbreitung von PGP einen unschätzbar wertvollen Beitrag geleistet hat,
- den praktischen Einsatz von PGP,
- die Weitergabe und Zertifizierung von elektronischen Schlüsseln,
- Installationshinweise,
- PGP-Programmversionen und
- die mathematischen Grundlagen der Kryptographie.

Der Einsatz von PGP kann jedem ernsthaft an der Telekommunikation Interessierten nur empfohlen werden. Die Bedienung ist sehr einfach, das Programm Public Domain. Das vorliegende Buch informiert nicht nur über den praktischen Einsatz, sondern auch über die Hintergründe, die zu PGP geführt haben. Eine Pflichtlektüre!



Autor: Simson Garfinkel, deutsche Übersetzung von Jörg Anslik
Titel: PGP - Pretty Good Privacy
Verlag: O'Reilly International Thomson Verlag
Untertitel: Verschlüsselung von E-Mail
Seitenzahl: 408
Preis: ??
ISBN: 3-930673-30-4
Mit Diskette: enthält PGP Version 2.6.3i

Irren ist menschlich. Aber wer richtigen Mist bauen will, braucht einen Computer!

Was halten Sie als Außenstehender von Intelligenz?

Es genügt nicht, keine Meinung zu haben. Man muß auch unfähig sein, sie auszudrücken.

Ich denke, also bin ich hier falsch.