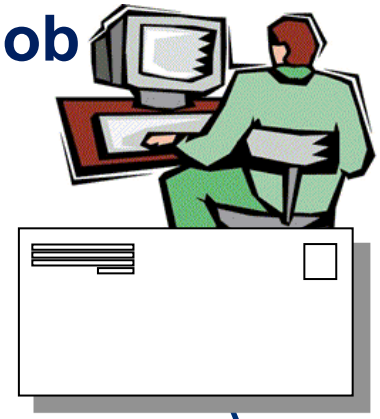
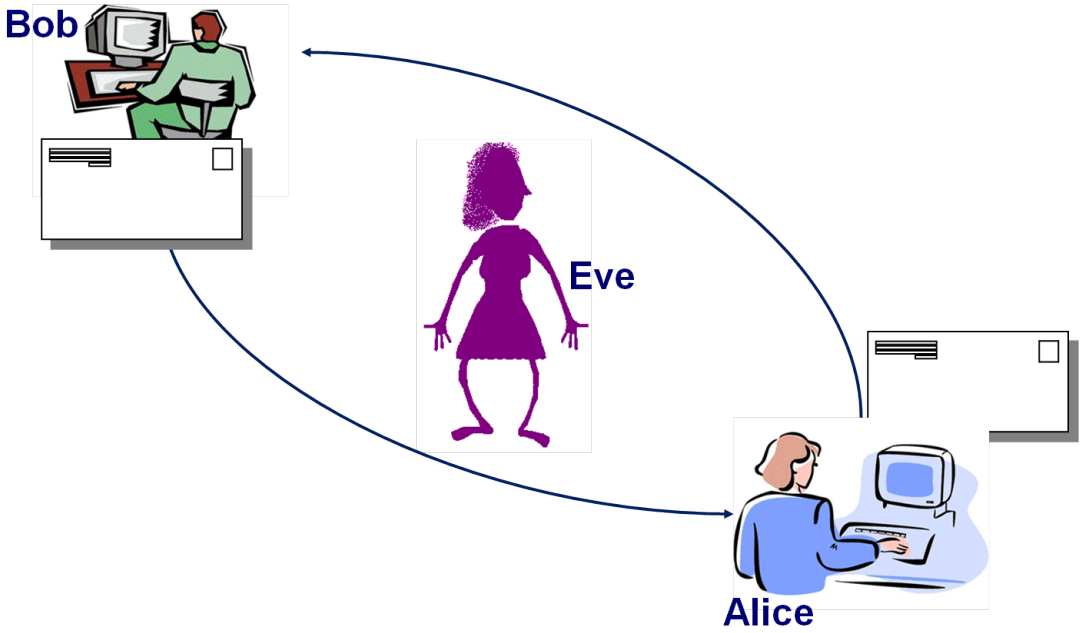
VIII. Digitale Signaturen



Eve möchte

- lauschen
- ändern
- personifizieren

Aufgaben



- Vertraulichkeit - Lauschen
- Authentizität - Tauschen des Datenursprungs
- Integrität - Änderung der Daten
- Zurechenbarkeit - Leugnen des Datenursprungs

Kryptographische Verfahren

- Verschlüsselungsverfahren ≙ Vertraulichkeit
- Authentifzierungscodes (MACs) ≙ Authentifizierung
- Hashfunktionen ≙ Integrität
- Digitale Signaturen ≙ Zurechenbarkeit

Handschriftliche Unterschriften

Bonn,4. Juli 1997

Kaufvertrag

Zwischen
Peter Mustermann aus Demostadt

und
Andre Reisen aus Bonn

wird folgender Vertrag geschlossen:

Villa Kunterbunt des Hrn. Mustermann geht für **400.000 DM** in das Eigentum von Hrn. Reisen über.

Mustermann *Andre Reisen*

P. Mustermann Andre Reisen

B. Glaubicht

Notar

- **Angegebene Identität wird authentisch.**
- **Integrität (Korrektheit) des Inhalts wird bestätigt.**
- **Sowohl Authentizität als auch Integrität können überprüft werden, denn**
- **Unterschrift ist individuell und schwer zu fälschen.**

VIII.1 Aufgaben und Definition

Digitale Signaturen sollen

- **handschriftliche Unterschriften ersetzen können,**
- **die Unverfälschtheit eines Dokuments garantieren (Integrität),**
- **den Unterzeichner eines Dokuments identifizieren (Authentizität),**
- **Integrität und Identität über längere Zeiträume hin verifizierbar machen (Verifizierbarkeit & Zurechenbarkeit).**

Einsatzmöglichkeiten

- Elektronische Rechnungen und Verträge
- Elektronische Archivierung, z.B. bei medizinischen Daten
- Einreichungen von Steuererklärungen
- Einreichung von Dokumenten bei Zivilgerichten
  - Bundesgerichtshof
  - Bundespatentgericht
  - verschiedene Oberlandesgerichte

Definition

Definition 8.1 Ein digitales Signaturverfahren ist ein 5-Tupel (P, U, K, S, V), wobei

1. P die Menge der Klartexte ist,
2. U die Menge der Unterschriften ist,
3. K die Menge von Schlüsselpaaren (pk, sk) ist,
4. $S = \{S_{sk} : (pk, sk) \in K\}$ eine Menge von Signierfunktionen $S_{sk} : P \to U$ ist,
5. $V = \{V_{pk} : (pk, sk) \in K\}$ eine Menge von Verifikationsfunktionen $V_{pk} : P \times U \to \{0,1\}$ ist,
6. für alle $(pk, sk) \in K$ und alle $m \in P$ gilt

$$V_{pk}(m, S_{sk}(m)) = 1.$$

Konventionen und Erweiterungen

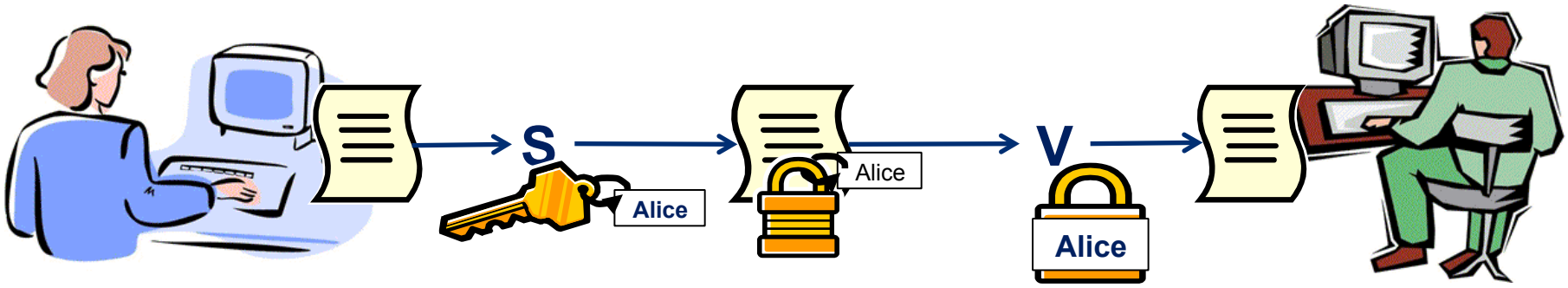
- pk in einem Schlüsselpaar (pk,sk) heißt öffentlicher Schlüssel, sk heißt privater Schlüssel.

- $V_{pk}(m,u) = 1 :\Leftrightarrow$ u wird als Unterschrift des Besitzers des zu pk gehörigen geheimen Schlüssels akzeptiert.

- Signierfunktionen und Verifikationsfunktionen können (randomisierte) Algorithmen sein.

- P und U können vom Schlüsselpaar (pk,sk) abhängen.

Schema digitale Unterschriften



VIII.2 Sicherheit digitaler Unterschriften

Sicherheit des privaten Schlüssels **Für alle Schlüsselpaare (pk,sk) darf sk nicht aus pk mit vertretbarem Aufwand berechenbar sein.**

No-Message-Modell

Ziel des Angreifers **Für eine beliebige Nachricht m eine gültige Unterschrift zum Schlüsselpaar (pk,sk) berechnen.**
(existentielle Fälschung)

Möglichkeiten des Angreifers **Angreifer kennt nur pk.**

No-Message-Modell

Unterschriften-Verfahren (P,U,K,S,V) ist sicher gegen No-Message-Angriffe, wenn kein Angreifer mit vertretbarem Aufwand und mit nicht vernachlässigbarer Wahrscheinlichkeit im No-Message-Modell eine gültige Unterschrift berechnen kann.

Chosen-Message-Modell

Ziel des Angreifers Für eine beliebige Nachricht m eine gültige Unterschrift zum Schlüsselpaar pk berechnen.

Möglichkeiten des Angreifers Angreifer kennt pk. Zusätzlich kann der Angreifer die Unterschriften (zum Schlüssel sk) beliebiger Nachrichten $m_1,\ldots,m_l \neq m$ anfragen.

Chosen-Message-Modell

Unterschriften-Verfahren (P,U,K,S,V) ist sicher gegen Chosen-Message-Angriffe, wenn kein Angreifer mit vertretbarem Aufwand und mit nicht vernachlässigbarer Wahrscheinlichkeit im Chosen-Message-Modell eine gültige Unterschrift berechnen kann.

VIII.3 RSA –Unterschriften

Schlüsselerzeugung

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

RSA – Unterschriften

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

Der Unterschriftenraum ist ebenfalls $U := \mathbb{Z}_N$.

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

Für alle $(m,u) \in \mathbb{Z}_N \times \mathbb{Z}_N$ gilt: $V_{(N,e)}(m,u) = 1 \Leftrightarrow u^e = m \mod N$.

RSA – Unterschriften

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

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

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

Damit $V_{(N,e)}(m,u) = 1 \Leftrightarrow u^e = m \bmod N$.

RSA-Unterschriften

Lemma 8.2 Sind der öffentliche und geheime Schlüssel (N,e) und (N,d), so kann die Unterschrift eines Klartexts und die Verifikation einer Unterschrift in Zeit $\mathcal{O}\left(\log(N)^3\right)$ berechnet werden.

Sicherheit von RSA-Unterschriften

Beobachtung **RSA-Unterschriften sind weder im Chosen-Message-Modell noch im No-Message-Modell sicher.**

RSA-Unterschriften mit Redundanz

Bei Wahl des öffentlichen Schlüssels $pk := (N, e)$ ist der Klartextraum $P := \{0,1\}^l$, $l := \lfloor \log(N)/2 \rfloor$, der Unterschriftenraum ist $U := \mathbb{Z}_N$.

Für alle $m \in \{0,1\}^l$ ist $S_{(N,d)}(m) = R(m)^d \mod N$

wobei $R(m)$ die natürliche Zahl mit Binärdarstellung $m \| m$ ist.

Für alle $(m,u) \in \{0,1\}^l \times \mathbb{Z}_N$ ist

$$V_{(N,e)}(m,u) = 1 \Leftrightarrow u^e = R(m) \mod N.$$

Angriffe gegen RSA-Unterschriften mit Redundanz nicht bekannt.

RSA-Unterschriften mit Hashing

Bei Wahl des öffentlichen Schlüssels $pk := (N, e)$ ist der

Klartextraum $P := \{0,1\}^*$, der Unterschriftenraum ist $U := \mathbb{Z}_N$.

$h : \{0,1\}^* \to \mathbb{Z}_N$ ist eine kollisionsresistente Hashfunktion.

Hash-then-Sign

Für alle $m \in \{0,1\}^*$ ist $S_{(N,d)}(m) = h(m)^d \bmod N$.

Für alle $(m,u) \in \{0,1\}^* \times \mathbb{Z}_N$ ist

$$V_{(N,e)}(m,u) = 1 \Leftrightarrow u^e = h(m) \bmod N.$$

Angriffe gegen RSA-Unterschriften mit Hashing nicht bekannt.

VIII.4 Elgamal–Unterschriften und DSA

Elgamal-Schlüsselerzeugung

1. Erzeuge eine Primzahl p und einen Generator g der Gruppe $\mathbb{Z}_p^*$.
2. Wähle ein zufälliges Element $a \in \{0,1,\ldots,p-2\}$ und setze $A := g^a \mod p$.
3. Der öffentliche Schlüssel ist $pk := (p,g,A)$, der private Schlüssel ist $sk := (p,g,a)$.

Elgamal – Unterschriften

Bei Wahl des öffentlichen Schlüssels $pk := (p, g, A)$ ist der Klartextraum $P := \mathbb{Z}_{p-1}$, der Unterschriftenraum ist $U := \mathbb{Z}_p \times \mathbb{Z}_{p-1}$.

Unterschrift bei Klartext $m \in \mathbb{Z}_{p-1}$ und $sk = (p, g, a)$

1. Wähle $k \in \{1, \ldots, p-2\}$ mit $ggT(k, p-1) = 1$ zufällig.
2. Setze $r := g^k \mod p$ und $s := k^{-1}(m - a \cdot r) \mod p - 1$.
3. Die Unterschrift ist $u := (r, s)$.

Für alle $(m, r, s) \in \mathbb{Z}_{p-1} \times \mathbb{Z}_p \times \mathbb{Z}_{p-1}$ ist

$$V_{(p,g,A)}(m, r, s) = 1 \Leftrightarrow A^r r^s = g^m \mod p.$$

Elgamal-Unterschriften

Lemma 8.3 Sind der öfffentliche und geheime Schlüssel (p,g,A) und (p,g,a), so kann die Unterschrift eines Klartexts und die Verifikation einer Unterschrift in Zeit $\mathcal{O}\left(\log(p)^3\right)$ berechnet werden.

Sicherheit von Elgamal-Unterschriften

Beobachtung **Elgamal-Unterschriften sind weder im Chosen-Message-Modell noch im No-Message-Modell sicher.**

Elgamal – Unterschriften mit Hashing

Bei Wahl des öffentlichen Schlüssels $pk := (p, g, A)$ ist der Klartextraum $P := \{0,1\}^*$, der Unterschriftenraum ist $U : \mathbb{Z}_p \times \mathbb{Z}_{p-1}$.

$h : \{0,1\}^* \to \mathbb{Z}_{p-1}$ ist eine kollisionsresistente Hashfunktion.

Unterschrift bei Klartext $m \in \{0,1\}^*$ und $sk = (p, g, a)$

1. Wähle $k \in \{1, \ldots, p-2\}$ mit $ggT(k, p-1) = 1$ zufällig.
2. Setze $r := g^k \bmod p$ und $s := k^{-1}(h(m) - a \cdot r) \bmod p - 1$.
3. Die Unterschrift ist $u := (r, s)$.

Für alle $(m, r, s) \in \{0,1\}^* \times \mathbb{Z}_p \times \mathbb{Z}_{p-1}$ ist

$$V_{(p,g,A)}(m, r, s) = 1 \Leftrightarrow A^r r^s = g^{h(m)} \bmod p.$$

DSA – Digital Signature Algorithm

- Seit 1991 Teil des Digital Signature Standards der NIST.
- Zunächst einziges Verfahren in DSS.
- Später RSA und ECDSA (Elliptic Curve DSA)
- Letzteres sehr ähnlich zu DSA.
- DSA beruht auf Elgamal-Unterschriften.

DSA

DSA-Schlüsselerzeugung

1. Erzeuge eine Primzahl q mit $2^{159} < q < 2^{160}$.
2. Erzeuge Primzahl p mit $2^{511+64t} < p < 2^{512+64t}, t \in \{1,\ldots,8\}$, so dass q Teiler von $p-1$ ist.
3. Wähle erzeugendes Element z von $\mathbb{Z}_p^*$ und setze $g := z^{(p-1)/q}$.
4. Wähle ein zufälliges Element $a \in \{1,\ldots,q-1\}$ und setze $A := g^a \mod p$.
3. Der öffentliche Schlüssel ist $pk := (p,q,g,A)$, der private Schlüssel ist $sk := (p,q,g,a)$.

Bemerkung g hat Ordnung q in $\mathbb{Z}_p^*$.

DSA – Unterschriften

Bei Wahl des öffentlichen Schlüssels $pk := (p, q, g, A)$ ist der Klartextraum $P := \{0,1\}^*$, der Unterschriftenraum ist $U := \mathbb{Z}_q \times \mathbb{Z}_q$.

$h: \{0,1\}^* \to \mathbb{Z}_q$ ist eine kollisionsresistente Hashfunktion.

Unterschrift bei Klartext $m \in \{0,1\}^*$ und $sk = (p, q, g, a)$

1. Wähle $k \in \{1, \ldots, q-1\}$ zufällig.
2. Setze $r := (g^k \bmod p) \bmod q$ und
$$s := k^{-1}(h(m) + a \cdot r) \bmod q.$$
3. Falls $s = 0$ zurück zu 1, sonst ist die Unterschrift $u := (r, s)$.

DSA – Unterschriften

Bei Wahl des öffentlichen Schlüssels $pk := (p,q,g,A)$ ist der Klartextraum $P := \{0,1\}^*$, der Unterschriftenraum ist $U := \mathbb{Z}_q \times \mathbb{Z}_q$.

$h: \{0,1\}^* \to \mathbb{Z}_q$ ist eine kollisionsresistente Hashfunktion.

Verifikation von $(m,r,s) \in \{0,1\}^* \times \mathbb{Z}_q \times \mathbb{Z}_q$

$$V_{pk}(m,r,s) = 1 \Leftrightarrow \begin{cases} 0 \le r \le q-1, 1 \le s \le q-1 \\ r = \left(\left(A^{(rs^{-1}) \bmod q} g^{(h(m)s^{-1}) \bmod q} \right) \bmod p \right) \bmod q \end{cases}.$$

Vergleich Elgamal und DSA

Unterschrift bei Klartext $m \in \{0,1\}^*$ und $sk = (p,g,a)$

1. Wähle $k \in \{1,\ldots,p-2\}$ mit $ggT(k,p-1) = 1$ zufällig.
2. Setze $r := g^k \bmod p$ und $s := k^{-1}\left(h(m) - a \cdot r\right) \bmod p-1$.
3. Die Unterschrift ist $u := (r,s)$.

Unterschrift bei Klartext $m \in \{0,1\}^*$ und $sk = (p,q,g,a)$

1. Wähle $k \in \{1,\ldots,q-1\}$ zufällig.
2. Setze $r := \left(g^k \bmod p\right) \bmod q$ und

$$s := k^{-1}\left(h(m) + a \cdot r\right) \bmod q.$$

3. Falls $s = 0$ zurück zu 1, sonst ist die Unterschrift $u := (r,s)$.

Beobachtung Wird das gleiche p verwendet sind DSA-Unterschriften deutlich kürzer als Elgamal-Unterschriften.

Vergleich Elgamal und DSA

Verifikation von $(m,r,s) \in \{0,1\}^* \times \mathbb{Z}_p \times \mathbb{Z}_{p-1}$

Für alle $(m,r,s) \in \{0,1\}^* \times \mathbb{Z}_p \times \mathbb{Z}_{p-1}$ **ist**

$$V_{(p,g,A)}(m,r,s) = 1 \Leftrightarrow A^r r^s = g^{h(m)} \bmod p.$$

Verifikation von $(m,r,s) \in \{0,1\}^* \times \mathbb{Z}_q \times \mathbb{Z}_q$

$$V_{pk}(m,r,s) = 1 \Leftrightarrow \begin{cases} 0 \le r \le q-1, 1 \le s \le q-1 \\ r = \left(\left(A^{(rs^{-1}) \bmod q} g^{(h(m)s^{-1}) \bmod q} \right) \bmod p \right) \bmod q \end{cases}.$$

Beobachtung Verifikation in DSA benötigt zwei Exponentiationen, in Elgamal dagegen drei.

Vergleich Elgamal und DSA

Vermutung **Bei Wahl des gleichen p haben Elgamal-Unterschrift und DSA-Unterschriften identische Sicherheitseigenschaften.**

Fazit **DSA liefert kürzere Unterschriften und größere Effizienz als Elgamal bei gleicher Sicherheit.**