PGP – warum, was und wie?

- Ziele: unsere und die der Bullen
- Knappe Theorie
- Verschlüsseln
- Signaturen
- Das Web of Trust
- Praktikalitäten
- Praxis

Warum PGP?

Auswertung von E-Mails ist ein Routineverfahren bei Polizei und Geheimdiensten.

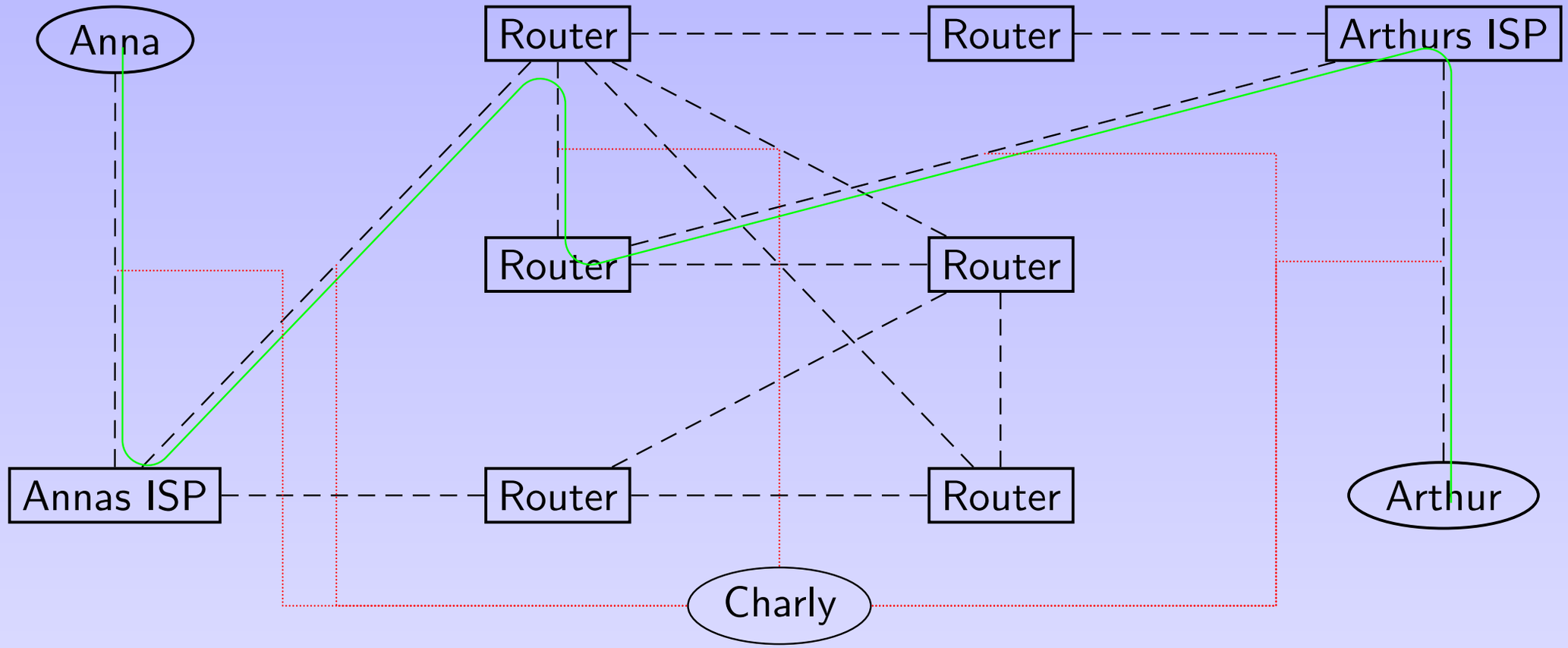
Viele Wege führen zur Mail.

PGP ist ein offener, interoperabler Standard.

PGP ist relativ einfach verständliche Krypto.

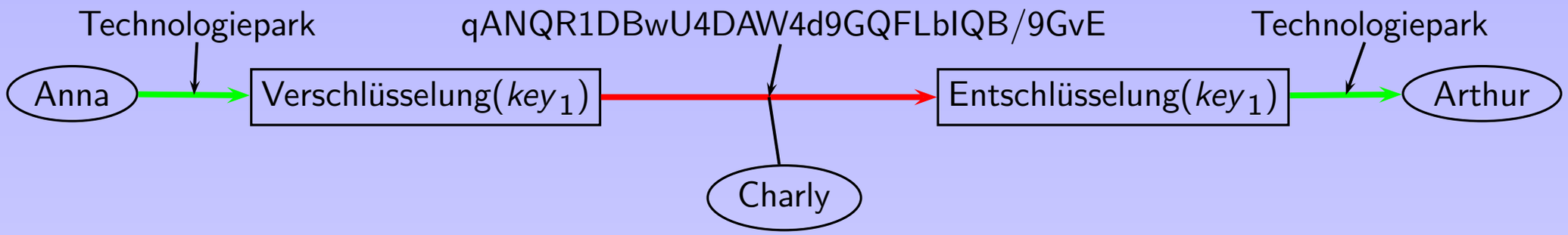
Mails verschlüsseln ist praktische Solidarität.

Wo wird Netzverkehr abgehört?



„Bedarfsträger“ haben an fast jeder Stelle Zugriff auf im Netz transportierte Daten.

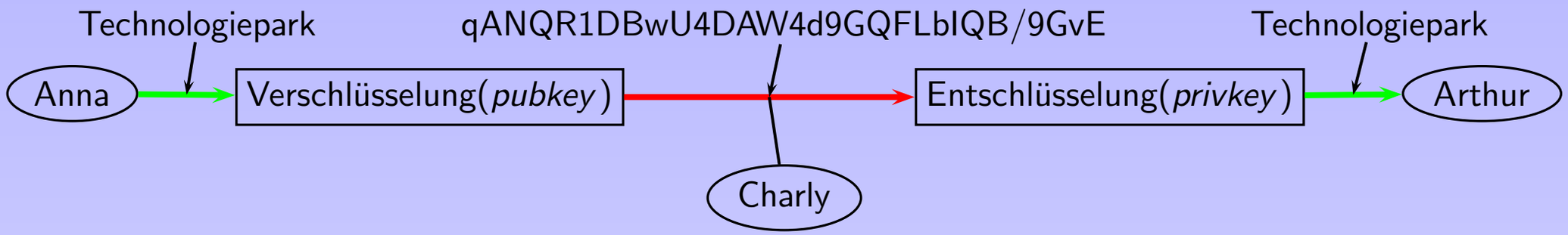
Symmetrische Verschlüsselung



Probleme:

1. Übermittlung des Schlüssels
2. Wer verschlüsseln kann, kann auch entschlüsseln
3. Gute Wahl der Verschlüsselungsfunktion
4. Sicherheit der Leitungen zwischen Anna und der Verschlüsselung bzw. zwischen der Entschlüsselung und Arthur

Asymmetrische Verschlüsselung



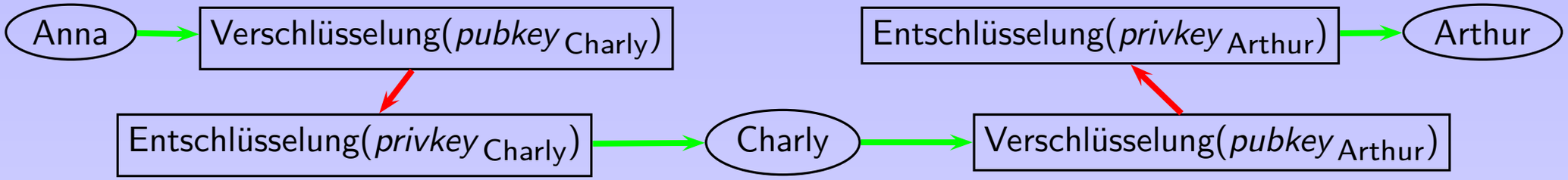
(Gute) Metapher: Briefkästen

Probleme:

1. Sicherheit des Schlüssels
2. Sicherheit bis zum Verschlüsseln („Staatstrojaner“)
3. „Vertauschen der Namenschilder“

Man in the middle

Wenn Charly Anna vortäuscht, Arthur zu sein und umgekehrt Arthur, er, Charly, sei Anna, kann Charly mitlesen:



Man-in-the-middle attack

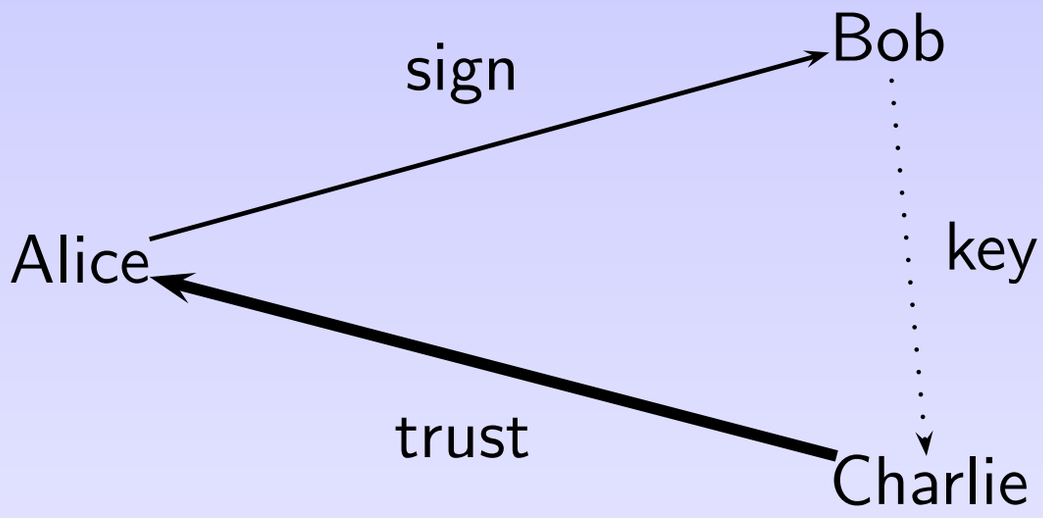
Krypto ohne Schlüsselverifikation stinkt.

- In euren Browsern sind die öffentlichen Schlüssel von Firmen (z.B. verisign) enthalten.
- In den neuen Personalausweisen sind Schlüssel, die vom Innenministerium unterschrieben werden.

Das Web of Trust

- Leute signieren die öffentlichen Schlüssel anderer Leute und bestätigen damit ihre Authentizität
- Leute vertrauen anderen Leuten, dass diese wirklich nur das signieren, was sie geprüft haben

Hier kann Charlie Bobs Schlüssel vertrauen, weil er Alices Unterschrift trägt und Charlie Alice vertraut.



Für die RH

Zentrales Problem des WoT: Die Unterschriften müssen öffentlich sein, und damit kann jedeR einen sozialen Graph malen („wer hat mit wem zu tun?“).

In der RH deshalb: Es gibt (derzeit) einen Schlüssel, der alle Organisations-Schlüssel unterschreibt. Also:

1. Ihr holt den Fingerprint des Datenschutzgruppen-Schlüssels aus der RHZ.
2. Ihr holt den Schlüssel von datenschutzgruppe@rote-hilfe.de vom Keyserver.
3. Ihr verifiziert den Schlüssel und stellt *danach* das Vertrauen auf dem Schlüssel auf „voll“.

Schlüsselwechsel

Manchmal will mensch einen neuen Schlüssel haben:

- Leute, die den Schlüssel haben, werden unheimlich
- Mensch will einen längeren Schlüssel
- Mensch will beschränken, wie viel verschlüsseltes Material es zu einem Schlüssel gibt

Wenn Leute ständig Schlüssel wechseln und die anderen die einfach importieren, haben MITM leichtes Spiel.

Deshalb: Macht ein Transition Statement und schickt es an alle@.

Näheres: http://datenschmutz/gc/html/sicherumziehen.html.

PGP/MIME

Noch eine wichtige Kleinigkeit:

In den alten Zeiten gab es keine Anhänge und keine deutschen Sonderzeichen.

Heute gibts das, und es funktioniert nicht gescheit, wenn ihr nicht PGP/MIME auswählt. Alte Enigmails haben das eher schwer gemacht.

Heute: (Rechtsklick auf Mailbox) $\rightarrow$ *Properties*, *OpenPGP Security*, *Use PGP/MIME by default*.

Zum Ende

https://www.datenschmutz.de