KRYPTOSYSTEME & RSA IM SPEZIELLEN

Kryptosysteme allgemein

Ein Kryptosystem ist eine Vorrichtung oder ein Verfahren, bei dem ein Klartext mithilfe eines Schlüssels in einen Geheimtext umgewandelt wird (Verschlüsselung) und umgekehrt, der Geheimtext wieder in den Klartext rückgewandelt werden kann (Entschlüsselung).

Bei einem Verschlüsselungsverfahren wird eine Nachricht N mit Hilfe einer Funktion E und eines Schlüssels e verschlüsselt:

K = Ee(N)

Die Dekodierung erfolgt mit der (zugehörigen) Funktion D und dem Schlüssel d:

Dd (K) = Dd (Ee(N)) = N .

Die Funktionen E und D sollten effizient berechnet werden können.

Grundsätzlich wird unterschieden zwischen symmetrischer(„Private-Key-Kryptoverfahren“) und asymmetrischer Kryptographie („Public-Key-Kryptoverfahren“).

Symmetrische Kryptographie

Dieses System verwendet für die Ver- und Entschlüsselung die gleichen Schlüssel, was auch zugleich als Nachteil gesehen wird. Da bei der Übermittlung der verschlüsselten Information auch der Schlüssel selbst mit übermittelt werden muss. Somit muss der Schlüssel über einen sicheren Kanal übertragen werden, da die Sicherheit des Verfahrens logischerweise von der Geheimhaltung des Schlüssels abhängt.
Beispiele für dieses Verfahren wären:

- DES (Data Encryption Standard)
- AES (Advanced Encryption Standard), Nachfolger des DES – heute Verschlüsselungsstandard der USA

Daher wurde als Alternative die asymmetrische Kryptographie entwickelt, um den symmetrischen Schlüssel selbst zu verschlüsseln und ihn so über einen unsicheren Kanal übertragen zu können.

[vgl. Swoboda et al. 2008, S. 2f; S. 43]

Asymmetrische Kryptographie

Solche Verfahren wurden 1976 von Diffie und Hellman eingeführt.

Das RSA-Verfahren ist ein Beispiel eines asymmetrischen Verschlüsselungsverfahrens. Es wurde 1977 von Ronald L. **R**ivest, Adi **S**hamir und Leonard **A**dleman am MIT entwickelt. Der

Name RSA steht für die Anfangsbuchstaben ihrer Familiennamen. Es galt damals als das erste asymmetrische Verschlüsselungsverfahren.

Hierbei verwenden Sender und Empfänger jeweils eigene Schlüssel e und d.
Der Schlüssel e wird jeweils öffentlich bekannt gegeben, während der Schlüssel d geheim bleibt.
Ein Schlüsselaustausch des jeweils persönlichen Dekodierungsschlüssels d ist demnach nicht erforderlich.
Demnach ermöglich der öffentliche Schlüssel jedermann, Daten für den Inhaber des privaten Schlüssels zu verschlüsseln, dessen digitale Signaturen zu prüfen oder ihn zu authentifizieren. Der private Schlüssel ermöglicht es seinem Inhaber, mit dem öffentlichen Schlüssel verschlüsselte Daten zu entschlüsseln, digitale Signaturen zu erzeugen oder sich zu authentisieren.

Sicherheit?
Es ist bis heute auch keine Formel bekannt, die es gestattet, schnell beliebig große Primzahlen zu berechnen, oder aus einer gegebenen Primzahl eine noch größere Primzahl herzustellen.
Nach wie vor stehen hier nur Probiermethoden zur Verfügung. Angesichts der riesigen Anzahl der durchzuprobierenden Zahlenwerte führen diese Probiermethoden bei entsprechend langen Schlüsselwerten nicht in vernünftiger Zeit zum gewünschten Ergebnis. (Nach den Abschätzungen der Mathematik gibt es vermutlich 10 mal mehr Primzahlen mit 512 bit Länge, als Atome im Universum.)

[vgl. Swoboda et al. 2008, S. 125ff]

Wo wird das RSA-Verfahren eingesetzt?

- bei der sicheren Anmeldung auf einem entfernten Computer: **secure shell (ssh)**

- beim Email Verkehr
  - Verfahren **PGP** (Pretty Good Privacy)
    auch bei elektronischer Unterschrift
  - S/MIME (Secure / Multipurpose Internet Mail Extensions)
    Standard für die Verschlüsselung und Signatur von MIME-gekapselter E-Mail

- Digitale Signaturen, die u. a. zur sicheren Abwicklung von Geschäften im Internet eingesetzt werden

- beim sicheren Datentransfer auf sicheren Webseiten (https), beispielsweise beim Online-Banking, Internetkauf, Zahlung mit Kreditkarte, etc.

- bei kryptografischen Protokollen wie SSL/TLS

Beispiel

- p, q als zwei große Primzahlen

- öffentlicher Schlüssel zum Chiffrieren (e : encrypt):
  (e; n)
  wobei n = p * q
  und e teilerfremd zu (p - 1) * (q - 1)

- privater Schlüssel zum Dechiffrieren (d : decrypt)
  mit d * e = 1 mod((p – 1) * (q – 1))

Um einen Text zu verschlüsseln, müssen zunächst Buchstaben in Zahlen umgewandelt werden. Dazu verwendet man in der Praxis zum Beispiel den ASCII-Code oder ISO-Werte.

einfaches Beispiel:

Klartext:	H	A	L	L	O
ISO-Wert:	72	65	76	76	79

Chiffrieren: $\mathbf{c' = c^e \bmod n}$
Dechiffrieren: $\mathbf{c = c'^d \bmod n}$

1.	Man wählt zwei Primzahlen **p** und **q**	Wir nehmen **11** und **17**
2.	p und q werden miteinander multipliziert, um n zu erhalten	**n** = 11 x 17 = **187**
3.	Man berechnet die **eulersche Phi-Funktion** phi(n) = (p – 1)(q – 1)	phi(n) = (11 – 1)(17 – 1) = **160**
4.	Man wählt eine **zu phi teilerfremde Zahl e**, für die gilt $1<e<phi(n)$	Wir wählen **e = 7 für den public key**
5.	Man berechnet den Entschlüsselungsexponenten **d als Multiplikativ Inverses von e mod phi(n)**. Es gilt: e*d + k*phi(n) = 1 = ggT (e, phi(n)) Im konkreten Bsp.: 7*d + k*160 = 1 Mit dem euklidischen Algorithmus ggT(a,b) = s*a + t*b	**d = 23 für den private key**
6.	Der Wert e wird zusammen mit n als öffentlicher Schlüssel definiert, der Wert d als privater Schlüssel. Der öffentliche Schlüssel, mit dem verschlüsselt wird, kann nun allgemein bekannt gemacht werden.	der ganze public key besteht also aus zwei Zahlen, nämlich (e; n), hier also (7; 187) der ganze private key

	Der private Schlüssel, muss geheim gehalten werden	besteht dann dem entsprechend aus den Zahlen (d; n), hier also (23; 187)

[vgl. Buchmann 2003, S. 137ff; Wiener 1990]

z…ISO-Wert

Chiffrieren	**Dechiffrieren**
$c' = c^e \bmod n$	$c = c'^d \bmod n$
↓	↓
H (72) $72^7 \bmod 187 = 30$	$30^{23} \bmod 187 = 72$ (H)
A (65) $65^7 \bmod 187 = 142$	$142^{23} \bmod 187 = 65$ (A)
L (76) $76^7 \bmod 187 = 32$	$32^{23} \bmod 187 = 76$ (L)
L (76) $76^7 \bmod 187 = 32$	$32^{23} \bmod 187 = 76$ (L)
O (79) $79^7 \bmod 187 = 139$	$139^{23} \bmod 187 = 79$ (O)

Literaturverzeichnis

Buchmann, J. (2003): Einführung in die Kryptographie. 3. Auflage, Springer Verlag, Berlin.

Swoboda, J.; Spitz, S.; Pramateftakis, M. (2008):Kryptographie und IT-sicherheit: Grundlagen und Anwendungen. 1. Auflage, Vieweg & Teubner Verlag, Wiesbaden

Wiener, M.J.: Cryptanalysis of short RSA secret exponents. Information Theory, IEEE Transactions on Volume 36, Issue 3, May 1990 Page(s):553 – 558