

Public-Key Kryptographie mit dem RSA Schema

Torsten Büchner
7.12.2004

1. Einleitung

1. symmetrische-, asymmetrische Verschlüsselung
2. RSA als asymmetrisches Verfahren

2. Definition von Begriffen

1. Einwegfunktionen
2. Eulersche Funktion
3. Ordnung einer Gruppe
4. Satz von Lagrange
5. kleiner Fermatscher Satz

3. Euklidischer Algorithmus und Chinesischer Restsatz

4. RSA-Algorithmus

symmetrische Verschlüsselung

Eigenschaften :

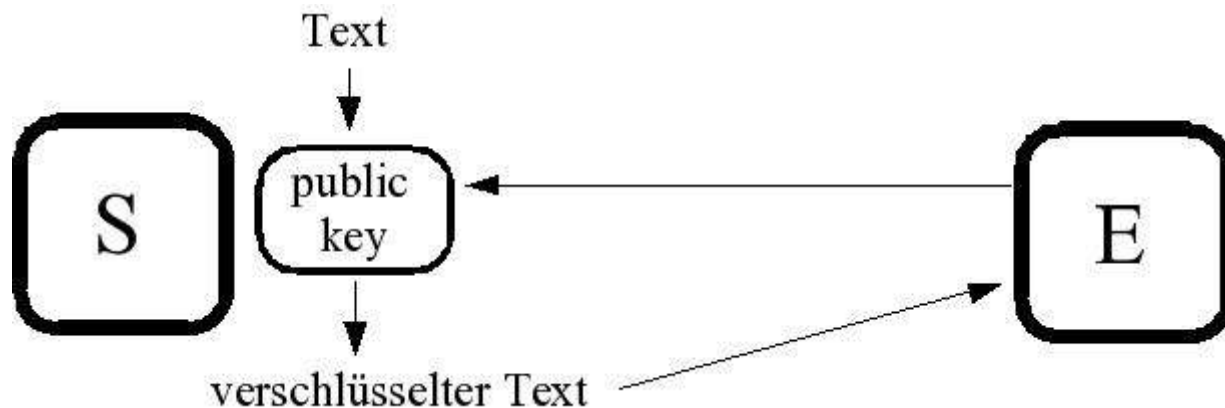
- benutzt zur Ver- und Entschlüsselung den selben Schlüssel -> wird über sicheren Kanal übermittelt (in Praxis schwierig)
- Ver- und Entschlüsselungsfunktionen sind gleich oder fast gleich
- Freilegen dieser macht System unsicher
- Bsp: DES

asymmetrische Verschlüsselung

- verschiedene Schlüssel zur Ver- und Entschlüsselung: e_K , d_K
- man kann von e_K nicht (ohne weiteres) auf d_K schließen \rightarrow e_K kann veröffentlicht werden!!
jeder kann Nachrichten verschlüsseln
- nur wer d_K hat kann Nachrichten entschlüsseln

public Key - RSA

- RSA ist ein asymmetrisches Verfahren
- Empfänger erzeugt öffentlichen und privaten Schlüssel
- jeder Sender kann mit Hilfe des öffentlichen Schlüssel Nachrichten verschlüsseln
- nur Empfänger kann entschlüsseln



RSA

- basiert auf mathematischem Problem der Faktorisierung großer Primzahlprodukte
- Produkt zweier großer Primzahlen $n = p \cdot q$
- Verschlüsselungsfunktion:

$$e_K: y = x^e \bmod n$$

- Entschlüsselungsfunktion:

$$d_K: x = y^d \bmod n$$

x und y sind aus Restklassenring Z_n

Historisches

Idee:

- 1970 Paper von James Ellis
- wurde erst 1997 veröffentlicht
- hat nie Patent angemeldet

Theorie zur Public-Key-Kryptografie:

- 1976 von Whitfield Diffie und Martin Hellman (Stanford Universität) ausgearbeitet und veröffentlicht

RSA:

- 1977 Entwicklung des RSA-Kryptosystem von Rivest, Shamir und Adleman

Definition von Begriffen

1. Einwegfunktionen
2. Eulersche Funktion
3. Ordnung einer Gruppe
4. Satz von Lagrange
5. kleiner Fermatscher Satz

Einwegfunktionen

- Einwegfunktion: ist eine Funktion, die schwer umzukehren ist
 - $y=f(x)$ kann in Polinomialzeit berechnet werden
 - es gibt kein effizientes Verfahren, um bei bekanntem y das x zu berechnen
- Geheimtürfunktionen (trapdoor function)
 - schnelles Umkehren möglich, wenn Zusatzinformationen vorhanden sind

Sicherheit in RSA basiert auf Geheimtürfunktion

Eulersche Funktion - $\varphi(n)$

- Anzahl aller natürlichen Zahlen k mit $1 \leq k \leq n$ die zu n teilerfremd sind
- Funktion wurde von Leonhard Euler im achtzehnten Jahrhundert gefunden
- Bsp:

n	1	2	3	4	5	6	7	8
zu n teilerfremd:	1	1	1;2	1;3	1;2;3;4	1;5	1;2;3;4;5;6	1;3;5;7
$\varphi(n)$	1	1	2	2	4	2	6	4

n	9	10	11
zu n teilerfremd:	1;2;4;5;7;8	1;3;7;9	1;2;3;4;5;6;7;8;9;10
$\varphi(n)$	6	4	10

Eulersche Funktion - $\varphi(n)$

Besonderheiten der Eulerschen Funktion:

- für 2 teilerfremde Zahlen gilt:

$$\varphi(b) \cdot \varphi(a) = \varphi(a \cdot b)$$

- wenn p eine Primzahl ist, gilt:

$$\varphi(p) = (p-1)$$

- für 2 Primzahlen p und q gilt:

$$\varphi(p \cdot q) = (p-1) \cdot (q-1)$$

Ordnung einer Gruppe

- Ordnung von Elementen einer Gruppe:
 - Anzahl der Multiplikationen mit sich selbst, so dass sich das neutrale Element ergibt
 - $a^n = 1$
 - $n \rightarrow$ Ordnung des Elements
- Ordnung einer Gruppe:
 - Mächtigkeit der Trägermenge (Kardinalität)

Satz von Lagrange

- gilt für jede Untergruppe (U, \cdot) einer Gruppe (G, \cdot)
- Ordnung $|U|$ ist Teiler der Ordnung $|G|$

kleiner Fermatscher Satz

- Grundlage für RSA-Kryptosystem

Aussage:

- Z_n^* ist eine multiplikative Gruppe der Ordnung $\varphi(n)$
- für alle Primzahlen n und zu n primen $a \in \mathbb{N}$
- $a^{\varphi(n)} \equiv 1 \pmod{n}$ für alle a aus $\{1, \dots, (n-1)\}$

Begründung:

- Satz von Lagrange

der Euklidische Algorithmus und der Chinesische Restsatz

Euklidischer Algorithmus

- kann größten gemeinsamen Teiler zweier Zahlen berechnen:

– ggT(a,b): $r_0 = a$ und $r_1 = b$ wobei $a < b$

$$r_2 = r_0 \bmod r_1$$

wenn $r_2 = 0$, dann ist $\text{ggT}(r_0, r_1) = r_1$

$$\text{sonst } r_3 := r_1 \bmod r_2$$

wenn $r_3 = 0$, dann ist $\text{ggT}(r_1, r_2) = r_2$

$$\text{sonst } r_4 := r_2 \bmod r_3$$

.....

– allgemein $\text{ggT}(a,b) = \text{ggT}(b, a \bmod b)$

Euklidischer Algorithmus

- \mathbb{Z}_n ist Restklassenring für jede positive ganze Zahl n
- $e \in \mathbb{Z}_n$ hat ein multiplikativ inverses Element, wenn e und n teilerfremd sind $\rightarrow \text{ggT}(e,n) = 1$
- wenn n eine Primzahl ist, dann ist \mathbb{Z}_n ein Körper

Euklidischen Algorithmus $\text{EA}(e,n)=1 \rightarrow e^{-1}$ existiert

jedoch keine Möglichkeit $e^{-1} \in \mathbb{Z}_n$ zu berechnen

Erweiterter Euklidischer Algorithmus

- \mathbb{Z}_n^* ist Restklassenkörper
- jedes $e \in \mathbb{Z}_n^*$ hat ein e^{-1}
- Erweiterter Euklidischer Algorithmus kann e^{-1} berechnen

Erweiterter Euklidischer Algorithmus

- $q_1 \dots q_m$ Quotienten: $q_m = \frac{r_{m-1}}{r_m}$

- $t_0 \dots t_m, s_0 \dots s_m$:

$$t_j = \begin{cases} 0 & \text{wenn } j=0 \\ 1 & \text{wenn } j=1 \\ t_{j-2} - q_{j-1} t_{j-1} & \text{wenn } j \geq 2 \end{cases} \quad s_j = \begin{cases} 1 & \text{wenn } j=0 \\ 0 & \text{wenn } j=1 \\ s_{j-2} - q_{j-1} s_{j-1} & \text{wenn } j \geq 2 \end{cases}$$

- für $0 \leq j \leq m$ gilt $r_j = s_j r_0 + t_j r_1$

$$e^{-1} \bmod n = t_m \bmod n$$

Chinesischer Restsatz

- Methode zum Lösen bestimmter Systeme von Kongruenzen
- m_1, \dots, m_r paarweise teilerfremd
($\text{ggT}(m_i, m_j) = 1$ wenn i ungleich j)
- es existiert für jedes Tupel a_1, \dots, a_r eine ganze Zahl x die die folgende simultane Kongruenz erfüllt:

$$x \equiv a_1 \pmod{m_1}$$

$$x \equiv a_2 \pmod{m_2}$$

$$\vdots$$

$$x \equiv a_r \pmod{m_r}$$

Chinesischer Restsatz

- der Chinesische Restsatz hat dafür eine eindeutige Lösung:

$$\text{modulo } M = m_1 \times m_2 \times \dots \times m_r$$

- Hilfsfunktion:

$$X : \mathbb{Z}_M \rightarrow \mathbb{Z}_{m_1} \times \dots \times \mathbb{Z}_{m_r}$$
$$X(x) = (x \bmod m_1, \dots, x \bmod m_r)$$

$$\begin{array}{l} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \\ x \equiv a_r \pmod{m_r} \end{array}$$

$$x = \sum_{i=1}^r a_i M_i y_i \pmod{M}$$

$$\text{wobei } M_i = \frac{M}{m_i} \text{ und } y_i = M_i^{-1} \pmod{m_i} \text{ f\u00fcr } 1 \leq i \leq r$$

RSA - Algorithmus

Empfänger generiert öffentlichen Schlüssel:

- 1) Generierung zweier stochastisch unabhängiger großer Primzahlen p und q die etwa gleich lang sind
- 2) Zufallszahl p erzeugen und 1 prüfen ob p eine Primzahl ist...
- 3) $n=pq$ und $\varphi(n)=(p-1)(q-1)$, φ ist die Eulersche Funktion
- 4) Zufallszahl e so wählen, dass
 - $1 < e < \varphi(n)$
 - $\text{ggT}(e, \varphi(n))=1$ (e und $\varphi(n)$ sind teilerfremd)
 - mit Hilfe des Euklidischen Algorithmus kann ggT berechnet werden
 - (n, e) öffentlicher Schlüssel

RSA - Algorithmus

RSA Algorithmus

Sender kann verschlüsseln:

- 1) public-Key **(e,n)** besorgen
- 2) Text in Ziffernfolge mit $x \leq n - 1$ umwandeln (x - gleichlange Blöcke)
- 3) für jeden Block **$m \equiv x^e \pmod n$** ausrechnen und die Folge von m senden

RSA Algorithmus

Empfänger generiert privaten Schlüssel

- 1) Entschlüsselung nur möglich, wenn die lineare Kongruenz $ed \equiv 1 \pmod{\varphi(n)}$ bekannt ist
- 2) $d = e^{-1} \pmod{\varphi(n)}$
- 3) mit Erweiterten Euklidischen Algorithmus kann d berechnet werden
- 4) privater Schlüssel ist (p, q, e)
- 5) $x \equiv m^d \pmod{n}$

RSA Algorithmus

Empfänger kann Nachricht entschlüsseln:

- 1) Empfänger erhält Folge von m
- 2) für jedes m $\mathbf{x \equiv m^d \bmod n}$ ausrechnen
- 3) Text zusammenfügen

RSA

aus der Definition des RSA-Kryptosystems:

- $e \cdot d \equiv 1 \pmod{\varphi(n)}$
- $n = p \cdot q$ p und q sind Primzahlen
- $\varphi(n) = \varphi(p \cdot q) = (p - 1) \cdot (q - 1)$

RSA

$$ab = t\varphi(n) + 1 \quad \text{für ein } t \geq 1$$

↓ wenn $x \in \mathbb{Z}_n^*$

$$(x^b)^a \equiv x^{t\varphi(n) + 1} \pmod{n}$$

$$(x^b)^a \equiv (x^{\varphi(n)})^t x \pmod{n}$$

↓ kleiner Fermatscher Satz

$$(x^b)^a \equiv 1^t x \pmod{n}$$

$$(x^b)^a \equiv x \pmod{n}$$

Sicherheit

- offensichtliche Attacke:
 - n faktorisieren (in Primzahlen zerlegen)
 - $\varphi(n)=(p-1)(q-1)$ kann berechnet werden und damit auch die Exponenten a und b
- falscher Sender:
 - jeder kann Empfänger verschlüsselte Nachrichten schicken
 - kann sich als „Anderer“ ausgeben

Quellen

- Douglas R. Stinson: Cryptography: Theory and Practice.
- Wikipedia: <http://de.wikipedia.org>
- http://www.wiwi.uni-bielefeld.de/StatCompSci/lehre/material_spezifisch/statalg00/rsa/
- Lukas Döle: Einwegfunktionen – Variationen und Beispiele
- Johannes Buchmann, Sachar Paulus: Einführung in die Kryptografie