VI.3 RSA

- RSA benannt nach seinen Erfindern R. Rivest, A. Shamir und L. Adleman
- vorgestellt 1977
- erstes Public-Key Verschlüsselungsverfahren
- auch heute noch das wichtigste Public-Key Verfahren

Verschlüsselungsverfahren

Definition 2.1 Ein Verschlüsselungsverfahren ist ein 5-Tupel (P,C,K,E,D), wobei

1. P die Menge der Klartexte ist.
2. C die Menge der Chiffretexte ist.
3. K die Menge der Schlüssel ist.
4. $E=\{E_k : k \in K\}$ eine Menge von Verschlüsselungsfunktionen $E_k : P \rightarrow C$ ist.
5. $D=\{D_k : k \in K\}$ eine Menge von Entschlüsselungsfunktionen $D_k : C \rightarrow P$ ist.
6. Zu jedem $e \in K$ existiert ein $d \in K$, so dass für alle $m \in P$

$$D_d(E_e(m)) = m.$$

Schlüssel e,d mit dieser Eigenschaft heißen **Schlüsselpaare**.

Symmetrische & asymmetrische Verfahren

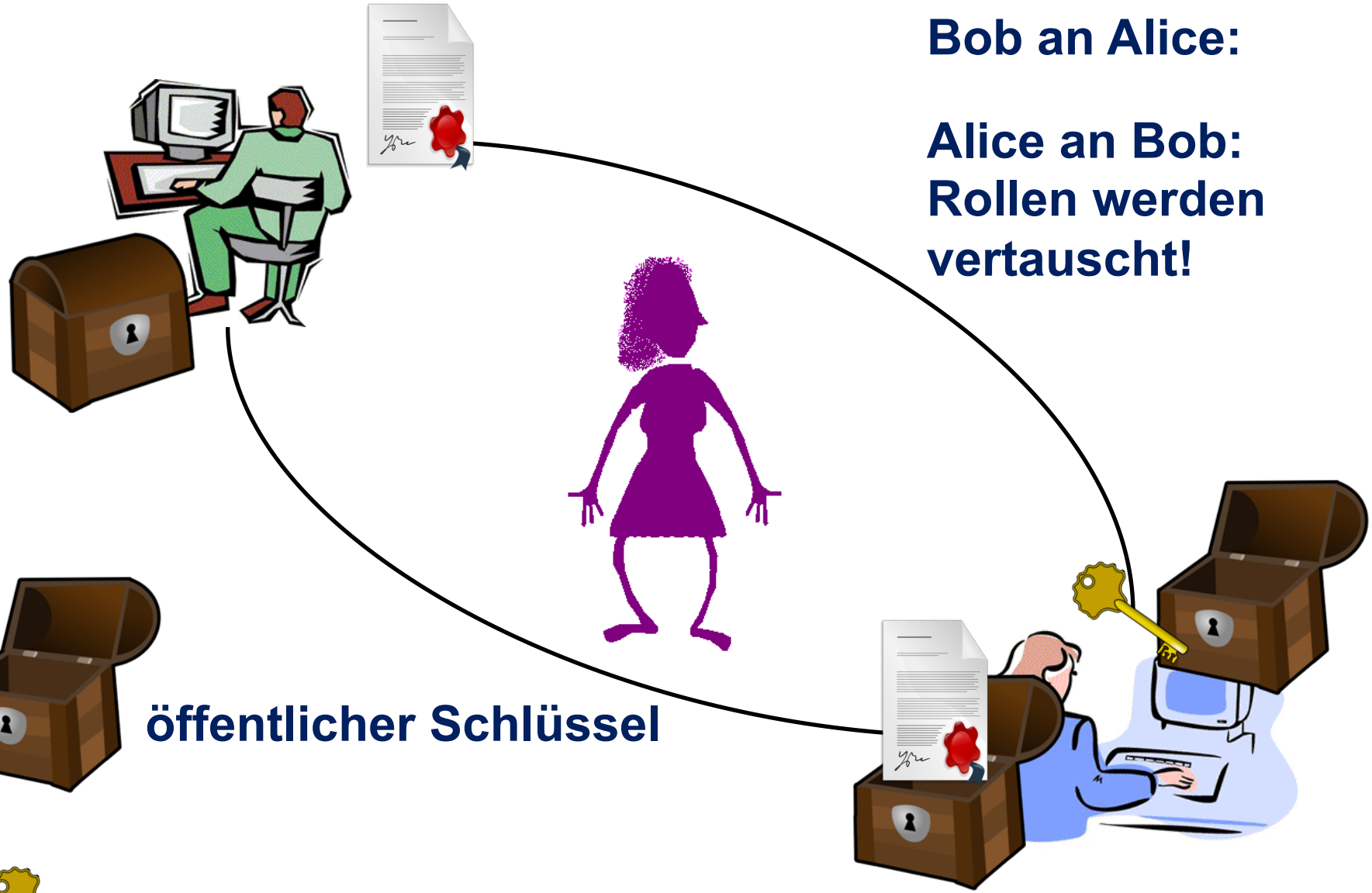
- auch Private-Key-Verfahren & Public-Key-Verfahren

Gilt für $e,d \in K$, dass $D_d(E_e(m)) = m$ für alle $m \in P$, so heißt (e,d) ein Schlüsselpaar.

- Symmetrische Verfahren Für alle Schlüsselpaare (e,d) gilt
  - e = d oder
  - d kann aus e leicht berechnet werden.

- Asymmetrische Verfahren Für alle Schlüsselpaare (e,d) gilt
  - d kann aus e nicht mit vertretbarem Aufwand berechnet werden.

Verschlüsselung (asymmetrisch)



Bob an Alice:

Alice an Bob:
Rollen werden vertauscht!

öffentlicher Schlüssel

geheimer Schlüssel

Vorbereitungen

Definition 6.1 Sei $n \in \mathbb{N}$. Dann ist

$$\mathbb{Z}_n^* := \left\{ a \in \mathbb{Z}_n : ggT(n,a) = 1 \right\}$$

die Menge der Elemente aus $\mathbb{Z}_n$, die zu n teilerfremd sind.

Wir setzen $\varphi(n) = \left| \mathbb{Z}_n^* \right|$.

Lemma 6.2 Sei $n \in \mathbb{N}$ mit Primfaktorzerlegung $n = \prod_{i=1}^{k} p_i^{e_i}$.

Dann gilt $\varphi(n) = \prod_{i=1}^{k} \left(p_i^{e_i} - p_i^{e_i - 1} \right) = n \cdot \prod_{i=1}^{k} \left(1 - 1/p_i \right)$.

Vorbereitungen

Lemma 6.3 Seien $a, b \in \mathbb{N}$ mit $ggT(a,b) = 1$. Dann existieren $s, t \in \mathbb{Z}$ mit $s \cdot a + t \cdot b = 1$.

Korollar 6.4 Seien $n \in \mathbb{N}$ und $a \in \mathbb{Z}_n^*$. Dann existiert ein Element $s \in \mathbb{Z}_n^*$ mit $a \cdot s = 1 \mod n$.

Lemma 6.5 Sei G eine endliche Gruppe und $a \in G$. Dann gilt $a^{|G|} = 1 (\text{in } G)$.

Korollar 6.6 Seien $n \in \mathbb{N}$ und $a \in \mathbb{Z}_n^*$. Dann gilt $a^{\varphi(n)} = 1 \mod n$.

RSA – Schlüsselerzeugung

1. Erzeuge zwei zufällige Primzahlen p, q geeigneter Länge und setze $N := p \cdot q$.
2. Wähle $e \in \mathbb{Z}^*_{\varphi(N)}$ und berechne $d \in \mathbb{Z}^*_{\varphi(N)}$ mit $e \cdot d = 1 \bmod \varphi(N)$.
3. Der öffentliche Schlüssel ist $pk := (N, e)$, der private Schlüssel ist $sk := (N, d)$.

RSA – Verschlüsselung und Entschlüsselung

Bei Wahl des öffentlichen Schlüssels $pk := (N, e)$ ist der Klartextraum $P := \mathbb{Z}_N$.

Der Chiffretextraum ist ebenfalls $C := \mathbb{Z}_N$.

Für alle $m \in \mathbb{Z}_N$ ist $E_{(N,e)}(m) = m^e \mod N$.

Für alle $c \in \mathbb{Z}_N$ ist $D_{(N,d)}(c) = c^d \mod N$.

RSA – Korrektheit

Lemma 6.7 Sei $N \in \mathbb{N}$, $N = p \cdot q$, für Primzahlen p,q, $p \neq q$.

Außerdem seien $e,d \in \mathbb{Z}^*_{\varphi(N)}$ mit $e \cdot d = 1 \bmod \varphi(N)$ und

$m \in \mathbb{Z}_N$ beliebig. Dann gilt $m^{e \cdot d} = m \bmod N$.

Satz 6.8 Seien $N_1,\ldots,N_k \in \mathbb{N}$ paarweise teilerfremd und

seien $a_1,\ldots,a_k \in \mathbb{Z}$. Dann besitzt das System von Kongruenzen

$$\begin{aligned} x &= a_1 \bmod N_1 \\ &\vdots \\ x &= a_k \bmod N_k \end{aligned}$$

eine eindeutige Lösung $a \in \mathbb{Z}_N$, wobei $N=N_1 \cdots N_k$. Die Lösung

kann in Zeit polynomiell in $\log(N)$ berechnet werden.

Effizienz von Ver- und Entschlüsselung

Lemma 6.9 Sind der öfffentliche und geheime Schlüssel (N,e) und (N,d), so kann die Verschlüsselung eines Klartexts und die Entschlüsselung eines Chiffretexts in Zeit $\mathcal{O}\left(\log(N)^3\right)$ berechnet werden.

Lemma 6.10 Arithmetische Operation in $\mathbb{Z}_N$ können in Zeit $\mathcal{O}\left(\log(N)^2\right)$ berechnet werden.

Square-and-Multiply

Ziel G endliche Gruppe, $g \in G$, $a \in N$, $a = \sum_{i=0}^{l-1} a_i 2^i$, $a_i \in \{0,1\}$,

berechne g^a in G.

```
Square-and-Multiply(g,a)
1  y := 1
2  z := g
3  for i = 0 to l – 1 do
4      if a_i = 1
5          then y := y · z
6      z := z^2
7  return y
```

Square-and-Multiply

Lemma 6.11 Der Square-and-Multiply Algorithmus benötigt höchstens $2 \cdot \lceil \log(a+1) \rceil$ Gruppenoperationen.

RSA - Schlüsselerzeugung

Zu zeigen sind 2 Dinge:

1. **Primzahlen p,q können effizient erzeugt werden.**
2. **Gegeben N, φ(N), können e,d mit ed=1mod φ (N) effizient erzeugt werden.**

Primzahlerzeugung

Beruht auf zwei Tatsachen:

1. **Es kann effizient entschieden werden, ob eine Zahl Primzahl ist (z.B. Miller-Rabin-Test).**
2. **Es gibt “viele” Primzahlen (Primzahlsatz).**

Primzahlerzeugung

Erzeuge zufällige Zahlen und teste, ob sie Primzahlen sind, bis eine Primzahl gefunden.

Erzeugung von e und d

Beruht auf zwei Tatsachen:

1. **Es kann effizient entschieden werden, ob zwei Zahlen teilerfremd sind. Falls ja, kann dann auch das modulare Inverse effizient berechnet werden (erweiterter euklidischer Algorithmus).**
2. **Zu jeder Zahl n gibt es “viele” Zahlen, die zu n teiler-fremd sind.**

Sicherheit des geheimen Schlüssels

Satz 6.12 Es existiert ein Algorithmus, der bei Eingabe N,e,d mit $N=pq$, p,q Primzahlen und mit $ed=1 \bmod \varphi(N)$ in Zeit erwartet polynomiell in log(N) die Primzahlen p und q berechnet.

Tatsache 6.13 Der zurzeit beste bekannte Algorithmus zur Faktorisierung einer natürlichen Zahl n besitzt Laufzeit

$e^{c \cdot \log(n)^{1/3} \cdot \log\log(n)^{2/3}}$, wobei $c \approx 1.94$.

Angriffe auf RSA

Satz 6.14 Seien N_1, N_2, N_3 drei unterschiedliche RSA-Module und sei $m \in \mathbb{N}$ mit $m<N_i$, $i = 1,2,3$. Gegeben $c_i := m^3 \bmod N_i$, $i = 1,2,3$, kann m in Zeit polynomiell in $\log(N_1 N_2 N_3)$ berechnet werden.

Satz 6.15 Sei N ein RSA-Modul und seien $e_1, e_2 \in Z^*_{\varphi(N)}$ mit $ggT(e_1, e_2) = 1$. Gegeben die Chiffretexte $c_i := m^{e_i} \bmod N$, i=1,2, kann der Klartext m in Zeit polynomiell in $\log(N)$ berechnet werden.

Angriffe auf RSA

Satz 6.16 [Wiener] Sei N ein RSA-Modul und sei $e \in Z^*_{\varphi(N)}$, so dass für das eindeutige $d \in Z^*_{\varphi(N)}$ mit $e \cdot d = 1 \bmod \varphi(N)$ gilt $d \leq \frac{1}{3} N^{1/4}$. Dann kann d aus e und N in Zeit $\mathcal{O}\left(\log(N)^2\right)$ berechnet werden.

Satz 6.17 RSA ist nicht sicher gegen Chosen-Ciphertext Angriffe.

Möglichkeiten eines Angreifers

- **Ciphertext-Only Angriff** Angreifer kennt nur Chiffretext c.
- **Known-Plaintext Angriff** Angreifer kennt Chiffretext c und Paare (m_i,c_i) von Klartexten und Chiffretexten unter dem gleichen Schlüssel e.
- **Chosen-Plaintext Angriff** Angreifer kann sich zu selbst gewählten Klartexten m_i die Chiffretexte c_i erzeugen.
- **Chosen-Ciphertext Angriff** Angreifer kann sich zu selbst gewählten Chiffretexten c_i die Klartexte m_i erzeugen.