

E-Mail-Verschlüsselung

Referat

2009-05-25

Stefan Hensel

Seminar: Office

Dozent: Peter Medwed

Staatliche Technikerschule Berlin

1 Einleitung

Vier Nachrichten belegen die Wichtigkeit von Datenschutz und Datensicherheit:

- Schaden der deutschen Wirtschaft durch IT-Angriffe: Mehrere Milliarden Euro pro Jahr.¹
- Gmail scannt E-Mails und wertet sie aus.²
- Über 10.000 Laptops verschwinden pro Woche auf US-Flughäfen.³
- Etwa die Hälfte der Bundesbürger würde eine Beratungsstellen nicht mehr per Telefon oder Mail kontaktieren, aus Angst vor der Online-Überwachung.⁴

Verschlüsselung ist längst nicht mehr nur ein Thema für Geheimdienste und Militärs. Auch die technischen Voraussetzungen für einen breiten Einsatz sind gegeben. Dieses Referat behandelt die Grundlagen und praktischen Voraussetzungen der Kryptografie, mit Schwerpunkt E-Mail-Verschlüsselung.

2 Geschichte der Kryptografie

Die Geschichte der Kryptografie soll hier nur kurz umrissen werden. Ziel ist, ihre bedeutendsten Erkenntnisse und Verfahren hervorzuheben.

2.1 Die Anfänge

Bereits im 3. Jahrtausend v. Chr. verschlüsselten Schreiber im Alten Reich Ägyptens religiös-mythologische Texte. Das Motiv war hier weniger die Geheimhaltung, sondern das Tabu: Die Namen mancher Gottheiten durften weder ausgesprochen noch geschrieben werden.⁵

Sparta nutzte die Skytale⁶ zur Übermittlung geheimer Nachrichten: Ein Stab, um den ein Pergamentstreifen gewickelt war. Der Pergamentstreifen wurde entlang des Stabes beschrieben und dann abgewickelt. Der Empfänger musste den Pergamentstreifen um einen Stab mit gleichem Durchmesser wickeln, um den Klartext lesen zu können. Kryptografisch stellt dieses Verfahren eine *Permutation* (Verwürfelung) dar.

Die berühmteste Verschlüsselungstechnik der Antike setzte der römische Feldherr und Diktator Caesar ein. Die *Caesar-Verschlüsselung*⁷ ist eine einfache Verschiebechiffre: Jeder Buchstabe wird z. B. um drei Zeichen im Alphabet verschoben; aus einem A wird so ein D, aus einem K ein N. Damit war die *Substitution* (Ersetzung) in die Kryptografie eingeführt. Die Caesar-Verschlüsselung ist durch Häufigkeitsanalyse leicht zu knacken. Dennoch bilden die in der Antike gefundenen Prinzipien Permutation und Substitution bis heute die Grundlage vieler kryptografischer Algorithmen, z. B. von DES (1976).

¹ "Die wirtschaftlichen Schäden von IT-Angriffen belaufen sich nach Schätzungen des Bundesforschungsministeriums auf mehrere Milliarden Euro pro Jahr - Tendenz steigend." Financial Times Deutschland online 06.04.2009

² Patholog [Pseudonym] 12.07.2008

³ Shah 30.06.2008

⁴ "Die Mehrheit der Befragten würde wegen der Vorratsdatenspeicherung davon absehen, per Telefon, E-Mail oder Handy Kontakt zu einer Eheberatungsstelle, einem Psychotherapeuten oder einer Drogenberatungsstelle aufzunehmen, wenn sie deren Rat benötigen (517 der Befragten). Hochgerechnet entspricht dies über 43 Mio. Deutschen." Arbeitskreis Vorratsdatenspeicherung 2008, S. 1

⁵ Wikipedia (de) 22.05.2009

⁶ Wikipedia (de) 05.04.2009

⁷ Wikipedia (de) 30.04.2009

2.2 Mittelalter und beginnende Neuzeit

Das „dunkle Zeitalter“ Europas brachte in der Kryptografie keine neuen Erkenntnisse. Vorwiegend wurden die antiken Verfahren weiter benutzt; daneben finden sich naive „Geheimschriften“, in denen die Buchstaben des Alphabets durch mehr oder weniger phantasievolle Symbole ersetzt werden.⁸

Eine entscheidende Verbesserung der althergebrachten Caesar-Verschlüsselung fand Blaise de Vigenère im 16. Jahrhundert.⁹ Ein „Schlüssel“ legte für jeden Buchstaben des Klartexts den Abstand für die Verschiebechiffre fest: Lautet dieser Schlüssel z. B. „BED“, so wird das erste Zeichen des Klartexts um eine Stelle im Alphabet, der zweite um vier, der dritte um drei verschoben. Ist der Schlüssel verbraucht, wird er neu über den Klartext gelegt, so dass der vierte Buchstabe wieder um eine Stelle verschoben wird. Dieses Verfahren ermöglichte zum ersten Mal die Verwendung parametrisierbarer, systematischer *Schlüssel* und galt für 300 Jahre als unentschlüsselbar.

2.3 Industrialisierung

Kryptografie beruhte bis dahin häufig auf „Security by obfuscation“, also der Geheimhaltung des Verfahrens. Auguste Kerckhoffs formulierte dagegen im Jahr 1883 sein Prinzip, das bis heute der Kryptografie zugrunde liegt: „Nur der Schlüssel ist das Geheimnis“¹⁰. Damit dürfte er einer der ersten Verfechter des Open-Source-Prinzips sein, nach dem die Offenlegung des Codes die Sicherheit nicht etwa vermindert, sondern erhöht, weil der Code kontrollierbar ist und damit die Chance, Fehler und versteckte Hintertüren zu entdecken, drastisch steigt (Peer-Review).

Die zunehmende Industrialisierung ermöglichte schließlich die maschinelle Verschlüsselung. Arthur Scherbius erfand 1918 die „Enigma“¹¹, eine Rotor-Schlüsselmachine, die den Klartext über rotierende Walzen und verschiedene Stromflüsse chiffriert. Auch nach heutigen Maßstäben ist ihre theoretische Verschlüsselungsstärke mit ca. 77 bit recht stark. Sie galt zu ihrer Zeit daher als unentschlüsselbar und weckte das Interesse des Militärs, so dass sie bald vom zivilen Markt verschwand. Das Deutsche Reich unter der Nazi Herrschaft benutzte vorwiegend die Enigma für die Verschlüsselung militärischer Nachrichten. Die Alliierten setzten daher beträchtliche Mittel ein, um diese Verschlüsselung zu knacken. Designfehler der Enigma und strategische Fehler beim Einsatz begünstigten dies. Allerdings ist die Entschlüsselung vor allem den Anstrengungen des polnischen Mathematikers Marian Rejewski zu verdanken. Somit konnten die Alliierten schon bald nach Kriegsbeginn einen Großteil der deutschen Funkprüche entschlüsseln und mitlesen. Dies dürfte den alliierten Sieg über den Faschismus entscheidend beschleunigt haben.

2.4 Zeitalter der Information

Claude Elwood Shannon¹² legte 1949 in seinem Artikel „Communication Theory of Secrecy Systems“ die Prinzipien einer modernen Kryptografie auf starker mathematischer Grundlage fest. Als Computer zunehmend leistungsfähiger wurden, waren damit leistungsfähige kryptografische Verfahren auch außerhalb von Militär und Geheimdiensten verfügbar.

1976 entwickelten IBM und NSA den Data Encryption Standard (DES), der bis heute (in seiner Weiterentwicklung TripleDES) eines der meist genutzten Verfahren darstellt. Etwa gleichzeitig legten Whitfield Diffie und Martin Hellman die Grundlage für das *Public-Key-Verfahren* der asymmetrischen Verschlüsselung. 1991 veröffentlichte Phil Zimmermann schließlich „Pretty Good Privacy“ (PGP) auf Grundlage des asymmetrischen RSA-Algorithmus und ermöglichte damit einer breiten Öffentlichkeit leistungsfähige und günstige asymmetrische Verschlüsselung für den Einsatz in der Kommunikation.

⁸ Müller-Quade o. J.

⁹ Wikipedia (de) 22.05.2009

¹⁰ "Das Kerckhoffs'sche Prinzip oder Kerckhoffs Maxime ist ein 1883 von Auguste Kerckhoffs formulierter Grundsatz der modernen Kryptographie, welcher besagt, dass die Sicherheit eines Verschlüsselungsverfahrens auf der Geheimhaltung des Schlüssels beruht, und nicht auf der Geheimhaltung des Verschlüsselungsalgorithmus. Dem Kerckhoff'schen Prinzip wird oft die sogenannte „Security by Obscurity“ gegenübergestellt: Sicherheit durch Geheimhaltung des (Verschlüsselungs-)Algorithmus, möglicherweise zusätzlich zur Geheimhaltung des Schlüssels." Wikipedia (de) 2009

¹¹ Wikipedia (de) 16.05.2009

¹² Wikipedia (de) 03.05.2009

3 Einsatz der Kryptografie

Kryptografie ist heute nicht mehr nur auf militärischen und geheimdienstlichen Einsatz beschränkt, sondern in der Informationstechnik unverzichtbar. So ermöglichen erst kryptografische Verfahren e-Commerce und Online-Banking.

Grundsätzlich muss man zwei Einsatzorte unterscheiden:

- lokale Verschlüsselung – z. B. Dateien, Ordner, Partitionen
- Remote-Verschlüsselung der Kommunikation, z. B. im Internet

E-Mail-Verschlüsselung liegt hierbei zwischen beiden Kategorien: Zum einen wird hier per definitionem Kommunikation verschlüsselt, zum anderen aber liegt der Inhalt auch nach dem Ende der Kommunikation verschlüsselt vor (im Gegensatz z. B. zu HTTPS).

4 Symmetrische und asymmetrische Verschlüsselung

4.1 Motivation für die asymmetrische Verschlüsselung

Ein Grundproblem der Kryptografie ist der Schlüsselaustausch. Bei der symmetrischen Verschlüsselung benutzen beide Kommunikationspartner den selben Schlüssel; die Sicherheit der Verschlüsselung hängt daher von der Sicherheit des Kommunikationskanals ab. Bei der Kommunikation im Internet mit vielen, häufig persönlich unbekannten Partnern ist dieses „Schlüsselaustauschproblem“ prinzipiell unlösbar. Zudem steigt mit der Zahl der Kommunikationspartner die Zahl der benötigten Schlüssel quadratisch an.

Beide Probleme löst die asymmetrische Verschlüsselung¹³. Sie teilt den Schlüssel in zwei Teile: einen privaten, geheim zu haltenden, und einen öffentlichen Schlüssel. Um eine Nachricht zu verschlüsseln, benutzt der Sender den öffentlichen Schlüssel des Empfängers. Zum Entschlüsseln benötigt der Empfänger nun seinen privaten Schlüssel. Hier kann der Schlüssel auch über einen unsicheren Kanal übertragen werden (gewöhnliche Internet-Verbindung), und die Zahl der Schlüssel ist nur noch linear von der Zahl der Kommunikationspartner abhängig.

Natürlich sind die Verfahren der symmetrischen Verschlüsselung nicht auf die asymmetrische Verschlüsselung anwendbar. Daher mussten für sie neue kryptografische Verfahren entwickelt werden, die hauptsächlich auf drei mathematischen Problemen beruhen:

- Faktorisierungsproblem
- Diskrete Logarithmen
- Elliptische Kurven

4.2 Hybride Verschlüsselung

Der größte Nachteil der asymmetrischen Verschlüsselung besteht im prinzipiell höheren Rechenaufwand. Er ist typischerweise um den Faktor 1.000 höher als bei der symmetrischen Verschlüsselung. Die in der Praxis angewendeten Verfahren (PGP und S/MIME) benutzen daher eine *hybride Verschlüsselung*. Dabei wird der Klartext zunächst symmetrisch verschlüsselt und nur der (relativ kurze) Schlüssel zusätzlich asymmetrisch verschlüsselt.

4.3 PGP und S/MIME

PGP¹⁴ und S/MIME¹⁵ sind die beiden Public-Key-Verfahren, die in der Praxis am häufigsten angewandt werden. Beides sind hybride Verschlüsselungssysteme. Der Hauptunterschied liegt in der PKI (Public Key Infrastructure):

Unter PGP kann jeder ein Schlüsselpaar für sich erzeugen und den öffentlichen Schlüssel bekanntgeben. Die Schlüsselservers sind weltweit synchronisiert, so dass jeder Teilnehmer recht

¹³ Wikipedia (de) 11.05.2009

¹⁴ Wikipedia (de) 30.03.2009

¹⁵ Wikipedia (de) 18.05.2009

einfach gefunden werden kann. Ob ein Schlüssel vertrauenswürdig ist, muss der Teilnehmer allerdings selbst entscheiden. Dabei helfen abgestufte Vertrauensstufen und die Möglichkeit, Schlüssel mehrfach zu signieren („Web of Trust“).

Bei S/MIME heißen die öffentlichen Schlüssel „Zertifikate“. Sie werden ausschließlich von Zertifizierungsstellen herausgegeben. Das Vertrauen in einen Schlüssel hängt davon ab, ob man der Zertifizierungsstelle vertraut. Zudem sind die meisten Zertifizierungsstellen privatwirtschaftlich, was für eine breite Akzeptanz des Verfahrens eine Hemmschwelle darstellt. So findet sich S/MIME auch überwiegend in der Kommunikation zwischen Unternehmen, während private Nutzer – wenn überhaupt – meist PGP bevorzugen.

S/MIME und PGP beruhen dabei zwar auf den gleichen Verfahren und setzen auch z. T. die gleichen Algorithmen ein, sind aber untereinander vollständig inkompatibel. Im Gegensatz zu anderen Konkurrenzsituationen in der IT (Windows vs. Linux vs. Mac, MS Office vs. OpenOffice) beflügelt diese Situation aber nicht die Entwicklung und den Einsatz der Kryptografie auf breiter Basis, sondern hemmt sie beträchtlich.

5 Quellenverzeichnis

Arbeitskreis Vorratsdatenspeicherung (2008): Forsa-Umfrage: Vorratsdatenspeicherung verhindert sensible Gespräche. Pressemitteilung des Arbeitskreis Vorratsdatenspeicherung vom 03./04.06.2008. Arbeitskreis Vorratsdatenspeicherung. Online verfügbar unter http://www.datenspeicherung.de/data/forsa_2008-06-03.pdf, zuletzt aktualisiert am 2008-06-03 Di, zuletzt geprüft am 2009-05-24 So.

Financial Times Deutschland online (2009): FTD.de - Forschungsprojekt: Alarmanlage gegen Hacker-Angriffe - Forschung. Financial Times Deutschland online. Online verfügbar unter http://www.ftd.de/forschung_bildung/forschung/:Forschungsprojekt-Alarmanlage-gegen-Hacker-Angriffe/497283.html, zuletzt aktualisiert am 2009-04-06, zuletzt geprüft am 2009-05-25 Mo.

Müller-Quade, Jörn (o. J.): Hieroglyphen, Enigma, RSA. Eine Geschichte der Kryptographie. Fakultät für Informatik, Universität Karlsruhe (TH). Online verfügbar unter <http://iaks-www.ira.uka.de/eiss/fileadmin/User/enigma.pdf>, zuletzt aktualisiert am 2006-10-26 Do, zuletzt geprüft am 2009-05-24 So.

Patholog [Pseudonym] (2008): Gmail and expose... Security for Dummies. Online verfügbar unter <http://security4dummies.wordpress.com/2008/07/12/gmail-and-expose/>, zuletzt aktualisiert am 23.05.09, zuletzt geprüft am 2009-05-23 Sa.

Shah, Agam (2008): Laptops Lost Like Hot Cakes at US Airports - Business Center - PC World. Monday, June 30, 2008 12:30 PM PDT. PC World Business Center. Online verfügbar unter http://www.pcworld.com/businesscenter/article/147739/laptops_lost_like_hot_cakes_at_us_airports.html, zuletzt aktualisiert am 2009-05-23, zuletzt geprüft am 2009-05-23 Sa.

Wikipedia (de) (2009): Claude Elwood Shannon – Wikipedia. Wikipedia (de). Online verfügbar unter http://de.wikipedia.org/wiki/Claude_Shannon, zuletzt aktualisiert am 2009-05-03, zuletzt geprüft am 2009-05-24 So.

Wikipedia (de) (2009): Asymmetrisches Kryptosystem – Wikipedia. Wikipedia (de). Online verfügbar unter http://de.wikipedia.org/wiki/Asymmetrisches_Kryptosystem, zuletzt aktualisiert am 2009-05-11, zuletzt geprüft am 2009-05-24 So.

Wikipedia (de) (2009): S/MIME - Wikipedia, the free encyclopedia. Wikipedia (de). Online verfügbar unter <http://en.wikipedia.org/wiki/S/MIME>, zuletzt aktualisiert am 2009-05-18, zuletzt geprüft am 2009-05-25 Mo.

Wikipedia (de) (2009): OpenPGP – Wikipedia. Wikipedia (de). Online verfügbar unter <http://de.wikipedia.org/wiki/OpenPGP>, zuletzt aktualisiert am 2009-03-30, zuletzt geprüft am 2009-05-25 Mo.

Wikipedia (de) (2009): Enigma (Maschine) – Wikipedia. Wikipedia (de). Online verfügbar unter [http://de.wikipedia.org/wiki/Enigma_\(Maschine\)](http://de.wikipedia.org/wiki/Enigma_(Maschine)), zuletzt aktualisiert am 2009-05-16, zuletzt geprüft am 2009-05-24 So.

Wikipedia (de) (2009): Skytale – Wikipedia. Wikipedia (de). Online verfügbar unter <http://de.wikipedia.org/wiki/Skytale>, zuletzt aktualisiert am 2009-04-05, zuletzt geprüft am 2009-05-25 Mo.

Wikipedia (de) (2009): Geschichte der Kryptographie – Wikipedia. Wikipedia (de). Online verfügbar unter http://de.wikipedia.org/wiki/Geschichte_der_Kryptographie, zuletzt aktualisiert am 2009-05-22, zuletzt geprüft am 2009-05-24 So.

Wikipedia (de) (2009): Kerckhoffs' Prinzip – Wikipedia. Wikipedia (de). Online verfügbar unter http://de.wikipedia.org/wiki/Kerckhoffs%E2%80%99_Prinzip, zuletzt aktualisiert am 2009-03-07, zuletzt geprüft am 2009-05-24 So.

Wikipedia (de) (2009): Verschiebechiffre – Wikipedia. Wikipedia (de). Online verfügbar unter <http://de.wikipedia.org/wiki/C%C3%A4sar-Chiffre>, zuletzt aktualisiert am 2009-04-30, zuletzt geprüft am 2009-05-24 So.