Die RSA-Verschlüsselung

Vortragender:Keszeg Attila

Universität Wien, Fakultät für Mathematik

2016.01.29.

Kryptographie ist die Lehre von Methoden zur Ver- und Entschlüsselung von Daten/Nachrichten mit Hilfe mathematischer Verfahren. Dank der Kryptographie können vertrauliche Daten gespeichert oder über unsichere Netzte (z.B. das Internet) übertragen werden, so dass diese nur vom eigentlichen Empfänger gelesen werden können.

Wozu dient Verschlüsselung?

1. Sicherung der Vertraulichkeit übertragener Information
2. Prüfung der Authentizität von Personen (digitale Unterschrift)
3. Sicherung der Vertraulichkeit gespeicherter Information

⋮

Arbeiten mit einem einzigen Schlüssel, der sowohl zum Entschlüsseln, als auch zum Verschlüsseln der Nachrichten dient.
Aus diesem Grund werden symmetrische Verschlüsselungsverfahren auch als **Secret-Key Verfahren** genannt.
Der Knackpunkt liegt in der Schlüsselübergabe zwischen den Kommunikationspartnern.

1. **Transpositionsverfahren:** Nachrichtenteile werden umgestellt (permutiert)
2. **Substitutionsverfahren:** Nachrichtenteile werden ersetzt z.B.: Cäsar-Verfahren

Beispiel:Cäsar-Verfahren

Caesar-Code : Jede Buchstabe des Alphabets wird um eine bestimmte Anzahl an Positionen verschoben ⇒ Grundprinzip: Alphabetrotation.

Klartext	a	b	c	d	e	f	g	h	i	j	k	l	m
Geheimtext	e	f	g	h	i	j	k	l	m	n	o	p	q

Klartext	n	o	p	q	r	s	t	u	v	w	x	y	z
Geheimtext	r	s	t	u	v	w	x	y	z	a	b	c	d

Klartext	dasisteinbeispiel
Geheimtext	hewmwximrfimwtmip

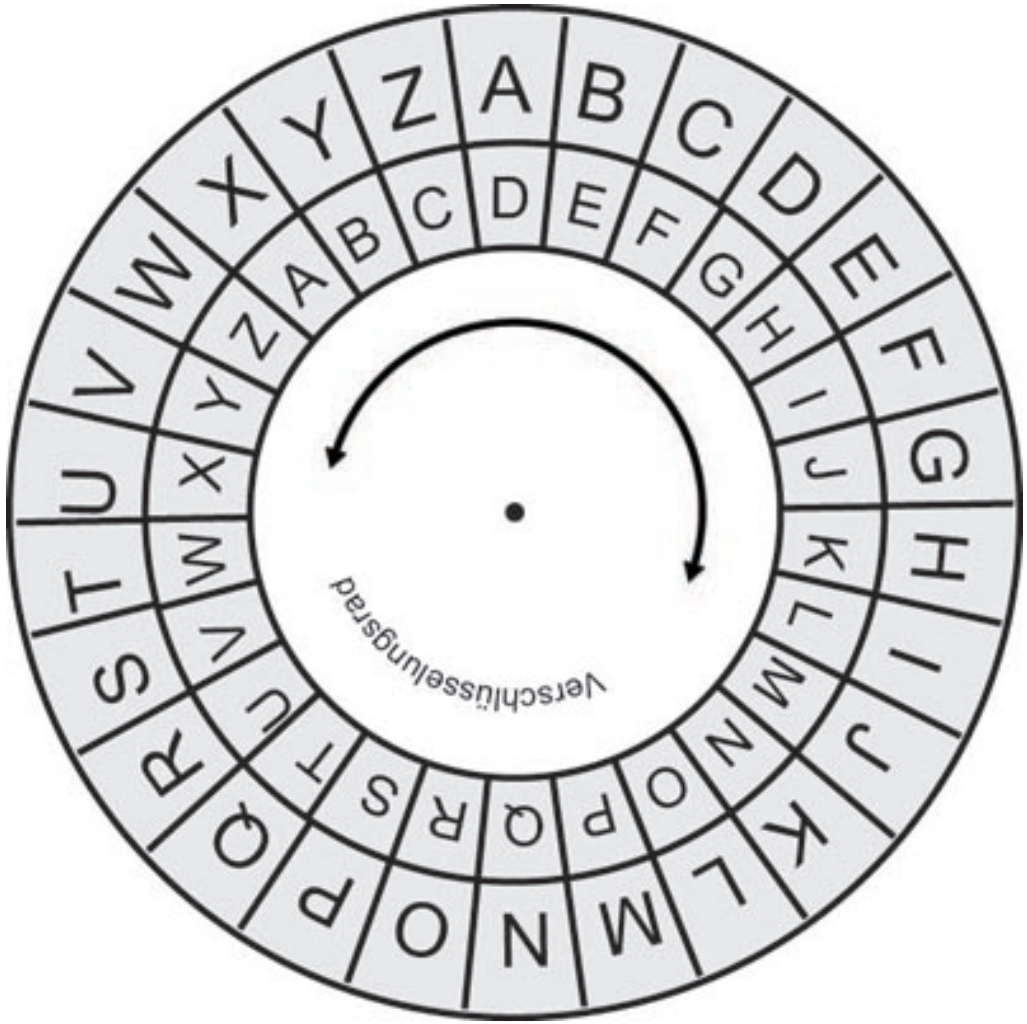


Abbildung: Caesar-Rad

1. Arbeiten mit zwei Schlüsseln. Mit einem öffentlichen, für jeden zugänglichen Schlüssel **(Public-Key)**, der bei der Verschlüsselung und mit einem privaten Schlüssel **(Privat-Key)**, der bei der Entschlüsselung verwendet wird.
2. Auch **Public-Key-Verfahren** genannt
3. Wichtig bei diesem Verfahren ist, dass der private Schlüssel vom Schlüsselbesitzer absolut geheim gehalten wird
4. Das Problem bei der asymmetrischen Kryptografie ist die Verteilung der öffentlichen Schlüssel
5. Rechenaufwand viel größer als bei symmetrischen Verschlüsselungsverfahren

Definition (Kongruenz)

Seien $a, b \in \mathbb{Z}$, $m \in \mathbb{N}$. Man sagt, a und b seine kongruent modulo m, wenn $m \mid (a - b)$
Notation: $a \equiv b \pmod{m}$. Die Zahl m heißt Modul.

Satz

Seien $a, b \in \mathbb{Z}$, $m \in \mathbb{N}$. *Dann sind folgende Aussagen äquivalent:*

1. $a \equiv b \pmod{m}$
2. *Bei Division durch* m *haben* a *und* b *den selben Rest*

Satz

Seien $a, b, c, d, k \in \mathbb{Z}, k \neq 0$ *und* $m, n \in \mathbb{N}$. *Dann gelten:*

1. $a \equiv b \pmod{m}$ *und*
   $c \equiv d \pmod{m} \Rightarrow a + c \equiv b + d \pmod{m}$
2. $a \equiv b \pmod{m}$ *und*
   $c \equiv d \pmod{m} \Rightarrow a \cdot c \equiv b \cdot d \pmod{m}$
3. $a \equiv b \pmod{m}$ *und* $k \mid m$, *so folgt* $a \equiv b \pmod{|k|}$
4. $a \equiv b \pmod{m} \Rightarrow k \cdot a \equiv k \cdot b \pmod{k \cdot m}$

Definition

(Restklasse modulo m)

Für $m \in \mathbb{N}$ wird jede Äquivalenzklasse $\bar{a}$ als Restklasse modulo m bezeichnet.

Jedes x aus $\bar{a}$ wird als Repräsentant von $\bar{a}$ genannt.

Für die Menge der Restklassen modulo m schreibt man: $\mathbb{Z}_m$ oder $\mathbb{Z}/m\mathbb{Z}$

$$\mathbb{Z}_m := \{\bar{a} \ : \ a \in \mathbb{Z}\} \text{ bzw. } \mathbb{Z}/m\mathbb{Z} := \{a + m\mathbb{Z} \ : \ a \in \mathbb{Z}\}$$

Definition (Die Eulersche φ-Funktion)

Für $n \in \mathbb{N}$ ist die Eulersche φ-Funktion wie folgt definiert:

$$\varphi(n) := \mid \{m \in \{1, ..., n\} : ggT(m, n) = 1\} \mid$$

$\varphi(n)$ ist also die Anzahl der natürlichen, n nicht übersteigenden Zahlen, die zu m teilerfremd sind.

Satz

Für eine Primzahl p gilt:

1. $\varphi(p) = p - 1$
2. $\varphi(p^k) = p^k - p^{k-1}$ *für alle* $k \in \mathbb{N}$

Satz (Der Satz von Euler-Fermat)

Für $m \in \mathbb{N}$ *und* $a \in \mathbb{Z}$ *mit* $ggT(a, m) = 1$ *gilt:*

$$a^{\varphi(m)} \equiv 1 \pmod{m}$$

Satz (Der kleine Satz von Fermat)

Für p *Primzahl und* $a \in \mathbb{Z}$ *mit* $ggT(a,p) = 1$ *gilt:*

$$a^{p-1} \equiv 1 \pmod{p}$$

Definition (Einwegfunktion)

Eine Funktion $f : X \to Y$ heißt Einwegfunktion *(one-way function)*, wenn gilt:

1. Es gibt ein effizientes Verfahren zur Berechnung von $y = f(x)$ für jedes $x \in X$. Anders ausgedruckt : $y = f(x)$ kann in Polinomialzeit berechnet werden.
2. Es gibt kein Effizientes Verfahren , um bei bekanntem y das $x := f^{-1}(y)$ zu berechnen für jedes $y \in Y$ *bis auf vernachlässigbar viele*.

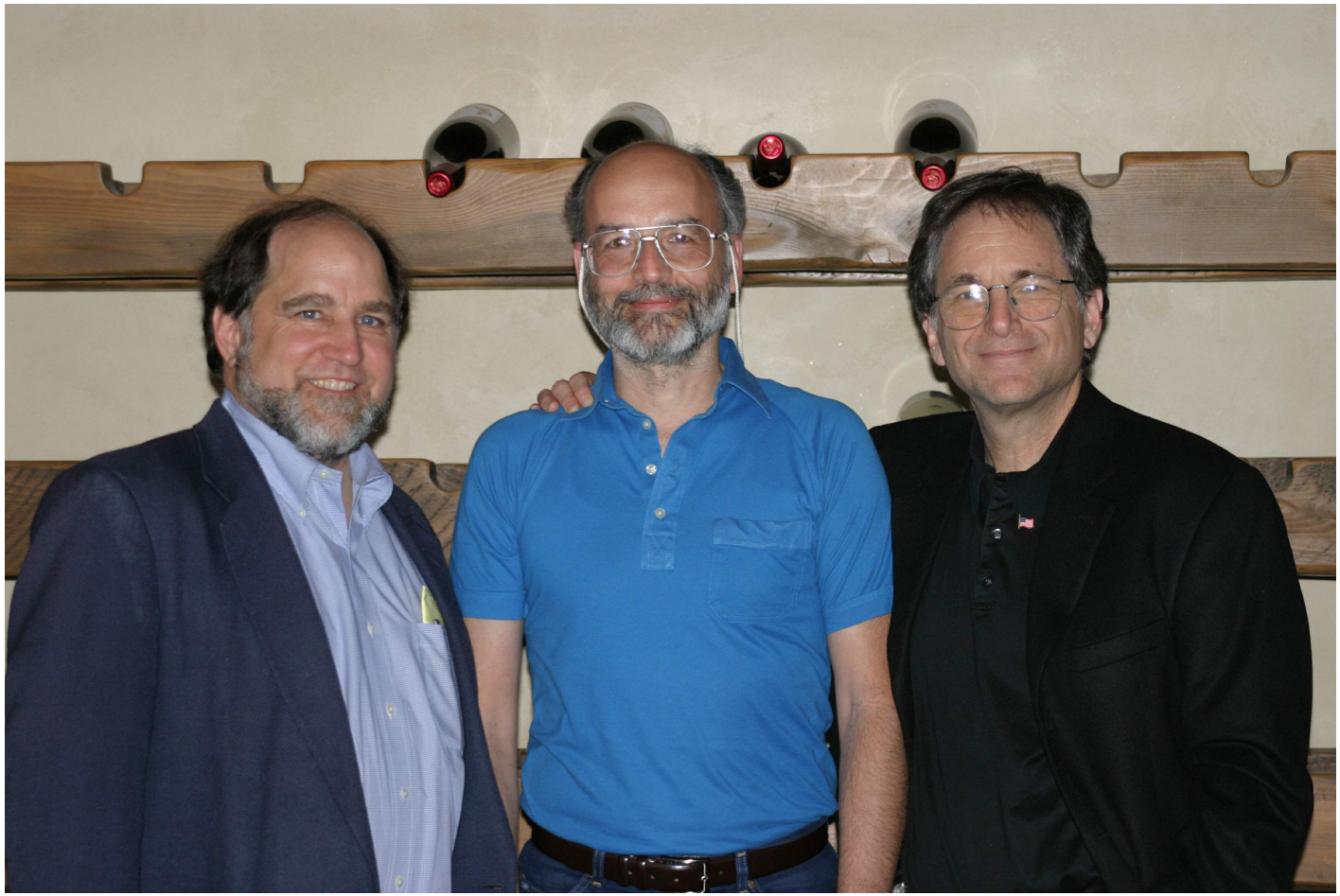


Abbildung: Ron **R**ivest, Adi **S**hamir und Leonard **A**dleman

Zwei Personen **A** und **B** wollen untereineander geheime Nachrichten austauschen. Sei **A** der Sender der Nachricht und **B** der Empfänger.

1. **B** denkt sich zwei große Primzahlen p und q aus . Dann bildet der **B**
$$n = p \cdot q$$
2. Im zweiten Schritt muss der Empfänger (**B**) $\varphi(n)$ bestimmen, wobei φ die Eulersche φ-Funktion bezeichnet.

   Es gilt :
$$\varphi(n) = \varphi(p \cdot q) = \varphi(p) \cdot \varphi(q) = (p-1)(q-1)$$

3. **B**sucht eine zu n teilerfremde Zahl $e \in \mathbb{N}$ mit
$$1 < e < \varphi(n)$$
4. **B** gibt den Öffentlichen Schlüssel $(n; e)$ bekannt
5. Will ***A*** eine Nachricht an **B** senden, so muss er den Text der geheimen Nachricht in eine Zifferfolge umwandeln, die aus gleichlangen Blöcken x besteht. Es muss aber $1 \leq x < n - 1$ gelten.

6. **A** berechnet

$$m \equiv x^e \pmod{n}$$

und sendet diese Zahl m an **B**

7. Um die Nachricht m entschlüsseln zu können muss **B** die Lösung folgender linearen Kongruenz kennen:

$$d \cdot e \equiv 1 \pmod{\varphi(n)}$$

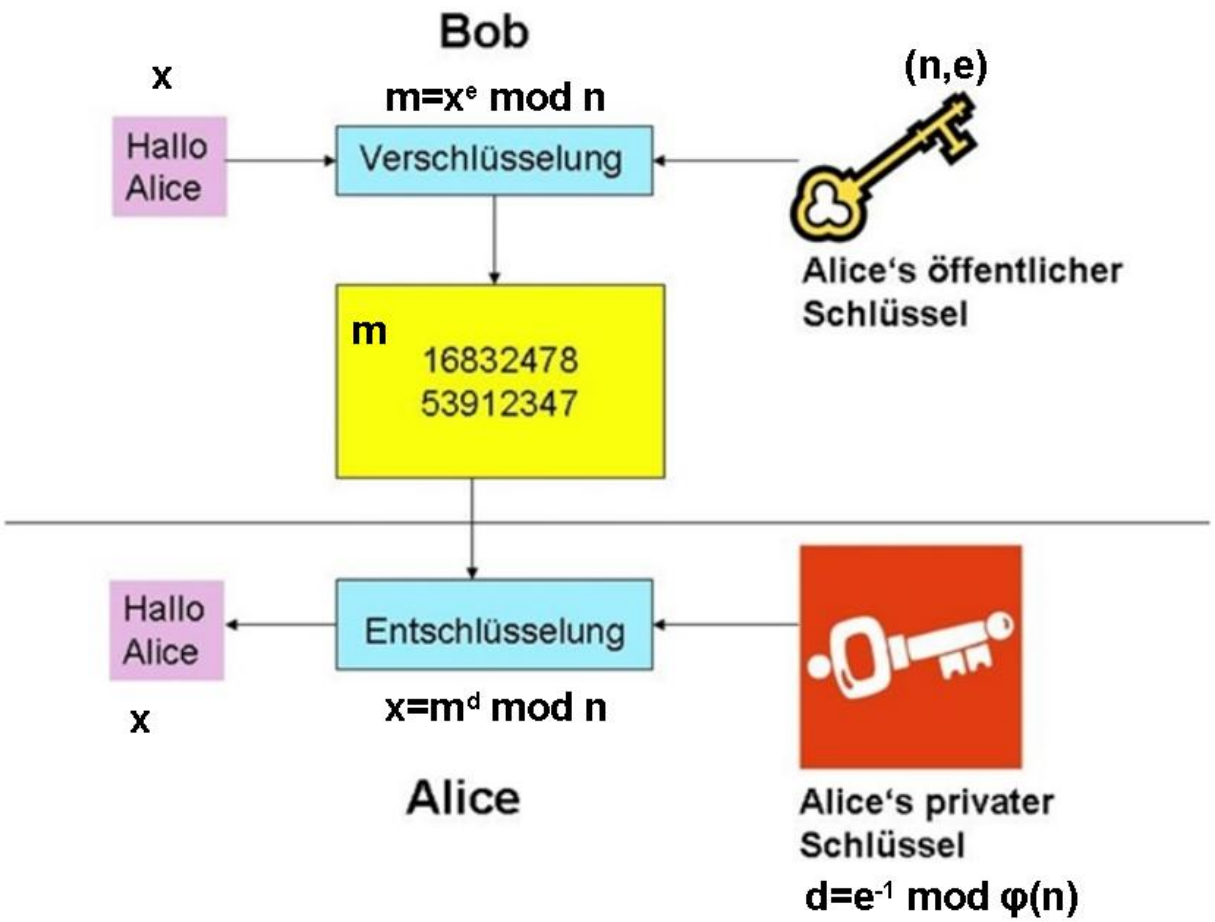
   1. d wird privater Schlüssel genannt
   2. d ist die Inverse zu $e \pmod{\varphi(n)}$ und gilt:
   $$1 < d < \varphi(n)$$

8. Für x gilt:

$$x \equiv m^d \pmod{n}$$

9. Nach all diesen Vorbereitungen kann **B** die Ziffernfolge x in Text umwandeln

Schematische Darstellung



Satz (Korrektheit des RSA-Algorithmus)

Es gelte:

1. $n = p \cdot q$ *für* p, q *Primzahlen*
2. $d \cdot e \equiv 1 \pmod{\varphi(n)}$
3. $m \equiv x^e \pmod{n}$

Dann ist der RSA-Algorithmus korrekt , das heißt:

$$m^d \equiv x \pmod{n}$$

Beweis.

$d \cdot e \equiv 1 \pmod{\varphi(n)}$ ist gleichbedeutend damit, dass ein $k \in \mathbb{Z}$ existiert, mit $d \cdot e = 1 + k \cdot \varphi(n)$.
Da nach Voraussetzung $m \equiv x^e \pmod{n}$ gilt, muss aufgrund der Rechenregeln $m^d \equiv (x^e)^d \pmod{n}$ gelten.

$$m^d \equiv (x^e)^d \pmod{n} \equiv x^{ed} \pmod{n} \equiv x^{1+k\cdot\varphi(n)} \pmod{n}$$

Es bleibt nurmehr zu zeigen, dass

$$x^{1+k\cdot\varphi(n)} \equiv x \pmod{n}$$

gilt. Bei diesem abschließenden Teil des Beweises müssen wir 4 Fälle betrachten:

Fortsetzung des Beweises.

1.Fall: $ggT(x, n) = 1$

$$x^{1+k\cdot\varphi(n)} \equiv x \cdot x^{k\cdot\varphi(n)} \pmod{n} \equiv x \cdot (x^{\varphi(n)})^k \pmod{n}$$

$$\underbrace{\Rightarrow}_{\text{Satz von Euler–Fermat}} \quad x^{1+k\cdot\varphi(n)} \equiv x \cdot 1 \pmod{n} \Rightarrow \textbf{Behauptung}$$

Fortsetzung des Beweises.

2.Fall: $ggT(x,n) = n = p \cdot q$

$$ggT(x,n) = n = p \cdot q \Rightarrow n \mid x$$

Nach Voraussetzung gilt: $0 \leq x \leq n-1 \Rightarrow x = 0$

$$\Longleftrightarrow$$

$$x \equiv 0 \pmod{n}$$

$$x^{1+k\cdot\varphi(n)} \equiv 0^{1+k\cdot\varphi(n)} \pmod{n} \equiv 0 \pmod{n} \equiv x \pmod{n}$$

Fortsetzung des Beweises.

3.Fall:

$$ggT(x,n) = p \text{ und } ggT(x,q) = 1$$

4.Fall:

$$ggT(x,n) = q \text{ und } ggT(x,p) = 1$$

An der Tafel

▸ Beispiel

$$
\begin{aligned}
m &\equiv x^e \pmod{n} \\
m &\equiv 6^{115} \pmod{2881} \\
m &\equiv (6^5)^{23} \pmod{2881} \\
m &\equiv (\underbrace{7776}_{2\cdot 2881+2014})^{23} \pmod{2881} \equiv (2014)^{23} \pmod{2881} \\
&\equiv (2014^2)^{11} \cdot 2014 \pmod{2881} \equiv (2629)^{11} \cdot 2014 \pmod{2881} \\
&\equiv (2629^2)^5 \cdot \underbrace{2629 \cdot 2014}_{1837\cdot 2881+2409} \pmod{2881} \equiv (2629^2)^5 \cdot 2409 \pmod{2881} \\
&\equiv (122^2)^2 \cdot 122 \cdot 2409 \pmod{2881} \equiv (14884)^2 \cdot 36 \pmod{2881} \\
&\equiv (479)^2 \cdot 36 \pmod{2881} \\
&\equiv (229441) \cdot 36 \pmod{2881} \equiv 1842 \cdot 36 \pmod{2881} \\
&\equiv \underline{\underline{49 \pmod{2881}}}
\end{aligned}
$$

Einfachere Berechnung von $6^{115} \rightarrow$ **Modulares Potenzieren**

Modulares Potenzieren

- Effizienter Weg zur Berechnung von $x = a^b \pmod{n}$
- Vorgehensweise:
  1. Stelle den Exponenten in Binärform dar
  2. Erster Faktor ist gleich der Basis
  3. Weitere Faktoren durch Quadrieren des vorhergehenden Faktors:
     1. Bit des Exponenten 1 $\Rightarrow$ das Ergebnis wird mit dem jeweiligen Faktor multipliziert
     2. Bit des Exponenten 0 $\Rightarrow$ das Ergebnis bleibt unverändert
- Nach jedem Quadrieren und jeder Multiplikation wird eine Modulo-Operation ausgeführt $\Rightarrow$ kein Einfluss auf das Endergebnis

Modulares Potenzieren (Beispiel)

Berechne $6^{115} \pmod{2881}$!

1. Binärdarstellung des Exponenten : $115 = 1110011_2$
2. Initialisierung: $\text{Ergebnis}_0=1$, $\text{Faktor}=6$

Berechnung:

3. Bit im Exponenten gesetzt
   $\text{Faktor}_1=6$
   Ergebnis_1
   $=\text{Ergebnis}_0 \cdot \text{Faktor}_1 \pmod{2881} \Rightarrow 1 \cdot 6 \pmod{2881} = 6$
4. Bit im Exponenten gesetzt
   $\text{Faktor}_2=\text{Faktor}_1^2 \pmod{2881} = 36$
   Ergebnis_2
   $=\text{Ergebnis}_1 \cdot \text{Faktor}_2 \pmod{2881} \Rightarrow 6 \cdot 36 \pmod{2881} = 216$

Fortsetzung des Beispiels

5. Kein Bit im Exponenten gesetzt
   $\text{Faktor}_3 = \text{Faktor}_2^2 \pmod{2881} = 1296$
   $\text{Ergebnis}_3 = \text{Ergebnis}_2 = 216$
6. Kein Bit im Exponenten gesetzt
   $\text{Faktor}_4 = \text{Faktor}_3^2 \pmod{2881} = 2874$
   $\text{Ergebnis}_4 = \text{Ergebnis}_3 = 216$
7. Bit im Exponenten gesetzt
   $\text{Faktor}_5 = \text{Faktor}_4^2 \pmod{2881} = 49$
   Ergebnis_5
   $= \text{Ergebnis}_4 \cdot \text{Faktor}_5 \pmod{2881} = 1941$

Fortsetzung des Beispiels

8. Bit im Exponenten gesetzt
   $\text{Faktor}_6 = \text{Faktor}_5^2 \pmod{2881} = 2401$
   Ergebnis_6
   $= \text{Ergebnis}_5 \cdot \text{Faktor}_6 \pmod{2881} = 1764$
9. Bit im Exponenten gesetzt
   $\text{Faktor}_7 = \text{Faktor}_6^2 \pmod{2881} = 2801$
   Ergebnis_7
   $= \text{Ergebnis}_6 \cdot \text{Faktor}_7 \pmod{2881} = 49$

Es gilt also $49 = 6^{115} \pmod{2881}$

Definition

Eine digitale Signatur ist ein 5-Tupel P, A, K, S, V

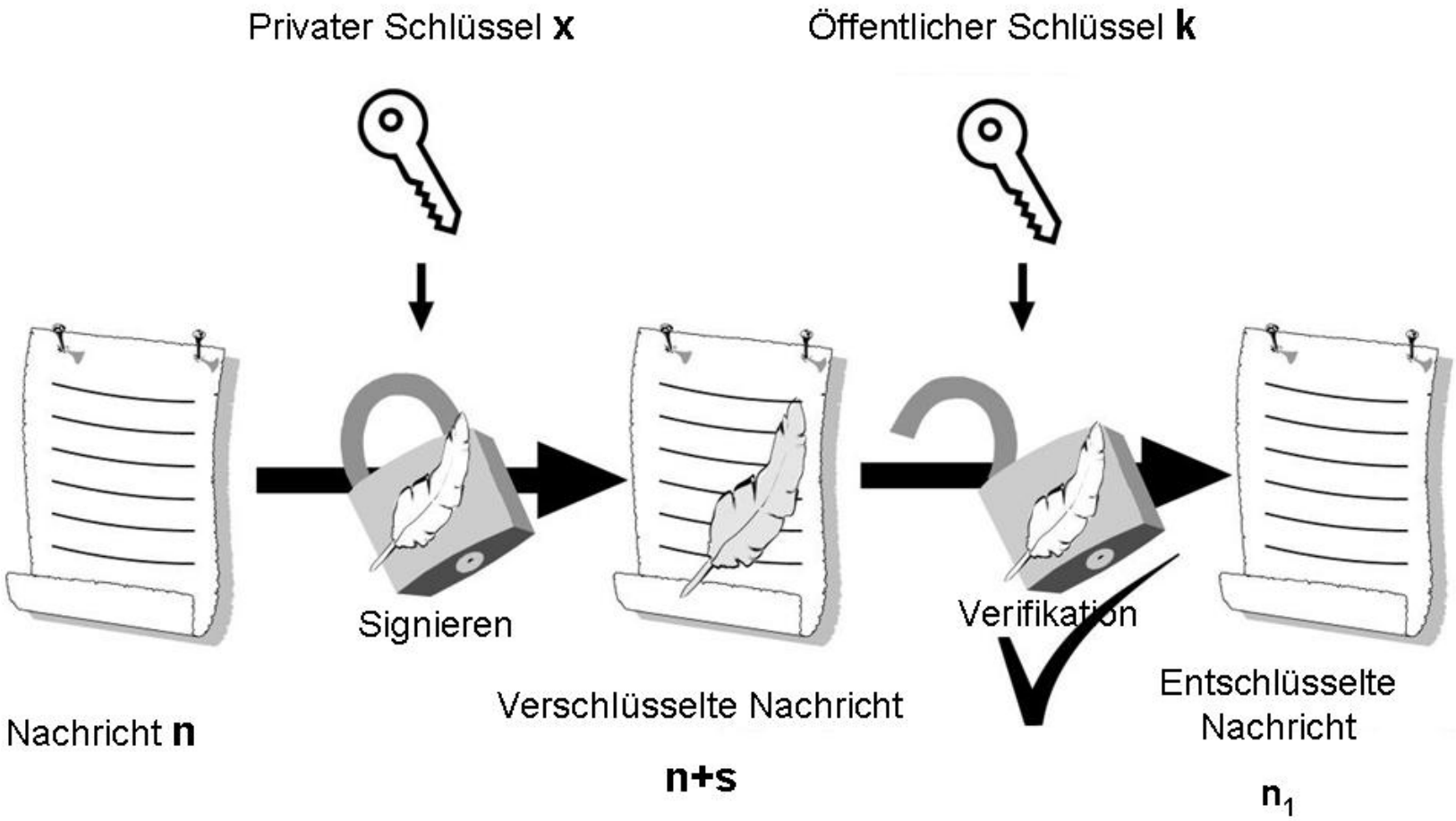
1. P ist eine endliche Menge von Nachrichten
2. A ist eine endliche Menge von Signaturen
3. K ist der Schlüsselraum
4. S ist die Menge der möglichen Signierfunktionen, sodass für alle $k \in K$ ein $sig_k \in S$ gibt , mit $sig_k : P \to A$
5. V ist die Menge der Verifikationsfunktionen, sodasses für alle $k \in K$ ein $ver_k \in V$ gibt mit $ver_k : P \times A \to \{richtig\ ,\ falsch\}$

Für jede Nachricht $x \in P$ und für jede Signatur $y \in A$ gilt:

$$verify(x, y) = \begin{cases} richtig & \text{falls} \quad y = sig(x) \\ falsch & \text{falls} \quad y \neq sig(x) \end{cases}$$

Eine digitale Signatur muss folgende Merkmale erfüllen:

- Die Signatur wurde absichtlich unter das Dokument gesetzt
- Die Signatur kann nicht gefälscht werden
- Die Unterschrift kann nicht auf andere Dokumente übertragen werden
- Nachträgliche Aenderungen im Dokument sind nicht möglich
- Die Unterschrift kann nachträglich nicht geleugnet werden


Privater Schlüssel x
Öffentlicher Schlüssel k
Signieren
Verifikation
Nachricht n
Verschlüsselte Nachricht
n+s
Entschlüsselte
Nachricht
n_1

Danke für die Aufmerksamkeit!