- Veranstaltung: „Elliptische Kurven und Kryptographie“
- Programm:
  - 19:30 – Der BraLUG e.V. stellt sich (kurz!) vor
  - 19:40 – Teil 1: Asymmetrische Kryptographie
    (Jan Tobias Mühlberg)
  - 20:15 – Pause
  - 20:25 – Teil 2: Kurven, elliptische
    (Arnd Zapletal)
  - 21:00 – Schluss. Aus. Ende.

Elliptische Kurven und Kryptographie

— Teil 1: Asymmetrische Kryptographie —

Jan Tobias Mühlberg
muehlber@fh-brandenburg.de

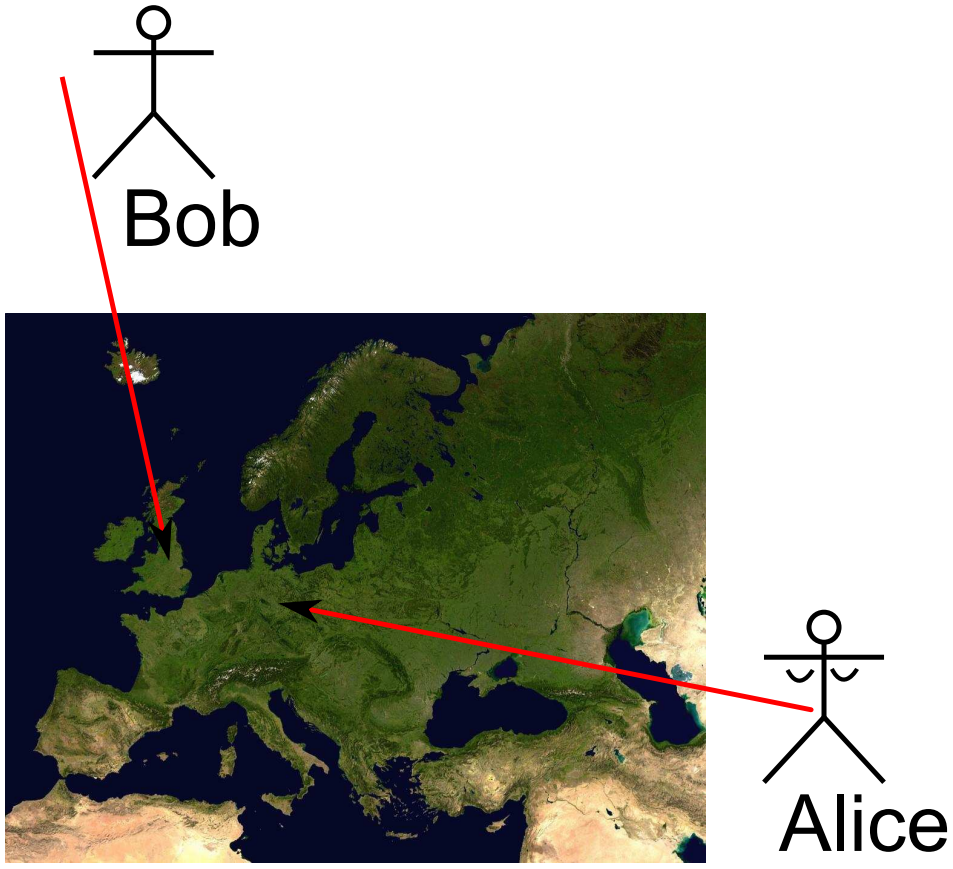
Brandenburger Linux User Group

Brandenburg, 20. Dezember 2006

Überblick

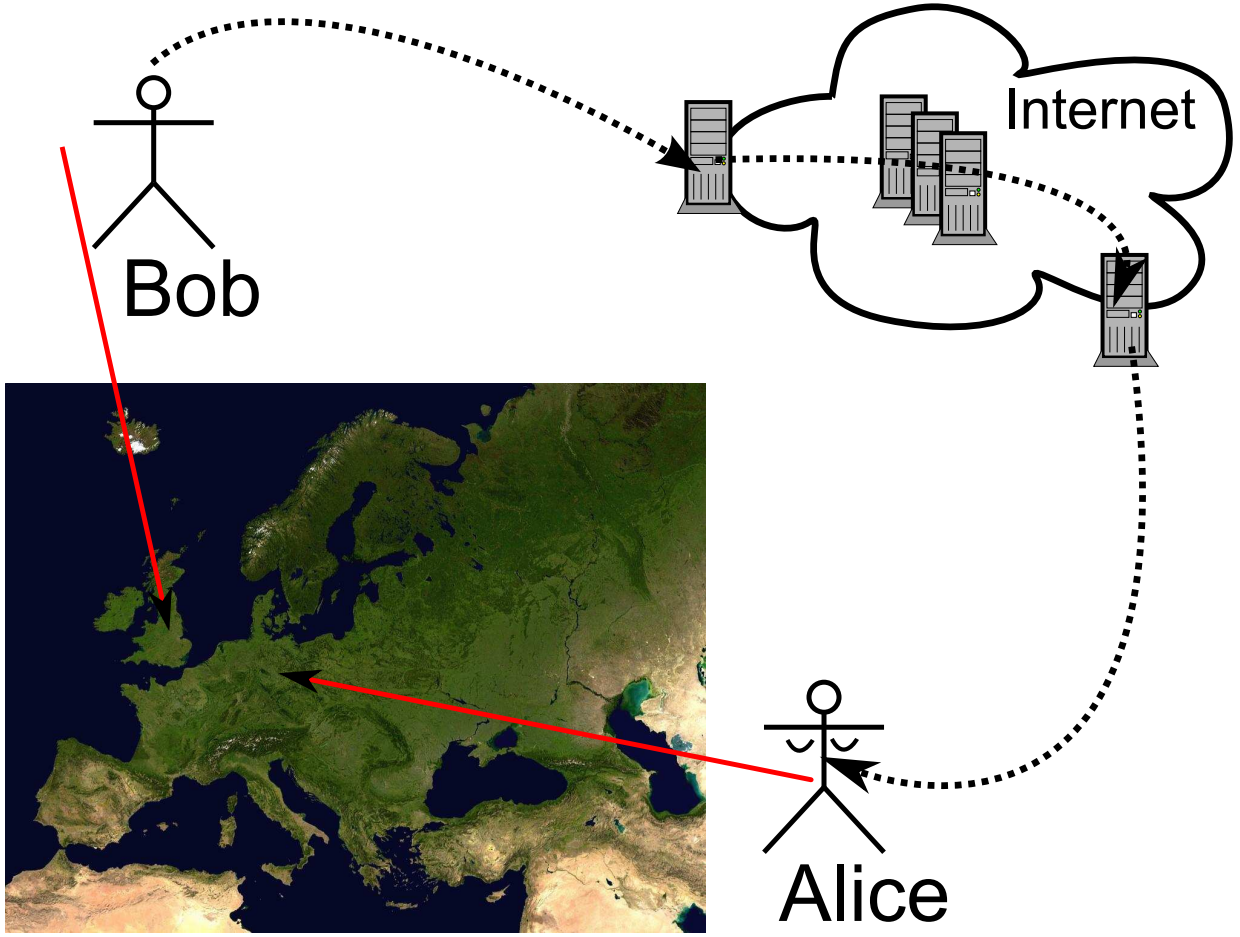
1. Die übliche Liebesgeschichte
2. Kryptographie?!
3. Asymmetrische Kryptographie
4. Die Mathematik dahinter
   - RSA und das Problem der Faktorisierung
   - ElGamal und der diskrete Logarithmus

1. Die übliche Liebesgeschichte



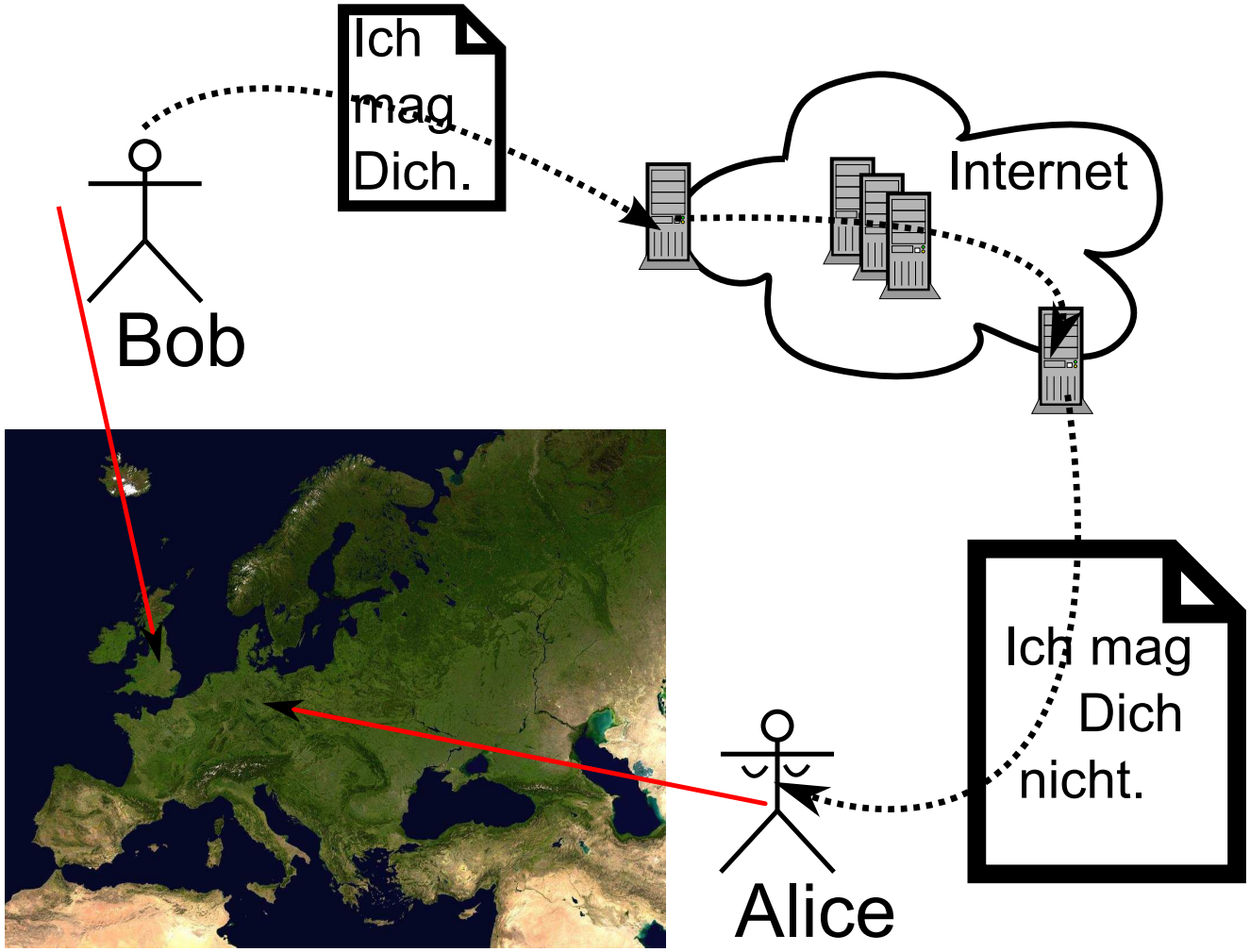
Satellitenbild von (NASA, 2002).

1. Die übliche Liebesgeschichte



Satellitenbild von (NASA, 2002).

1. Die übliche Liebesgeschichte



Satellitenbild von (NASA, 2002).

Kryptographie?!

- Grundsätzlich werden mit kryptographischen Verfahren die folgenden Ziele verfolgt:
  - **Vertraulichkeit**
  - **Authentizität**
  - **Integrität**

Kryptographische Verfahren

- Wichtige Begriffe:
  - **Kryptographisches Verfahren**
  - **Klartext**, **Geheimtext**
  - **Schlüssel**
  - **verschlüsseln**, **entschlüsseln**

Kryptographische Verfahren

- In Abhängigkeit davon, wie in einem Verfahren mit dem Schlüsselmaterial umgegangen wird, unterscheidet man zwischen
  - **symmetrischen** Verschlüsselungsverfahren und
  - **asymmetrischen** Verschlüsselungsverfahren.

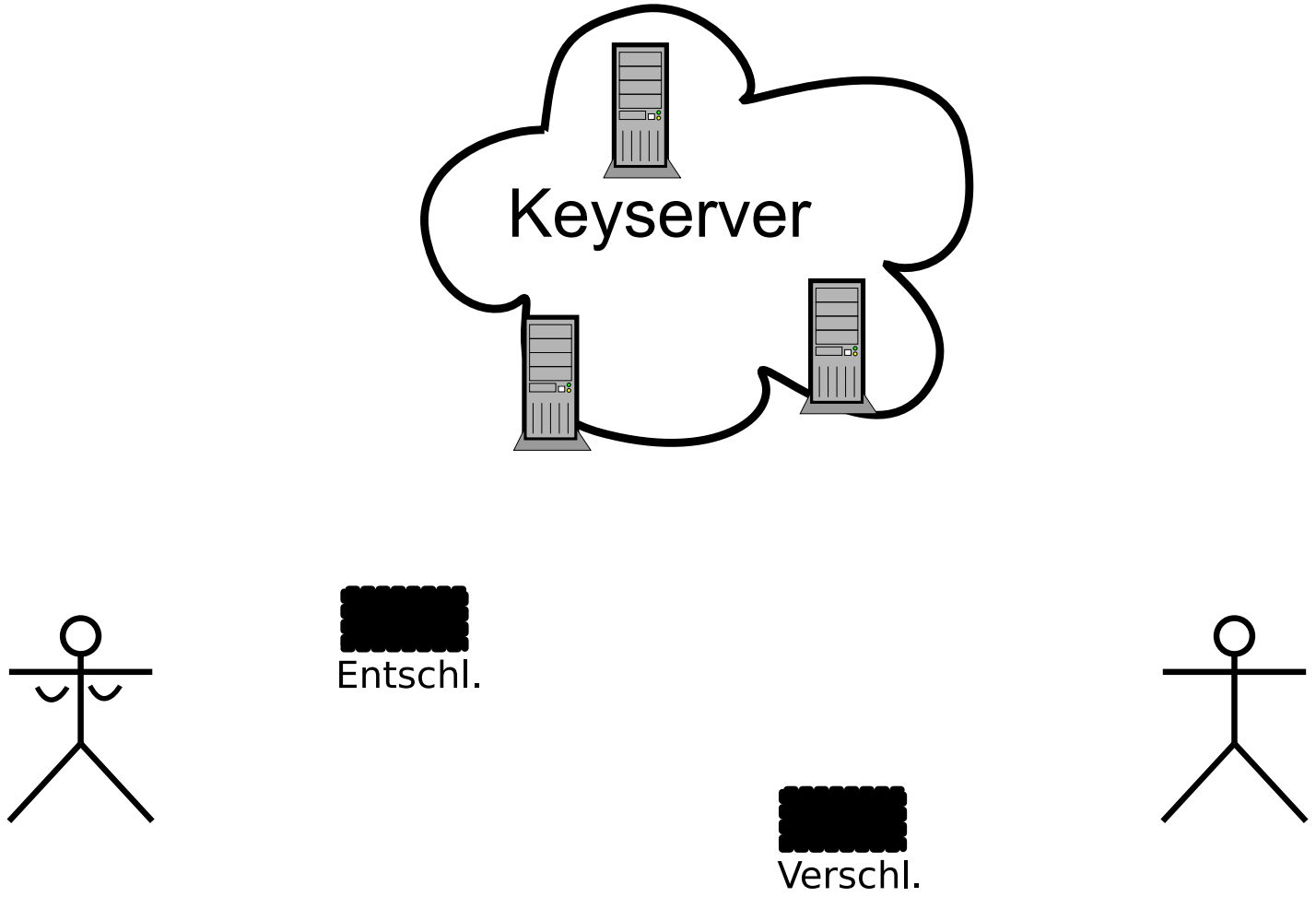
Asymmetrische Kryptographie

- junge Gruppe kryptographischer Verfahren
- erste Veröffentlichung 1976 (Diffie and Hellman, 1976); seit etwa 20 Jahren praktisch eingesetzt
- jeder Teilnehmer besitzt ein Schlüsselpaar, einen **öffentlichen** und einen **privaten Schlüssel**.

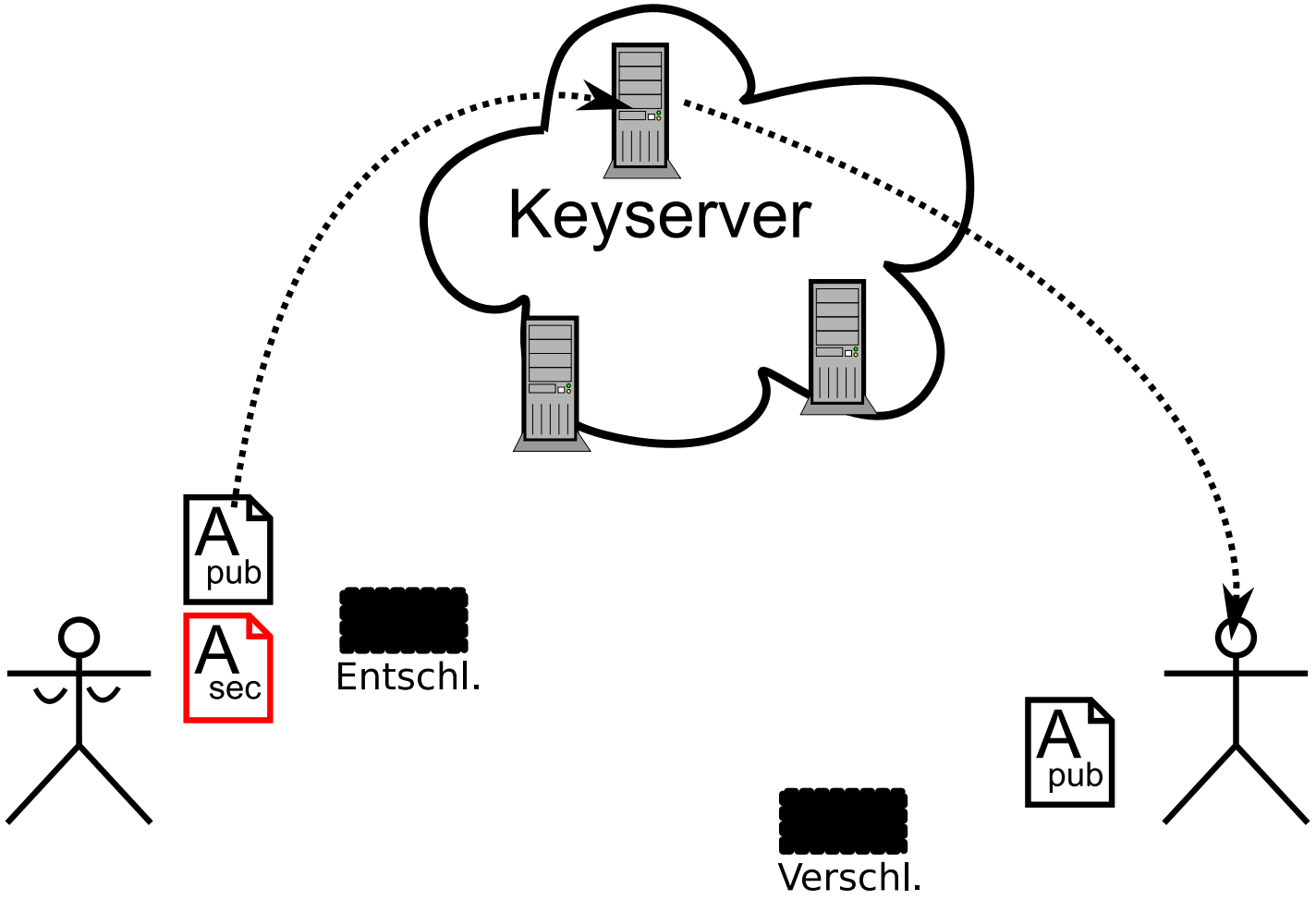
Asymmetrische Kryptographie

- **öffentliche Schlüssel** werden frei zugänglich hinterlegt
- **private Schlüssel** werden um jeden Preis geheimgehalten
- Nachrichten die mit dem **öffentlichen Schlüssel verschlüsselt** sind, können man nur mit dem zugehörigen **privaten Schlüssel entschlüsselt** werden, und umgekehrt.

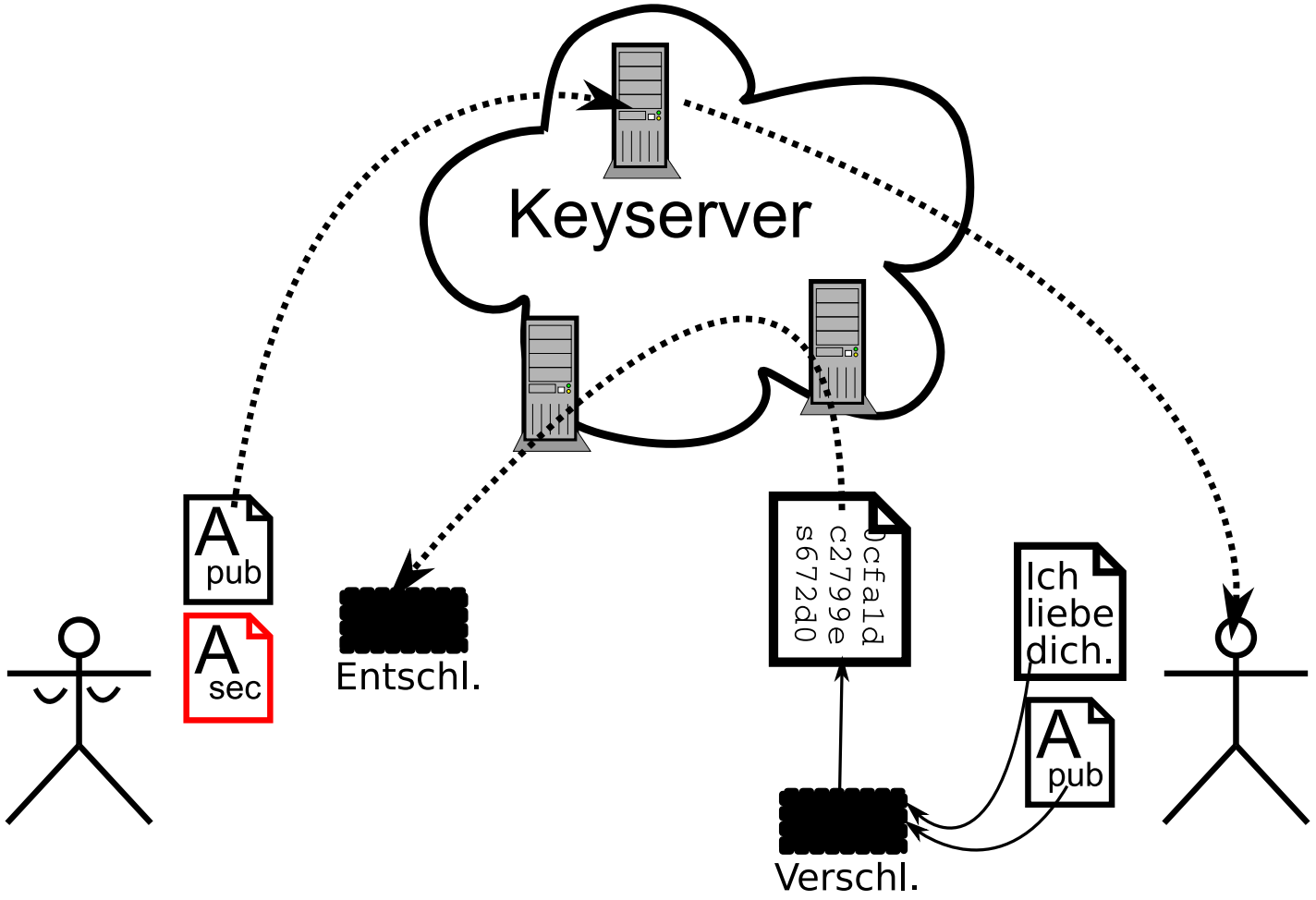
Ver- und Entschlüsselung



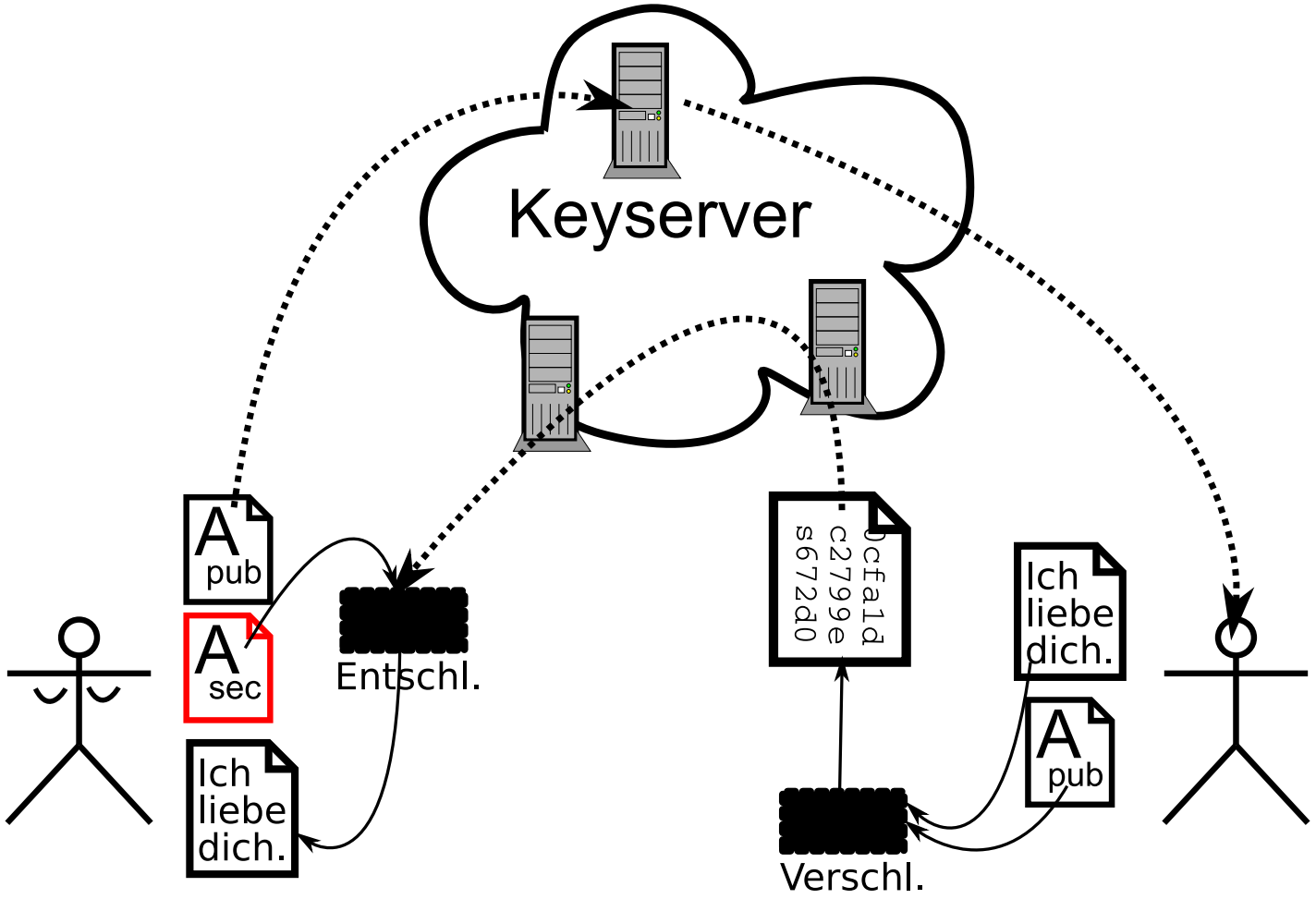
Ver- und Entschlüsselung



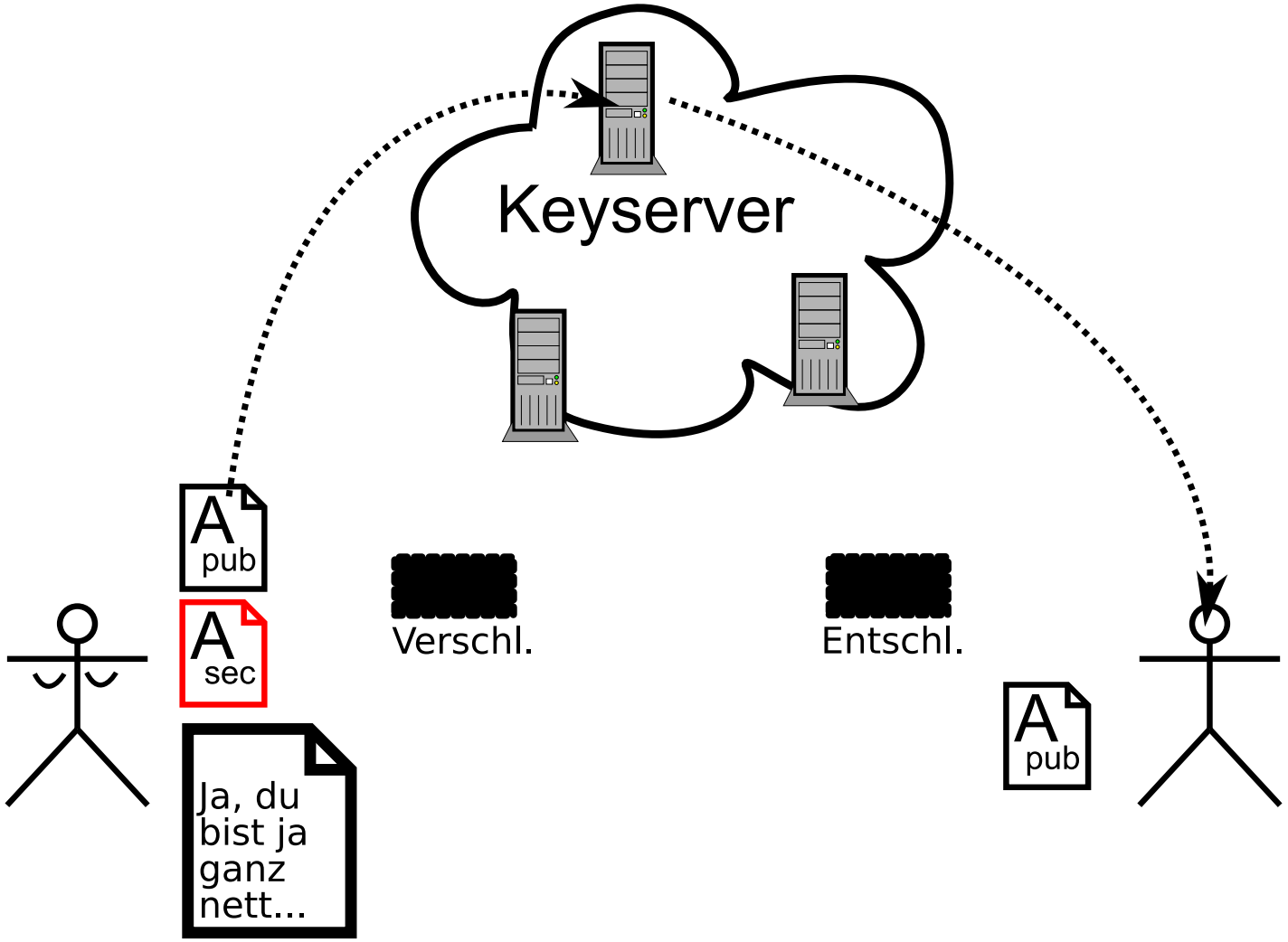
Ver- und Entschlüsselung



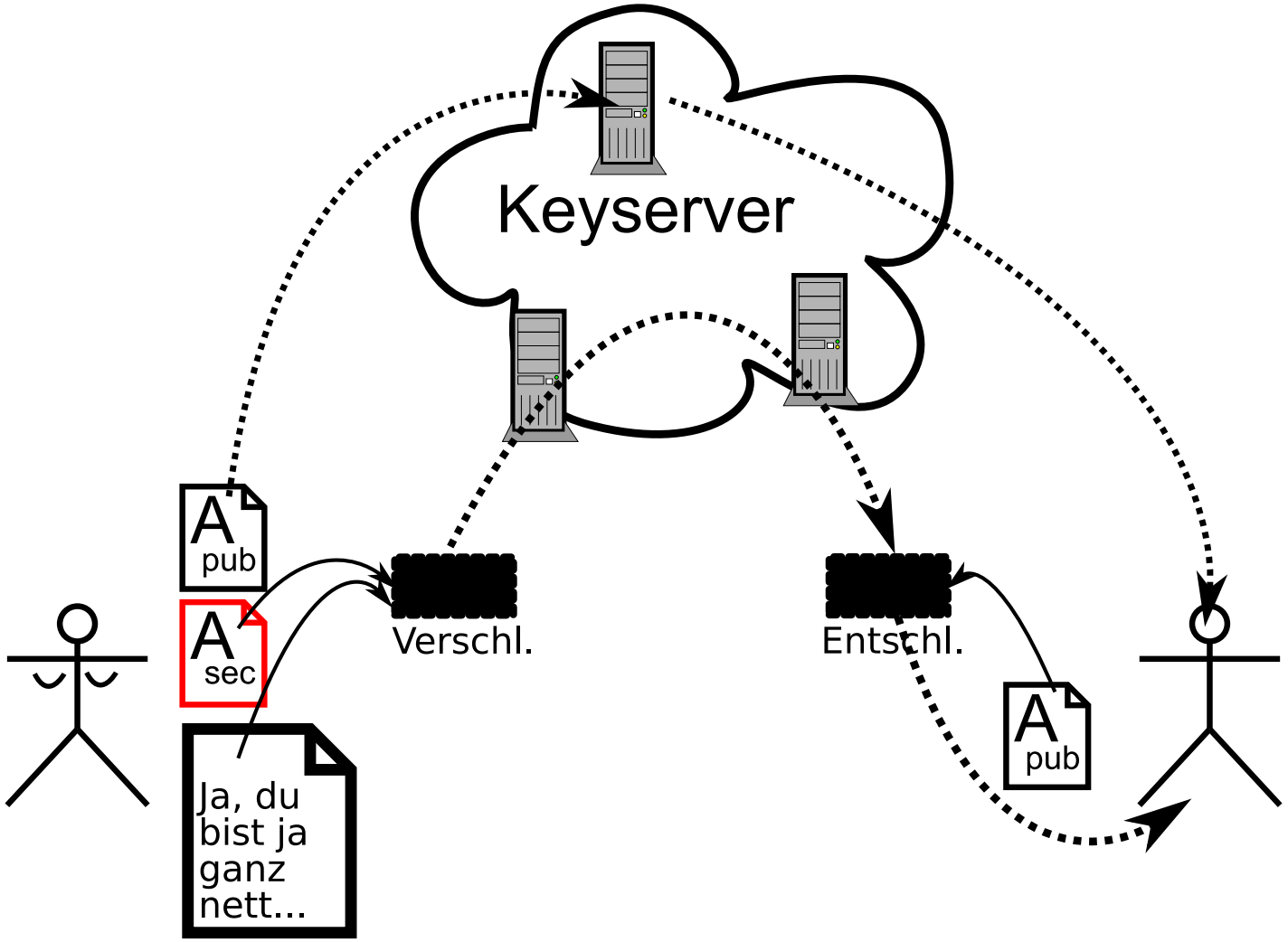
Ver- und Entschlüsselung



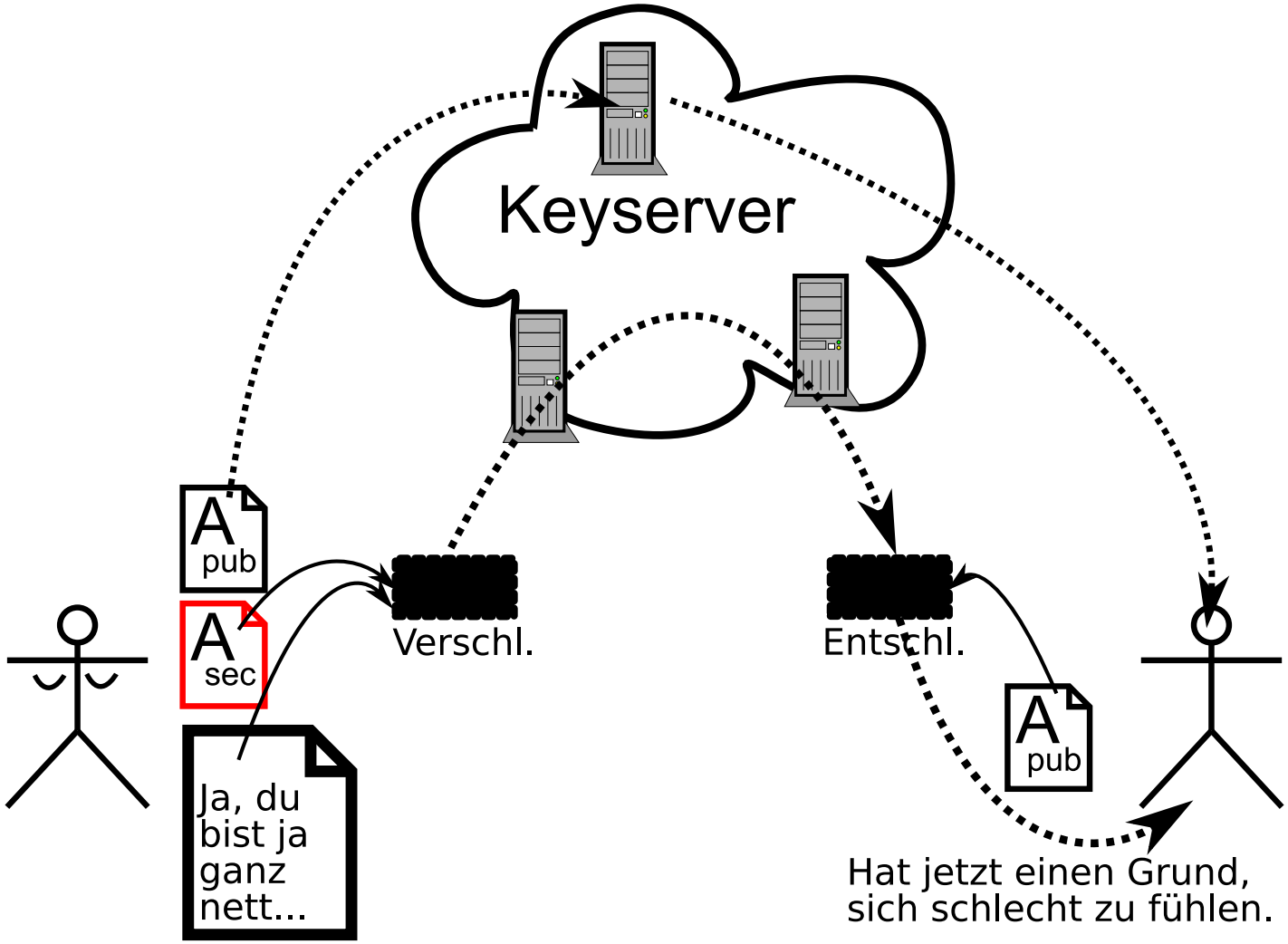
Digitale Signaturen



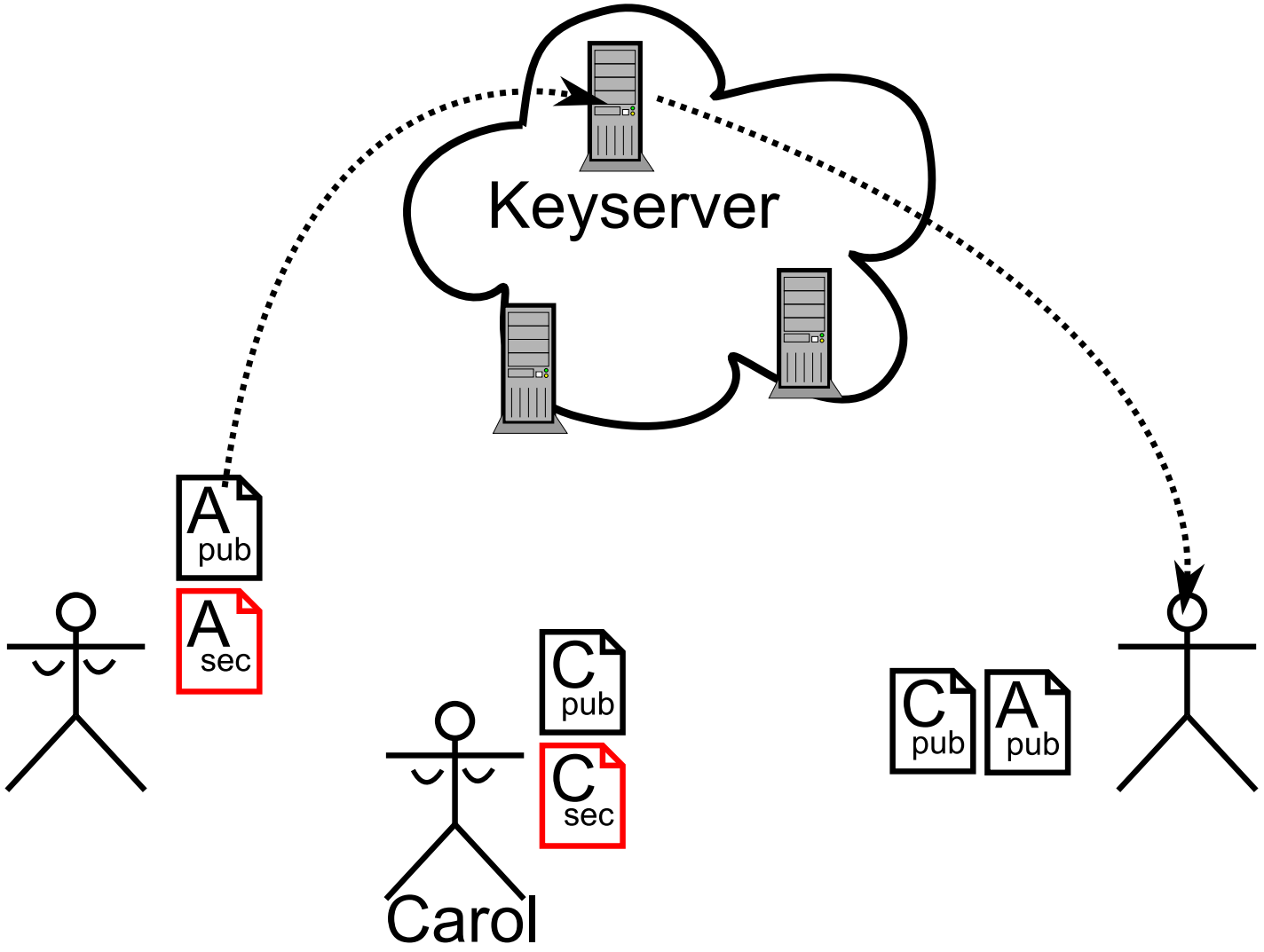
Digitale Signaturen



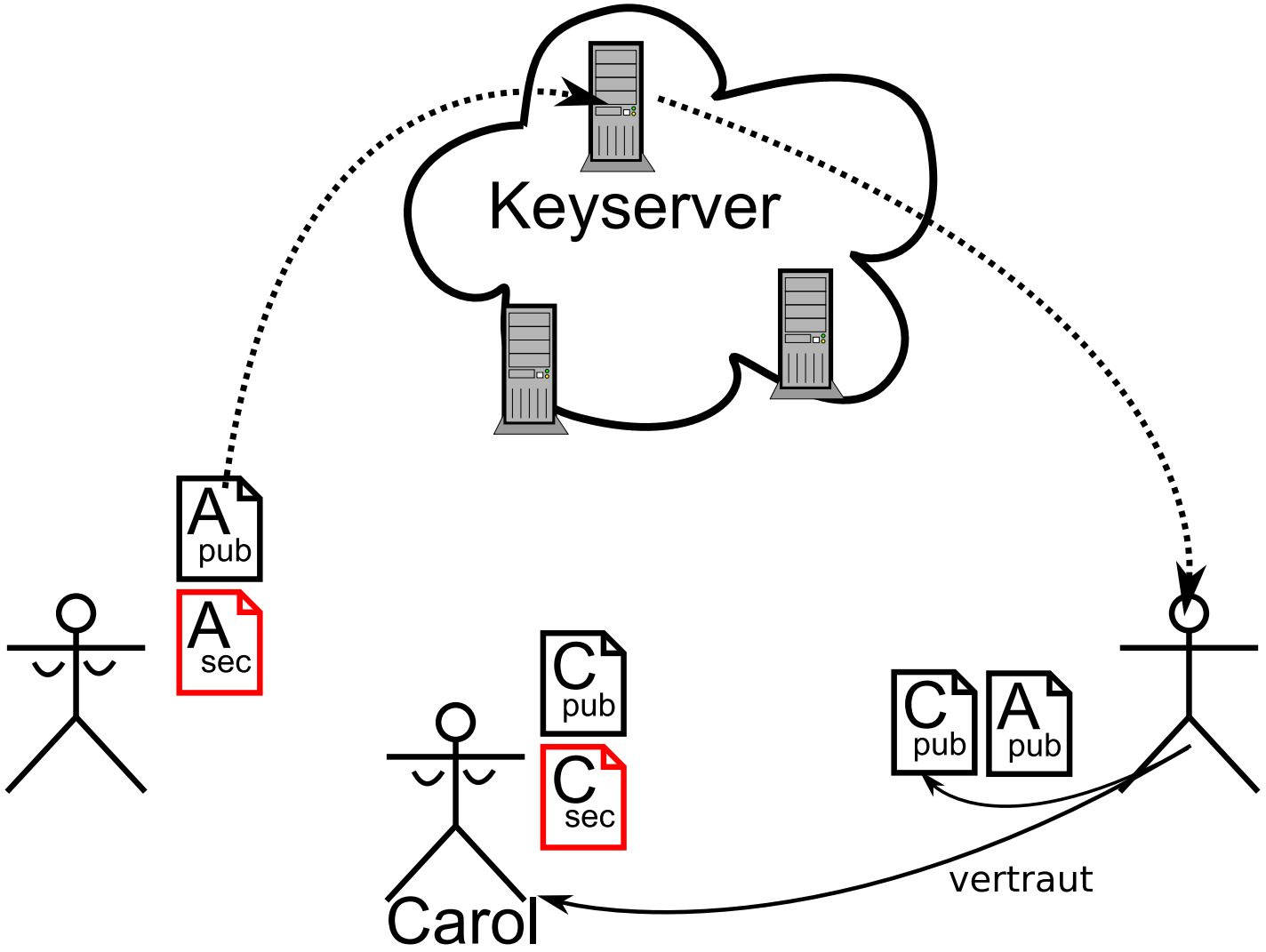
Digitale Signaturen



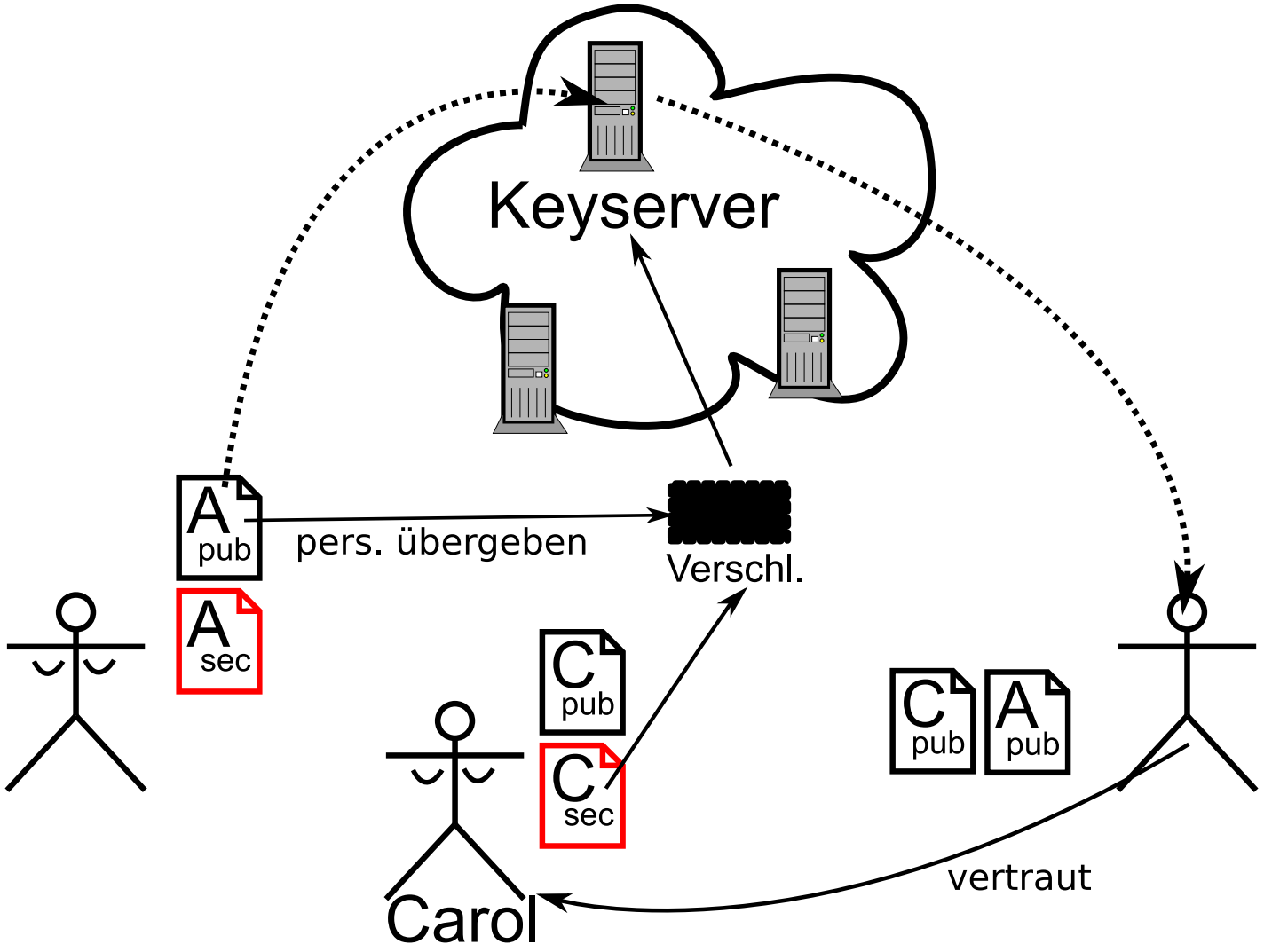
Schlüssel signieren



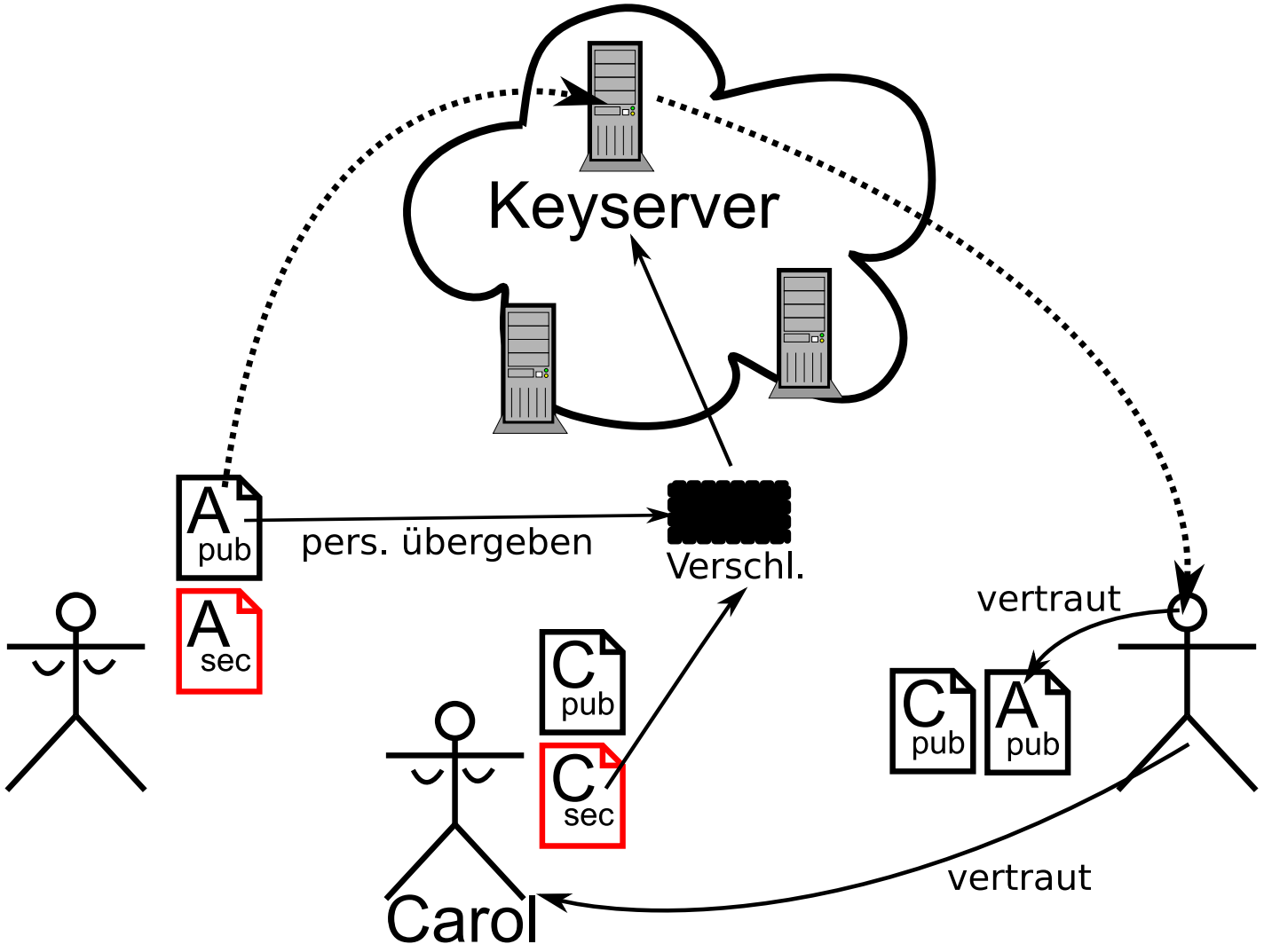
Schlüssel signieren



Schlüssel signieren



Schlüssel signieren



Die Mathematik dahinter

- Asymmetrische Kryptosysteme basieren auf komplizierten mathematischen Problemen.

  Folgendes ist dabei wichtig:

  – Privater und öffentlicher Schlüssel müssen relativ „einfach“ zu erzeugen sein.

  – Der private Schlüssel darf „nicht“ aus dem öffentlichen Schlüssel zu errechnen sein.

Die Mathematik dahinter (cont'd)

- In der Praxis werden vor allem zwei mathematische Probleme ausgenutzt:
  - Faktorisierung einer Zahl in ihre Primfaktoren
  - Diskreter Logarithmus

4.1 Faktorisierung (cont’d)

4.1 Faktorisierung (cont'd)

- wird in RSA (Rivest et al., 1978) genutzt, weit verbreitet
- Idee: Die Multiplikation zweier Primzahlen ist einfach zu berechnen, die Zerlegung des Produktes in seine Faktoren ist dagegen mit viel Aufwand verbunden.

4.1 Faktorisierung (cont'd)

- Schlüsselerzeugung in RSA:
  - wähle zwei zufällige Primzahlen $p \neq q$
  - berechne $N = pq$
  - bestimme $\varphi(N) = (p-1)(q-1)$
  - wähle e, so dass $1 < e < \varphi(N)$ und e teilerfremd zu $\varphi(N)$ ist

4.1 Faktorisierung (cont'd)

- Schlüsselerzeugung in RSA:
  - berechne d, so dass $de \equiv 1 \ (mod \ \varphi(N))$ gilt
  - privater Schlüssel: d, N
  - öffentlicher Schlüssel: e, N

4.1 Faktorisierung (cont'd)

- Um den privaten Schlüssel aus dem öffentlichen Schlüssel zu berechnen, muss man also d bestimmen.
- Dazu braucht man vor allem $\varphi(N)$, und das ist wiederum nur dann effizient möglich, wenn man p und q kennt.

4.1 Faktorisierung (cont'd)

- Das Faktorisierungsproblem lässt sich heute am effizientesten mit einem zweistufigen Ansatz lösen:
  - Siebungsschritt – sucht bestimmte Quadratzahlen, gut parallelisierbar
  - Zahlkörpersieb – sucht Abhängigkeiten in einer großen Zahlenmatrix

4.1 Faktorisierung (cont'd)

- Für den Siebungsschritt kann Spezialhardware verwendet werden (TWIRL, (Geiselmann and Steinwand, 2003))
- Für etwa 10 Mio. USD lässt sich ein 1 kBit Schlüssel in einem Jahr brechen
- Das Verfahren ist hochgradig parallelisierbar, die Hardware ist hinterher nicht verbraucht (siehe auch (Weiss et al., 2003))

4.2 Diskreter Logarithmus

4.2 Diskreter Logarithmus

- Diskrete Exponentialfunktion: $y = b^x \, mod \, p$ (Divisionsrest von $\frac{b^x}{p}$, berechenbar in $\leq 2 \, log_2(x)$ Multiplikationen)
- Wir verwenden p, b, y als öffentlichen und x als privaten Schlüssel (ElGamal-Verfahren).
- Diskreter Logarithmus: Wir suchen $x = log_b \, y$ für $y \equiv b^x \, mod \, p$ (unendlich viele Antworten)

4.2 Diskreter Logarithmus (cont'd)

- Beispiel:

$$3^4 \, mod \, 17 = 81 \, mod \, 17 = 13$$

weil: $4 * 17 + 13 = 81$

$x = log_3 \, y$ für $y \equiv 3^x \, mod \, 17 = 13$

$\rightarrow$ Ausprobieren.

4.2 Diskreter Logarithmus (cont'd)

- Beispiel:

$$3^0 = 1 \equiv 1 \,(mod\, 17) \quad 3^3 = 27 \equiv 10 \,(mod\, 17)$$
$$3^1 = 3 \equiv 3 \,(mod\, 17) \quad 3^4 = 81 \equiv 13 \,(mod\, 17)$$
$$3^2 = 9 \equiv 9 \,(mod\, 17)$$

$\longrightarrow$ x könnte 4 sein. Vielleicht aber auch nicht. 1732, 2388 und 2628 sind ebenfalls Lösungen.

– In der Praxis haben alle Zahlen ziemlich viele Stellen. . .

4.2 Diskreter Logarithmus (cont'd)

- Bislang sind keine effizienten Lösungsverfahren für den diskreten Logarithmus bekannt.
- Einziger Nachteil: Verschlüsselung und Entschlüsselung sind recht rechenaufwendig.
- → *elliptische Kurven*

Danke!

Folien:

http://zeus.fh-brandenburg.de/~muehlber/bralug/ecc-intro/ecc-intro_teil1.pdf

Literatur

Diffie, W. and Hellman, M.: 1976, *Information Theory, IEEE Transactions on* **22**, 644

Geiselmann, W. and Steinwand, R.: 2003, A dedicated sieving hardware, in *Public Key Cryptography Conference*, No. 2567 in LNCS, pp 254 – 266

NASA: 2002, *A satellite composite image of Europe*, http://visibleearth.nasa.gov/view_rec.php?vev1id=11656

Rivest, R., Shamir, A., and Adleman, L.: 1978, *Communications of the ACM* **21**, 120

Weiss, R., Lucks, S., and Bogk, A.: 2003, *Die Datenschleuder*