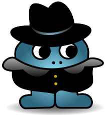
CryptoCampaign
RSA, ElGamal, GPG

Niklas Steenfatt

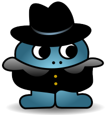
KunterBuntesSeminar
WiSe 2013/14

Dienstag, 29. Oktober 2013



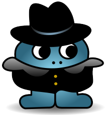
Warum E-Mails verschlüsseln?

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



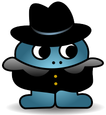
Warum E-Mails signieren?

- Absender kann gefaket sein
- Inhalt kann verfälscht sein
- Zeitstempel kann manipuliert sein
- weil es geht

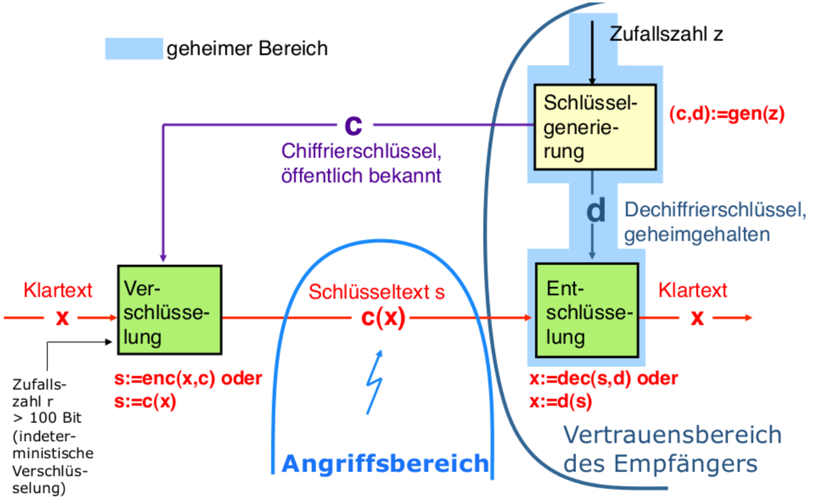


Asymmetrische Verschlüsselung

- 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

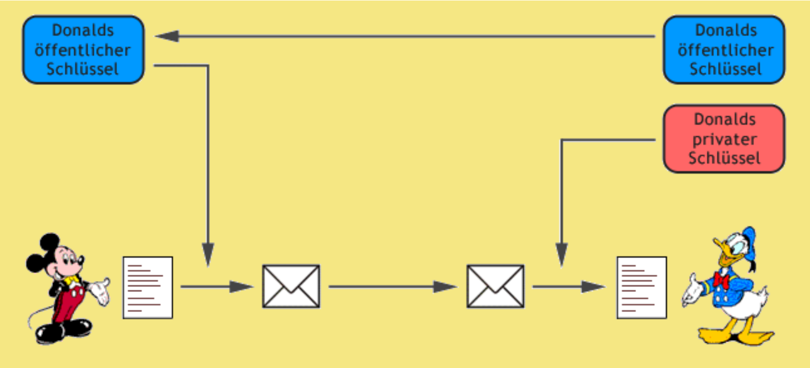


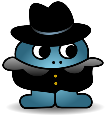
Asymmetrische Verschlüsselung (© Hannes Federrath)



Kasten mit Schnappschloss. Es gibt nur einen Schlüssel.

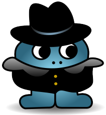
Und jetzt nochmal Erstie-gerecht:





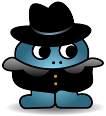
Schlüsselgenerierung – in Worten

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



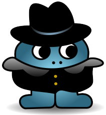
RSA – Vorbereitung

Satz 1 (Satz von Euler).

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

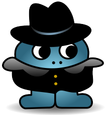
$$m = m^{k \cdot \phi(n)+1} \mod n$$

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



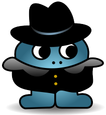
RSA – Schlüsselgenerierung

1. Wähle zwei (große) 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. Sei $k \in \mathbb{N}$ mit $ed = k \cdot \phi(n) + 1$ (es gilt $\phi(n) \mid ed - 1$).
6. privat: (d, n), öffentlich: (e, n).



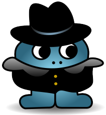
RSA – Verschlüsselung

- 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 $\mathbb{Z}_n$)



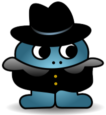
RSA – Besonderheit

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



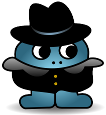
RSA – Signatur

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



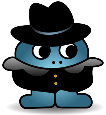
RSA – Einwegfunktion

- 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



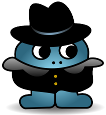
ElGamal – Schlüsselgenerierung

1. Es sei p eine Primzahl.
2. Es seien $g, x \in \mathbb{N}$ beliebig gewählt, mit der Bedingung $g < p \land x < p$.
3. Es sei $y = g^x \mod p$.
4. privat x, öffentlich: (y, g, p).



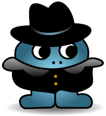
ElGamal – Signatur

- Absender wählt ein $k \in \mathbb{N}$ mit $ggT(k, p-1) = 1$.
- Absender berechnet $a = g^k \mod p$
- sowie b mit $M = (xa + kb) \mod (p-1)$.
- (a, b) ist die Signatur.
- Verifikation durch $y^a a^b = g^M$.



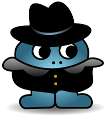
ElGamal – Verschlüsselung

- Absender wählt ein $k \in \mathbb{N}$ mit $ggT(k, p-1) = 1$.
- Absender berechnet $a = g^k \mod p$
- sowie $b = y^k M \mod p$.
- (a, b) ist der Chiffretext.
- Entschlüsselung durch $M = \frac{b}{a^x} \mod p$.



ElGamal – Einwegfunktion

- Einwegfunktion: $f : M(private) \rightarrow M(public)$
- $f(x) = g^x \mod p$
- f^{-1} ist ein diskreter Logarithmus auf G
- G ist eine multiplikative Gruppe über $\mathbb{Z}_p$



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/