VP WAP
„Kryptographie “

Martin Hargassner, Claudia Horner, Florian Krisch
Universität Salzburg

11. Juli 2002

Übersicht

- Definiton
- Ziele
- Entwicklung
- Private- / Public-Key Verfahren
- Sicherheit
- Anwendungsbeispiel: PGP
- Gesellschaftliche Relevanz

Definition & Ziele

- Unter *Kryptographie* versteht man die Disziplin, die sich mit der Entwicklung und Bewertung von Verschlüsselungsverfahren (Kryptosystemen) zum Schutz (geheimer) Daten vor unbefugten Zugriffen befasst.

- Die *Kryptoanalyse* beschäftigt sich mit der Analyse Kryptographischer Verfahren, um diese zu brechen, bzw. sicherer zu machen.

- Ziele
  - ⋆ Vertraulichkeit
  - ⋆ Integrität
  - ⋆ Authentizität
  - ⋆ Nichtabstreitbarkeit

Entwicklung

- Transpositionsalgorithmus
- Substitutionsalgorithmus
  - ⋆ Beispiel:

    Klartext:

    a b c d e f g h i j k l m n o p q r s t u v w x y z

    Geheimtext:

    D E F G H I J K L M N O P Q R S T U V W X Y Z A B C
  - ⋆ Chiffrierzylinder
  - ⋆ Rotormaschinen
- Moderne Verfahren
  - ⋆ Symmetrische Verfahren
  - ⋆ Asymmetrische Verfahren

Symmetrische Verfahren (1)

- Ein Schlüssel für Ver- und Entschlüsselung
- Schlüssellänge 64+ Bit
- Block Cipher
- Transpositionen der Blöcke
- Sicherheit beruht auf Geheimhaltung des Schlüssels
- Key Space: $2^{64} \approx 7.2 * 10^{16}$ verschiedene Schlüssel

Symmetrische Verfahren (2)

- DES / 3DES (Data Encryption Standard)
- IDEA (International Data Encryption Algorithm)
- RC4
- Blowfish

Asymmetrische Verfahren

- Private Key - Public Key
- Kein Sicherheitsrisiko beim Schlüsselaustausch
- Sicherheit beruht auf schwer umkehrbaren mathematischen Verfahren
- Z. B. mit grossen Primzahlen

Asymmetrische Verfahren: Mathematik 1

Sei $n = pq$ das Produkt zweier verschiedener Primzahlen p, q. Es gilt für jede Zahl $m \leq n \in \mathbb{N}$, $k \in \mathbb{N}$ die Gleichung

$$m^{k(p-1)(q-1)+1} \bmod n = m$$

.

Man wähle nun zwei natürliche Zahlen e, d, sodass das Produkt

$$e * d = k(p-1)(q-1)+1$$

oben genannter Exponent ist. ($k \in \mathbb{N}$) So gilt:

$$(m^e)^d \bmod n = m$$

.

Asymmetrische Verfahren: Mathematik 2

Die Schlüsselerzeugung erfolgt durch die Wahl zweier (grosser) Primzahlen p, q. Es wird $n = pq$ und $\varphi(n) = (p-1)(q-1)$ berechnet. Die Zahl e wird teilerfremd zu $\varphi(n)$ gewählt, und die Zahl d mit

$$ed \bmod \varphi(n) = 1$$

also

$$ed = 1 + k(p-1)(q-1)$$

für eine natürliche Zahl k.

Den öffentlichen Schlüssel bilden e und n, die Zahl d ist der geheime Schlüssel.

Asymmetrische Verfahren: Mathematik 3

Seien n, e der öffentliche Teil des erzeugten Schlüssels, M die zu verschlüsselnde Nachricht. ($M < n \in \mathbb{N}$). Es gelte $(M, n) \neq 1$. (Ansonsten erzeugt man ein M^* mit $(M^*, n) = 1$.)

Die Zahl E

$$E \equiv M^e \pmod{n}$$

ist die verschlüsselte Nachricht und wird verschickt. Der Empfänger kennt die Zahl d und kann mit

$$E^d \equiv (M^e)^d \equiv M \pmod{n}$$

die Nachricht M rekonstruieren.

Sicherheit

- Angriffsmethoden:
  - ⋆ Statistische Angriffe
  - ⋆ Angriffe auf Schwachstellen im Algorithmus
  - ⋆ Angriffe auf die Übermittlung (Man-In-The-Middle)
  - ⋆ Brute Force Attacke

Sicherheit: Symmetrische Verfahren

- Gelten als sehr sicher
- Keine internen Schwächen
- Angriff durch Ausspionieren des Schlüssels, oder Brute Force Attack
- Rechenzeit nimmt exponential mit Länge des Schlüssels zu

Sicherheit: Asymmetrische Verfahren

- Sicherheit beruht auf Funktion mit aufwändiger Umkehrung
- Spezielle Primfaktoren sind leicht zu errechnen
- Bessere Algorithmen für allgemeine Primzahlen würden asymmetrische Verfahren gefährden
- Man-In-The-Middle Angriffe möglich. Lösung:
  - ⋆ Key Server
  - ⋆ Trust Center
  - ⋆ Dezentrales Network Of Trust

PGP: Pretty Good Privacy

- By Phil Zimmermann, 1991
- Im Eigentum von *Network Associates, Inc.*, http://www.nai.com
- Verwendet symmetrische und asymmetrische Verschlüsselung
- Verschlüsselt Dateien, EMails,...
- Beinhaltet weitere nützliche Sicherheitstools
- Gibt’s frei für individuellen Gebrauch
- Gibt’s frei für fast alle Plattformen
- Key-Authentifizierung durch Network of Trust

PGP: Arbeitsweise

- Public Keys hängen am *Public Key Ring*
- Private Key verschlüsselt und durch Passwort geschützt
- Verschlüsselung:
  - ⋆ Plaintext (komprimiert) $\overrightarrow{SessionKey}$ Cipher Text
  - ⋆ Session Key $\overrightarrow{PublicKey}$ Cipher Key
- Entschlüsselung:
  - ⋆ Cipher Key $\overrightarrow{PrivateKey}$ Session Key
  - ⋆ Cipher Text $\overrightarrow{SessionKey}$ Plaintext

PGP: Digital Signatures

- Identifying Message $\overrightarrow{HashFunktion}$ Output fixer Länge
- Output $\overrightarrow{PrivateKey}$ Signatur
- Signatur $\overrightarrow{PublicKey}$ Identität
- Signaturen beglaubigt durch Network of Trust
- Zertifikate enthalten zusätzliche Information

Gesellschaftliche Relevanz

- Know-How
- Militär & Geheimdienste: Enigma, NSA,. . .
- Privatsphäre vs. Polizeiarbeit
- Analogie Brief - Email
- Verschwörungstheorien

Weiterführende Literatur

- *Cryptography for the Internet*, by Philip R. Zimmermann. Scientific American, October 1998.
- *Privacy on the Line*, by Whitfield Diffie and Susan Eva Landau. MIT Press; ISBN: 0262041677.
- PGP: Documentation, Intro to Crypto
- *Kryptologie*, by Beutelspacher A., 1996, Vieweg & Sohn, Braunschweig. ISBN 3528489901
- *Moderne Verfahren der Kryptographie*, by Beutelspacher A., 1995, Vieweg & Sohn, Braunschweig. ISBN 3528065907
- *Abenteuer Kryptologie*, by Wobst R., 2001, Addison-Wesley, München. ISBN 3827318157
- *Geheime Botschaften*, by Singh S., dt. von Fritz K., 2000, Hanser Verlag, ISBN 3446198733

Das war’s

Wir bedanken uns fürs Zuhören!
Martin Hargassner, Claudia Horner, Florian Krisch