CryptoCampaign

RSA, GPG

Marcel Hellwig, Felix Wiedemann

KunterBuntesSeminar
WiSe 2014/15

Donnerstag, 30. Oktober 2014

Warum E-Mails verschlüsseln?

- vertrauliche Inhalte
- E-Mails können abgefangen werden
- Sysadmins können E-Mails lesen :o
- weil es geht

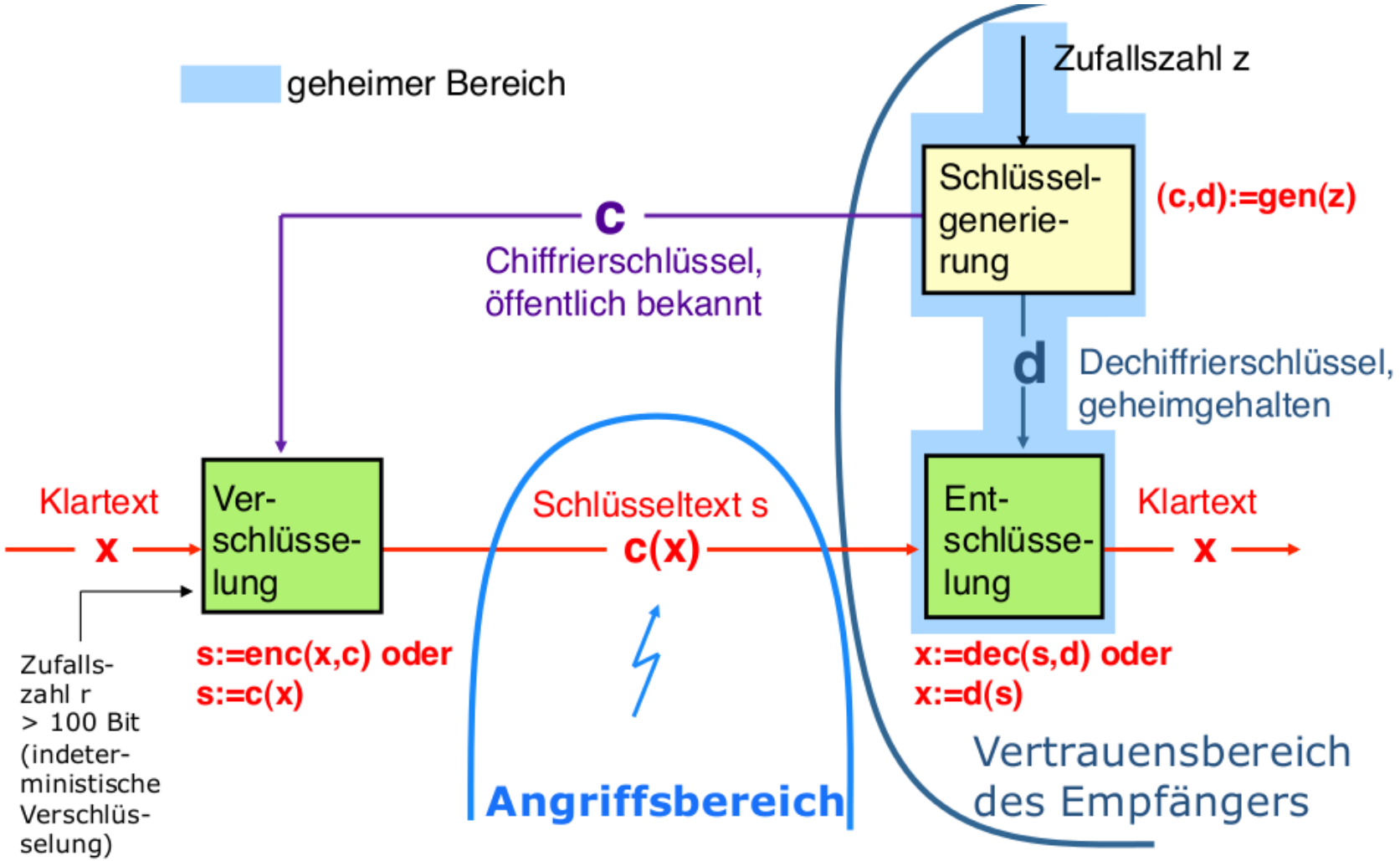
Warum E-Mails signieren?

- Absender kann gefälscht sein
- Inhalt kann verfälscht sein
- weil es geht

Asymmetrische Verschlüsselung

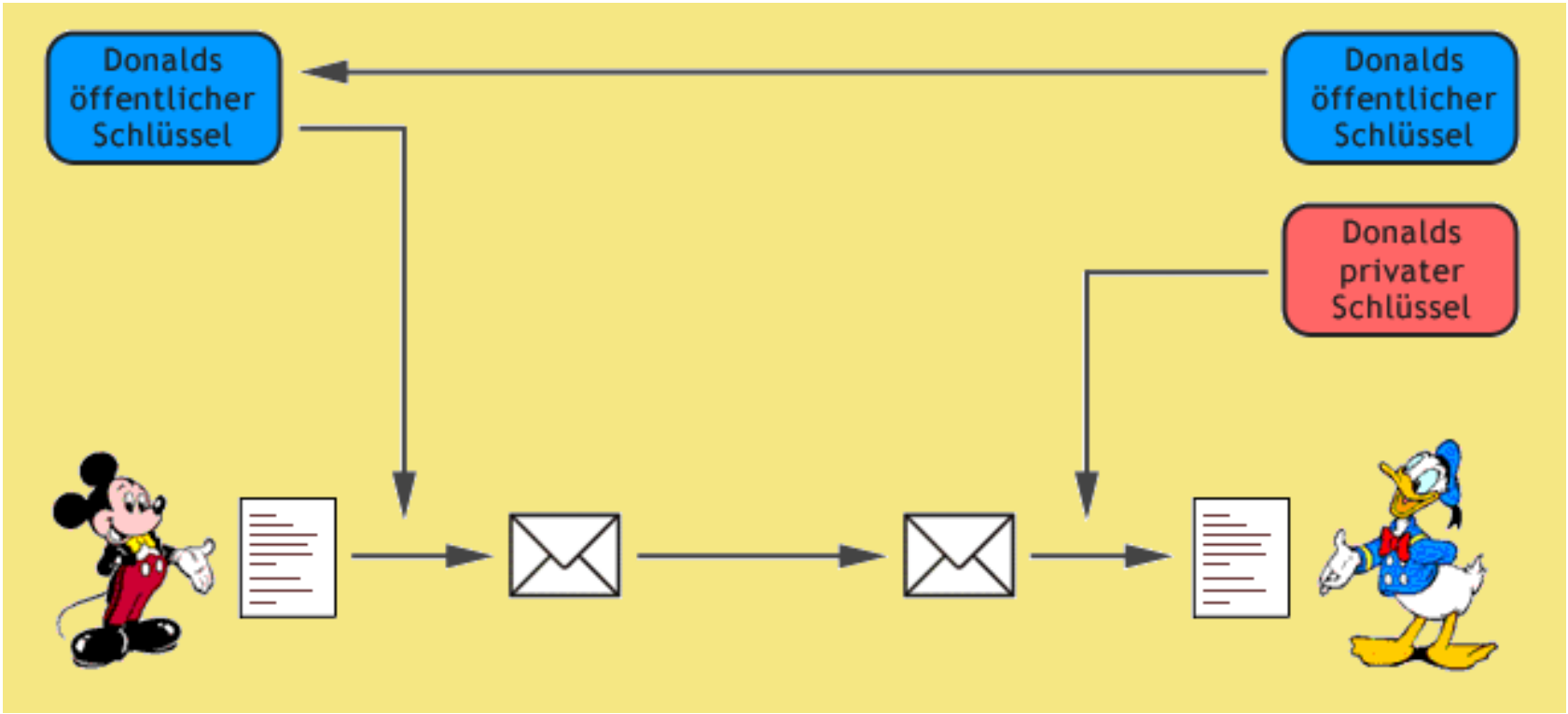
- asymmetrisch: privater vs. öffentlicher Schlüssel
- verschlüsseln: öffentlicher Schlüssel des Empfängers
- entschlüsseln: privater Schlüssel des Empfängers
- signieren: privater Schlüssel des Absenders
- verifizieren: öffentlicher Schlüssel des Absenders

Asymmetrische Verschlüsselung (© Hannes Federrath)



Kasten mit Schnappschloss. Es gibt nur einen Schlüssel.

Und jetzt nochmal Erstie-gerecht:



Schlüsselgenerierung – in Worten

- privater Schlüssel wird zufällig gewählt
- öffentlicher Schlüssel wird mit einem bestimmten Verfahren *aus dem Privaten* errechnet
- der öffentliche Schlüssel ist öffentlich!
- das besagte Verfahren ist öffentlich! (*ba dum ts*)
- also: wir benötigen ein Einweg-Verfahren

Schlüsselgenerierung – etwas mathematischer

- *private* zufällig gewählt
- $f : M(private) \rightarrow M(public)$
- $M(private) = M(public) = \mathbb{N}$
- f ist eine Einwegfunktion
  - f mit polynomialem Aufwand berechenbar
  - f^{-1} nur mit exponentiellem Aufwand
- f ist eine Bijektion

RSA – Vorbereitung

Satz (abgewandelter Satz von Euler)

Sei n das Produkt zweier (verschiedener) Primzahlen p und q. Dann gilt für beliebige $k, m \in \mathbb{N}$ mit $m < n$:

$$m = m^{k \cdot \phi(n)+1} \mod n$$

- ϕ ist die eulersche Funktion
- $\phi(n) = (p-1)(q-1)$

RSA – Schlüsselgenerierung

1. Wähle zwei (große, teilerfremde) Primzahlen p und q.
2. Berechne: $n = p \cdot q$ sowie $\phi(n) = (p-1)(q-1)$.
3. Wähle eine Zahl $e \in \mathbb{N}$ mit $ggT(e, \phi(n)) = 1$.
4. Bestimme das Inverse d von e in $\mathbb{Z}_{\phi(n)}$ $(e \cdot d \mod \phi(n) = 1)$.
5. privat: (d, n), öffentlich: (e, n).

RSA – Verschlüsselung

- Verschlüsselung: $c = m^e \mod n$
- Entschlüsselung: $m = c^d \mod n$
- Begründung: $c^d = m^{ed} = m^{k \cdot \phi(n)+1} = m$ (in $\mathbb{Z}_n$)

RSA – Besonderheit

- privater und öffentlicher Schlüssel zueinander invers
- Inversitätsbeziehungen sind gegenseitig
- $\Rightarrow$ die Schlüssel sind beliebig vertauschbar
- RSA ist das *einzige* Verfahren mit dieser Eigenschaft!

RSA – Signatur

- Absender verschlüsselt Hashwert der Nachricht mit *privatem* Schlüssel
- Nachricht wird unverschlüsselt versendet
- Empfänger entschlüsselt Hashwert mit öffentlichem Schlüssel
- Signatur okay, wenn das Ergebnis mit dem Hashwert der Nachricht übereinstimmt

RSA – Einwegfunktion

- Einwegfunktion: $f(p, q) = p \cdot q = n$
- f^{-1} bedeutet Primfaktorzerlegung
- Trapdoor-Einwegfunktion: $g : M(private) \rightarrow M(public)$
- g^{-1} benötigt Kenntnis von $\phi(n)$
- $\phi(n)$ benötigt Kenntnis von f^{-1}
- $\Rightarrow$ f umkehrbar gdw. g umkehrbar

GPG

- Linux: /usr/bin/gpg
- Windows: gpg4win.org
- Mac OS X: gpgtools.org
- alle: Thunderbird (mozilla.org/thunderbird) + Enigmail
- Keyserver der Fachschaft: https://mafiasi.de/pks/ bzw. hkp://mafiasi.de