Einführung in die (E-Mail-)Kryptographie

KBS • WS2020/21

Pascal Wichmann

Universität Hamburg

25. Januar 2021

Gründe für (E-Mail-)Verschlüsselung

- E-Mails werden beim Transport häufig im Klartext übertragen
- keiner weiß, wer dort alles mitliest

Verhindern, dass ...

- sensible Inhalte von Dritten gelesen werden (können)
- andere Leute Nachrichten im eigenen Namen schreiben können
- der Inhalt verändert werden kann
- gezielte Phishing-Angriffe und E-Mail-Betrug ermöglicht werden
- der E-Mail-Anbieter die eigenen Daten weiterverkauft

Und weshalb nicht nur vertrauliche E-Mails verschlüsseln?

- Verschlüsselung verrät, dass vertraulicher Inhalt vorliegt
- Angreifer sehen sofort, bei welchen E-Mails sich ein Angriff lohnt
- Identitätsdiebstahl wird erschwert
- Schutz vor Massenüberwachung

„Ich habe aber gar nichts zu verbergen!“

"If one would give me six lines written by the hand of the most honest man, I would find something in them to have him hanged.“ — Cardinal Richelieu in 1641

Und wenn die eigene Meinung nicht zur Linie der Regierung passt?

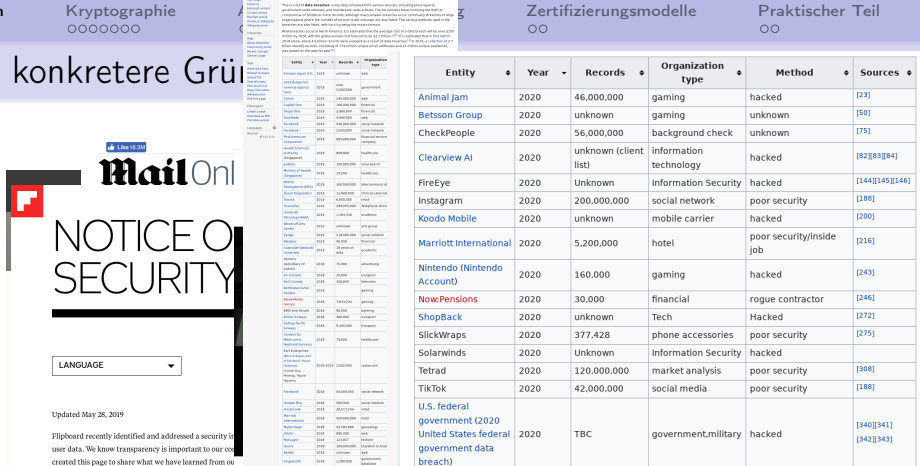
(insbesondere in weniger demokratischen Staaten)

Wie wäre es dann mit einer Webcam im Badezimmer?

Umgang mit Datenschutz betrifft auch andere!

- Hochladen von Fotos, auf denen (auch) andere zu sehen sind
- Hochladen des Adressbuchs bei WhatsApp, Telegram, ...
- Nutzung von Sprachassistenen, smarten Lautsprechen, ...

Noch konkretere Grü



Entity	Year	Records	Organization type	Method	Sources
Animal Jam	2020	46,000,000	gaming	hacked	[23]
Betsson Group	2020	unknown	gaming	unknown	[50]
CheckPeople	2020	56,000,000	background check	unknown	[75]
Clearview AI	2020	unknown (client list)	information technology	hacked	[82][83][84]
FireEye	2020	Unknown	Information Security	hacked	[144][145][146]
Instagram	2020	200,000,000	social network	poor security	[188]
Koodo Mobile	2020	unknown	mobile carrier	hacked	[200]
Marriott International	2020	5,200,000	hotel	poor security/inside job	[216]
Nintendo (Nintendo Account)	2020	160,000	gaming	hacked	[243]
Now:Pensions	2020	30,000	financial	rogue contractor	[246]
ShopBack	2020	unknown	Tech	Hacked	[272]
SlickWraps	2020	377,428	phone accessories	poor security	[275]
Solarwinds	2020	Unknown	Information Security	hacked	
Tetrad	2020	120,000,000	market analysis	poor security	[308]
TikTok	2020	42,000,000	social media	poor security	[188]
U.S. federal government (2020 United States federal government data breach)	2020	TBC	government,military	hacked	[340][341] [342][343]
Vastaamo	2020	130,000	healthcare	hacked	[347]
Virgin Media	2020	900,000	mobile carrier	accidentally exposed	[349][350]
Wattpad	2020	270,000,000	web	hacked	[356]
Wawa (company)	2020	30,000,000	retail	hacked	[357]
YouTube	2020	4,000,000	social media	poor security	[188]
Unknown agency (believed to be tied to United States Census Bureau)	2020	200,000,000	financial	accidentally published	[381]
National Health Information Center (NCZI) of Slovakia	2020	391,250	healthcare	poor security	[382]
Les Éditions	2020	380,000	publisher	unknown	[383]

Rechtliche Datenschutzperspektive

Recht auf informationelle Selbstbestimmung

„GG Art. 2 Abs. 1 in Verbindung mit GG Art. 1 Abs. 1 [...] gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. Einschränkungen dieses **Rechts auf „informationelle Selbstbestimmung“** sind nur im überwiegenden Allgemeininteresse zulässig.“
— Volkszählungsurteil des Bundesverfassungsgerichts, 15.12.1983

Grundrecht auf Vertraulichkeit und Integrität von IT-Systemen

„Das allgemeine Persönlichkeitsrecht (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) umfasst das **Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme**.“ — Urteil des Bundesverfassungsgerichts, 27.02.2008

Europäisches Grundrecht

Schutzziele

- **Vertraulichkeit**
- Verdecktheit

- **Integrität**
- **(Zurechenbarkeit)**
- **(Rechtsverbindlichkeit)**

- Anonymität
- Unbeobachtbarkeit

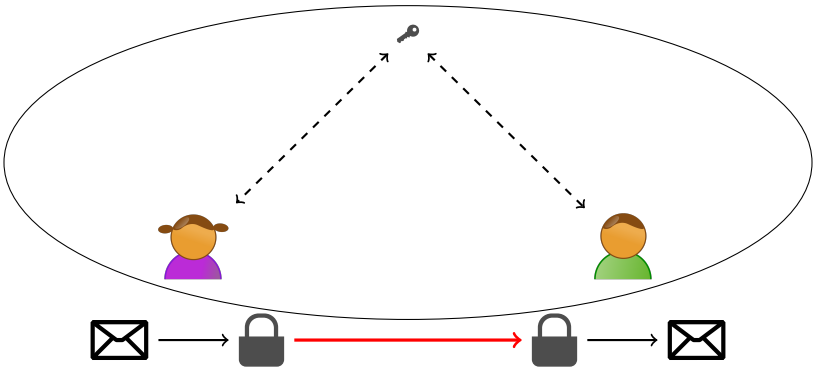
- Erreichbarkeit
- Verfügbarkeit

Was können wir wie erreichen?

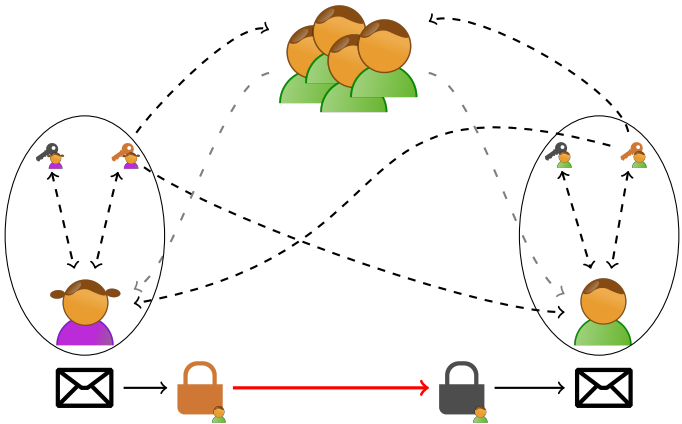
- **Verschlüsseln** von E-Mails und Textnachrichten, damit sie von keiner dritten Person gelesen werden können (Vertraulichkeit)
- **Digitales Signieren** von E-Mails und Textnachrichten, damit niemand anderes im eigenen Namen senden kann (Integrität bzw. Authentizität)

- **Verstecken** von Nachrichten in Grafiken o. ä., damit keine dritte Person von deren Existenz weiß (Verdecktheit)
- Internetzugang über das **Tor-Netz**, damit niemand weiß, welche Internetseiten aufgerufen werden (Anonymität)

Symmetrische Kryptographie



Asymmetrische Kryptographie

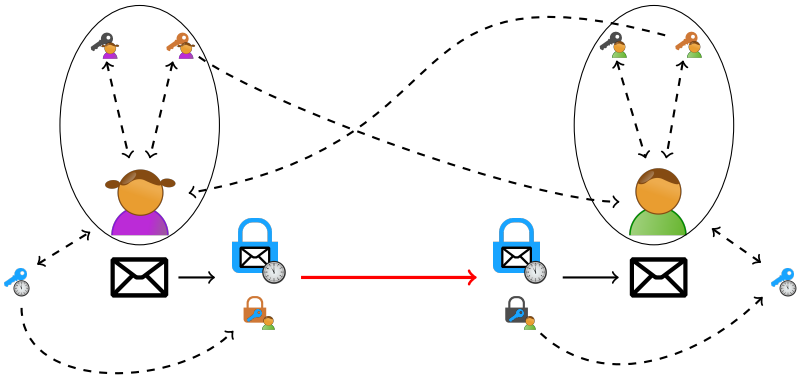


Hybrides Kryptosystem

- Asymmetrische Kryptosysteme ...
  - ... ermöglichen einen einfachen Schlüsselaustausch
  - ... sind vergleichsweise langsam
- Symmetrische Kryptosysteme ...
  - ... verursachen einen hohen Aufwand für den Schlüsselaustausch
  - ... sind vergleichsweise schnell

$\Rightarrow$ Hybride Kryptosysteme ...
  - ... nutzen ein asymmetrisches Kryptosystem für den Schlüsselaustausch
  - ... nutzen ein symmetrisches Kryptosystem für die Verschlüsselung der Inhalte

Hybrides Kryptosystem



Sichere Schlüsselaustauschprotokolle

- Alice und Bob möchten sich auf einen sicheren Schlüssel (für ein symmetrisches Kryptosystem) einigen
- Werden die dabei ausgetauschten Nachrichten abgehört, ist die Sicherheit des Schlüssels nicht beeinträchtigt

Primzahl

Definition (Primzahl)

$p \in \mathbb{N}$, $p > 1$, ist **prim**, wenn sie nur durch 1 und durch p teilbar ist.

Primitivwurzel

Definition (Primitivwurzel)

$a \in \mathbb{Z}$, $1 \leq a < p$, ist **Primitivwurzel** von p, wenn

- a und p teilerfremd sind und
- für alle $1 \leq d < \varphi(p)$ gilt: $a^d \not\equiv 1 \pmod{p}$ $\quad (\varphi(p) = p - 1$, falls p prim$)$

Schlüsselaustauschprotokoll nach Diffie-Hellman

Alice

- empfange a, p und y_B von Bob.
- wähle x_A mit $1 \leq x_A \leq \varphi(p)$ *(geheim)*
- berechne $y_A = a^{x_A} \mod p$ *(öffentlich)*
- berechne $k_{AB} = y_B^{x_A} \mod p$

Bob

- wähle Primzahl p
- wähle Primitivwurzel a von p
- wähle x_B mit $1 \leq x_B \leq \varphi(p)$ *(geheim)*
- berechne $y_B = a^{x_B} \mod p$ *(öffentlich)*
- empfange y_A von Alice
- berechne $k_{BA} = y_a^{x_B} \mod p$

$$k_{AB} \equiv y_B^{x_A} \equiv a^{x_B^{x_A}} \equiv a^{x_B x_A} \equiv a^{x_A x_B} \equiv a^{x_A^{x_B}} \equiv y_A^{x_B} \equiv k_{BA} \pmod{p}$$

Schlüsselaustauschprotokoll nach Diffie-Hellman: Beispiel

Alice

- empfange $a = 6$, $p = 11$ und $y_B = 7$ von Bob.
- wähle $x_A = 8$ mit $1 \leq x_A \leq \varphi(p)$ *(geheim)*
- berechne $y_A = a^{x_A} \mod p = 6^8 \mod 11 = 4$ *(öffentlich)*
- berechne $k_{AB} = y_B^{x_A} \mod p = 7^8 \mod 11 = 9$

Bob

- wähle Primzahl $p = 11$
- wähle Primitivwurzel $a = 6$ von p
- wähle $x_B = 3$ mit $1 \leq x_B \leq \varphi(p)$ *(geheim)*
- berechne $y_B = a^{x_B} \mod p = 6^3 \mod 11 = 7$ *(öffentlich)*
- empfange $y_A = 4$ von Alice
- berechne $k_{BA} = y_A^{x_B} \mod p = 4^3 \mod 11 = 9$

Verschlüsselungssystem nach Rivest, Shamir, Adleman (RSA)

- **Schlüsselerzeugung**
  - wähle Primzahlen p und q
  - berechne $n = p \cdot q$
  - wähle $e, d \geq 3$, sodass $e \cdot d \equiv 1 \pmod{\varphi(n)}$
    $(\varphi(n) = (p-1) \cdot (q-1)$, falls p und q prim$)$
  - öffentlicher Schlüssel (n, e), privater Schlüssel (n, d)
- **Verschlüsselung** einer Nachricht m
  - $c := m^e \mod n$
- **Entschlüsselung** eines Schlüsseltextes c
  - $m' := c^d \mod n$

Verschlüsselungssystem nach Rivest, Shamir, Adleman (RSA): Beispiel

- **Schlüsselerzeugung**
  - wähle Primzahlen $p = 3$ und $q = 11$
  - berechne $n = p \cdot q = 33$
  - $\varphi(n) = 2 \cdot 10 = 20$
  - wähle $e = 7, d = 3$, sodass $e \cdot d \equiv 1 \pmod{20}$
  - öffentlicher Schlüssel $(33, 7)$, privater Schlüssel $(33, 3)$
- **Verschlüsselung** einer Nachricht $m = 18$
  - c $:= m^e \mod n = 18^7 \mod 33 = 6$
- **Entschlüsselung** eines Schlüsseltextes $c = 6$
  - $m' := c^d \mod n = 6^3 \mod 33 = 18$

Signatursystem nach Rivest, Shamir, Adleman (RSA)

- **Schlüsselerzeugung**
  - wähle Primzahlen p und q
  - berechne $n = p \cdot q$
  - wähle $e, d \geq 3$, sodass $e \cdot d \equiv 1 \pmod{\varphi(n)}$
    $\varphi(n) = (p-1) \cdot (q-1)$, falls p und q prim
  - öffentlicher Schlüssel (n, e), privater Schlüssel (n, d)
- **Signatur** einer Nachricht m
  - s $:= m^d \mod n$
- **Test** einer Signatur s zu einer Nachricht m
  - $m \stackrel{?}{=} s^e \mod n$

Verschlüsselungssystem nach ElGamal

- **Schlüsselerzeugung**
  - wähle Primzahl p, Primitivwurzel a von p
  - wähle privaten Schlüssel k $(k < \varphi(p))$
  - berechne $-k \mod \varphi(p)$
  - öffentlicher Schlüssel $y := a^{-k} \mod p$

$\varphi(p) = p - 1$, falls p prim

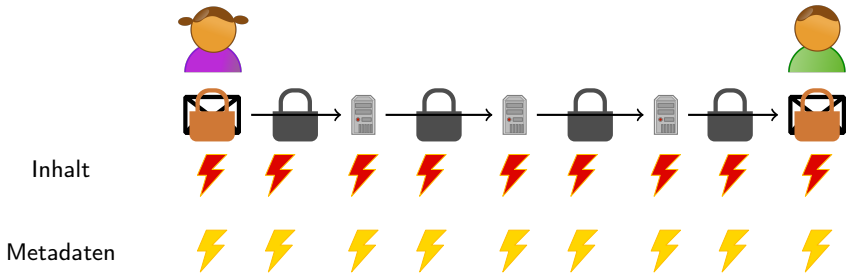
- **Verschlüsselung** einer Nachricht $m < p$
  - wähle Zufallszahl $z < p$
  - berechne $c := y^z \cdot m \mod p$
  - sende Schlüsseltext $(a^z \mod p, c)$
- **Entschlüsselung** eines Schlüsseltextes $(a^z \mod p, c)$
  - $m' := (a^z)^k \cdot c \mod p$

$$m' \equiv (a^z)^k \cdot c \equiv (a^z)^k \cdot y^z \cdot m \equiv a^{zk} \cdot (a^{-k})^z \cdot m \equiv a^{zk-zk} \cdot m \equiv m \pmod{p}$$

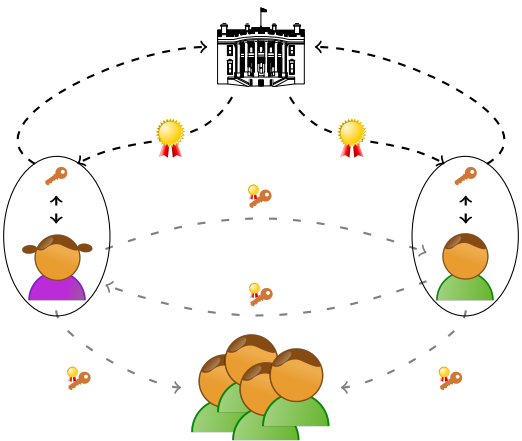
Verschlüsselungssystem nach ElGamal: Beispiel

- **Schlüsselerzeugung**
  - wähle Primzahl $p = 11$, Primitivwurzel $a = 6$ von p
  - wähle privaten Schlüssel $k = 4$ $(k < \varphi(p))$
  - berechne $-k \equiv -4 \equiv 6 \pmod{\varphi(p)}$
  - öffentlicher Schlüssel $y := a^{-k} \mod p = 6^6 \mod 11 = 5$
- **Verschlüsselung** einer Nachricht $m = 4$
  - wähle Zufallszahl $z = 9$
  - berechne $c := y^z \cdot m \mod p = 5^9 \cdot 4 \mod 11 = 3$
  - sende Schlüsseltext $(a^z \mod p, c) = (2, 3)$
- **Entschlüsselung** eines Schlüsseltextes $(a^z \mod p, c) = (2, 3)$
  - $m' := (a^z)^k \cdot c \mod p = 2^4 \cdot 3 \mod 11 = 4$

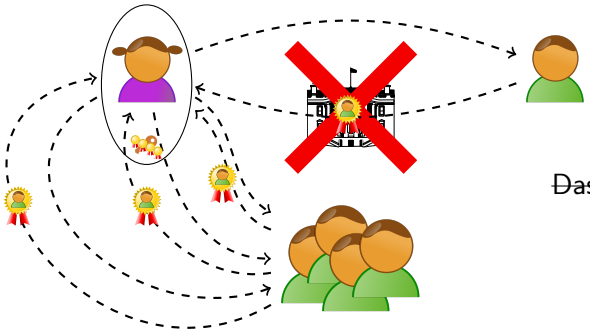
Ende-zu-Ende- und Transportverschlüsselung



Hierarchische Zertifizierung (z. B. S/MIME)



Web of Trust (z. B. PGP)



~~Das machen wir heute!~~

Exkurs: SMTP

Live-Demo

- Wie sendet man eine E-Mail über SMTP?

Thunderbird-Konfiguration

Live-Hacking (gemeinsam)

- Wie nutzt man PGP in Thunderbird?
- Wie nutzt man S/MIME in Thunderbird?

Was man heute mitnehmen konnte

- Was ist informationelle Selbstbestimmung und wieso ist diese wichtig?
- Welche Schutzziele existieren und wie können diese erreicht werden?
- Was sind die grundlegenden Konzepte der Kryptographie?
- Wie funktioniert der Versand von E-Mails über SMTP?
- Wie kann ich meine E-Mails verschlüsselt und digital signiert versenden?