Informatik Kursstufe

Datensicherheit und
Informationsgesellschaft

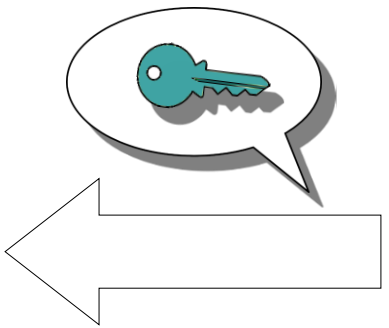
Kryptologie

Asymmetrische Verschlüsselung

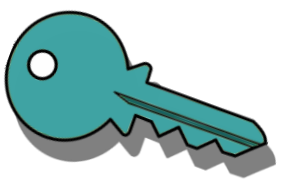
Steidlinger, Walliser

Symmetrische Verschlüsselung

Agatha

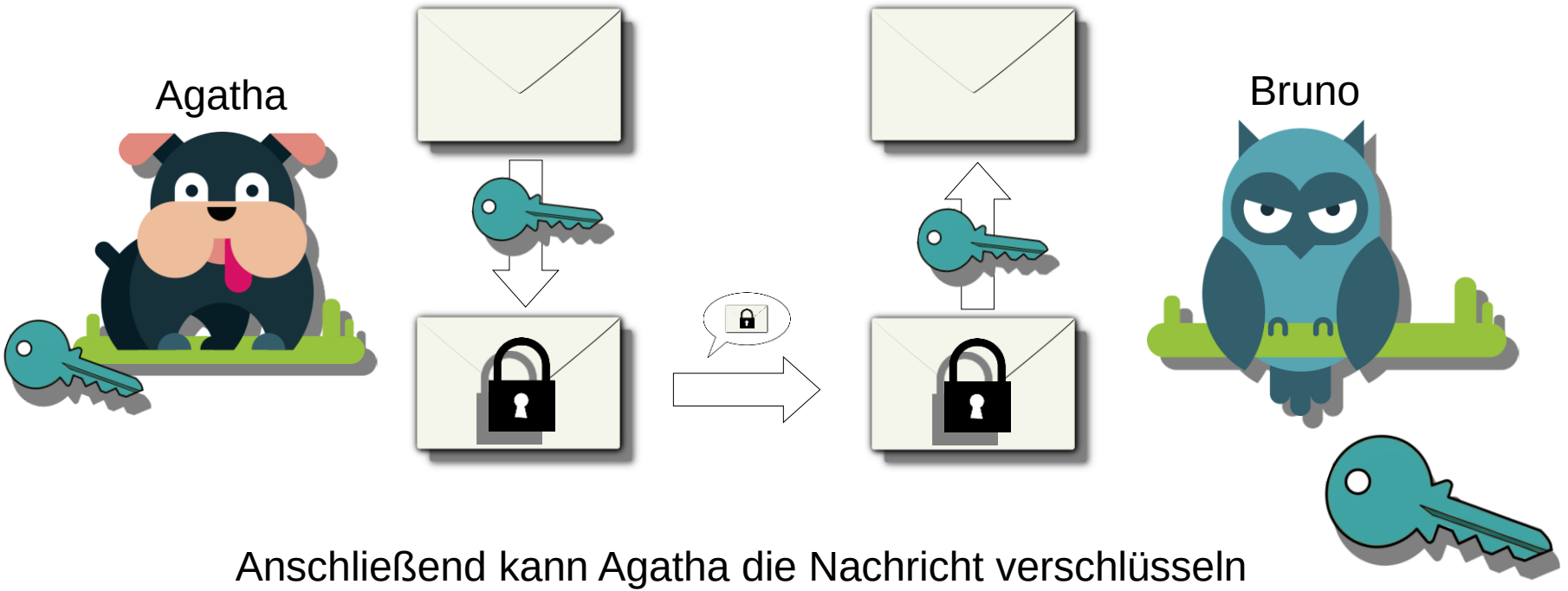


Bruno



Agatha möchte Bruno eine geheime Nachricht schicken.
Dafür muss Bruno zuerst einen Schlüssel zu Agatha schicken.

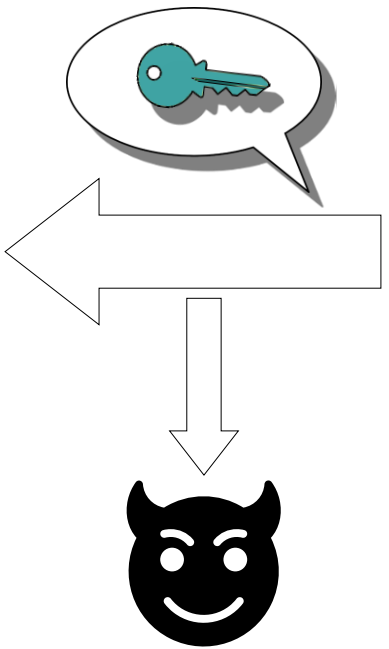
Symmetrische Verschlüsselung



Anschließend kann Agatha die Nachricht verschlüsseln (siehe Caesar, Vigenère) und versenden.

Symmetrische Verschlüsselung

Agatha

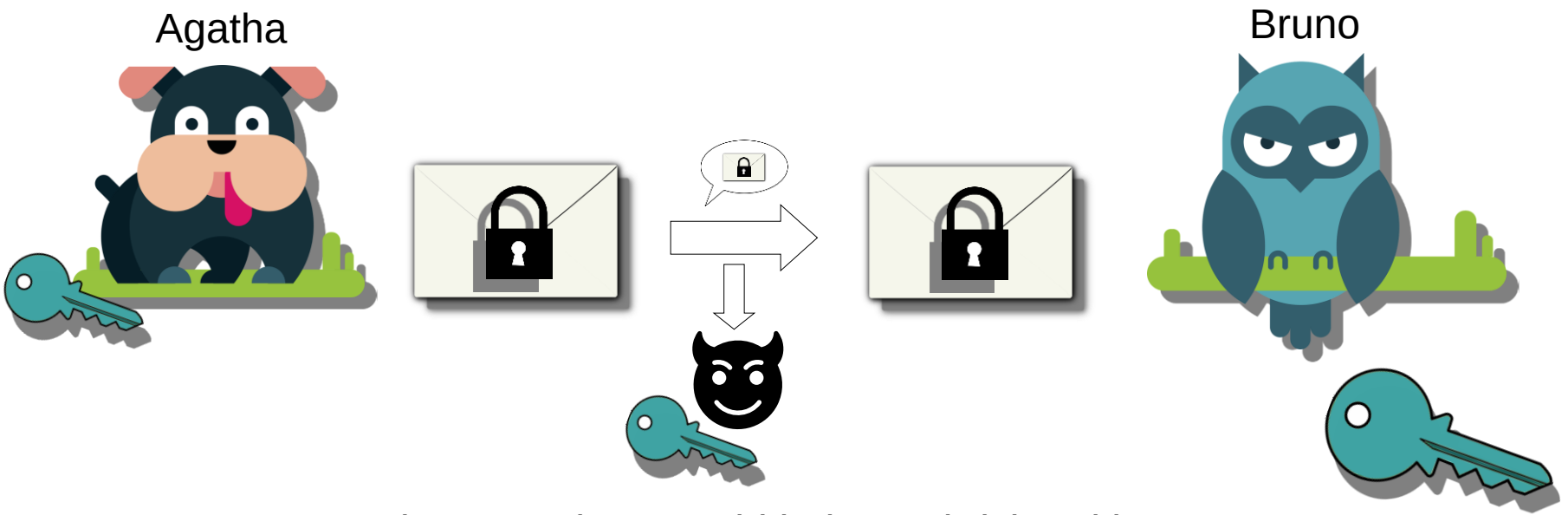


Bruno

Hacker Harald schafft es, die Schlüsselübergabe abzuhören.

Hacker Harald

Symmetrische Verschlüsselung



Jetzt kann Hacker Harald jede Nachricht mitlesen,
da auch er nun den Schlüssel besitzt.

Das Schlüsseltausch-Problem

Es ist kaum möglich, eine vollständig sichere Schlüsselübergabe durchzuführen.

⇨ Ein **einziger** Schlüssel für Ver- und Entschlüsselung ist nicht sicher!

Schlüsselpaar

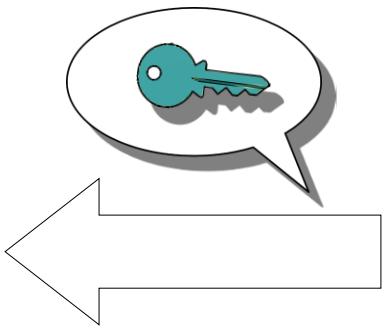
Rein hypothetische Überlegung: Wenn wir die Nachricht doch nur mit zwei verschiedenen Schlüsseln ver- und entschlüsseln könnten…

- Dann wäre das Schlüsseltausch-Problem gelöst.
- Dann wäre die Verschlüsselung trotzdem sicher, solange kein anderer Schlüssel zur Entschlüsselung verwendet werden kann.

– **Wie könnte das funktionieren?**

Geheime und öffentliche Schlüssel

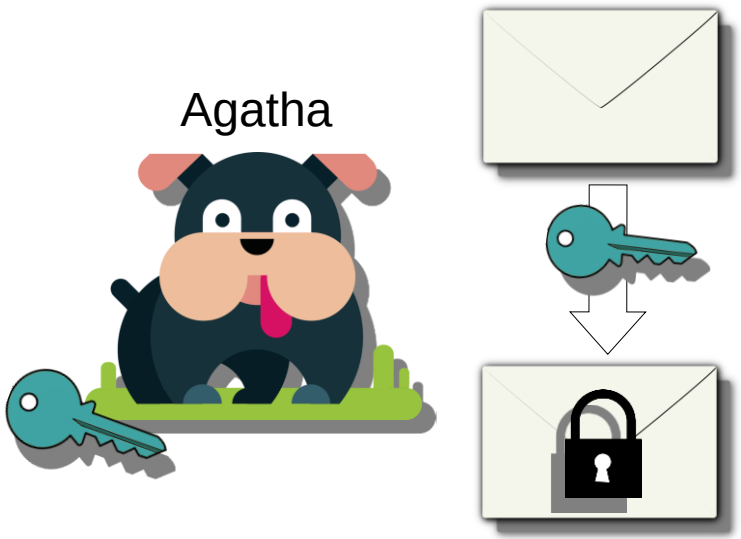
Agatha



Bruno

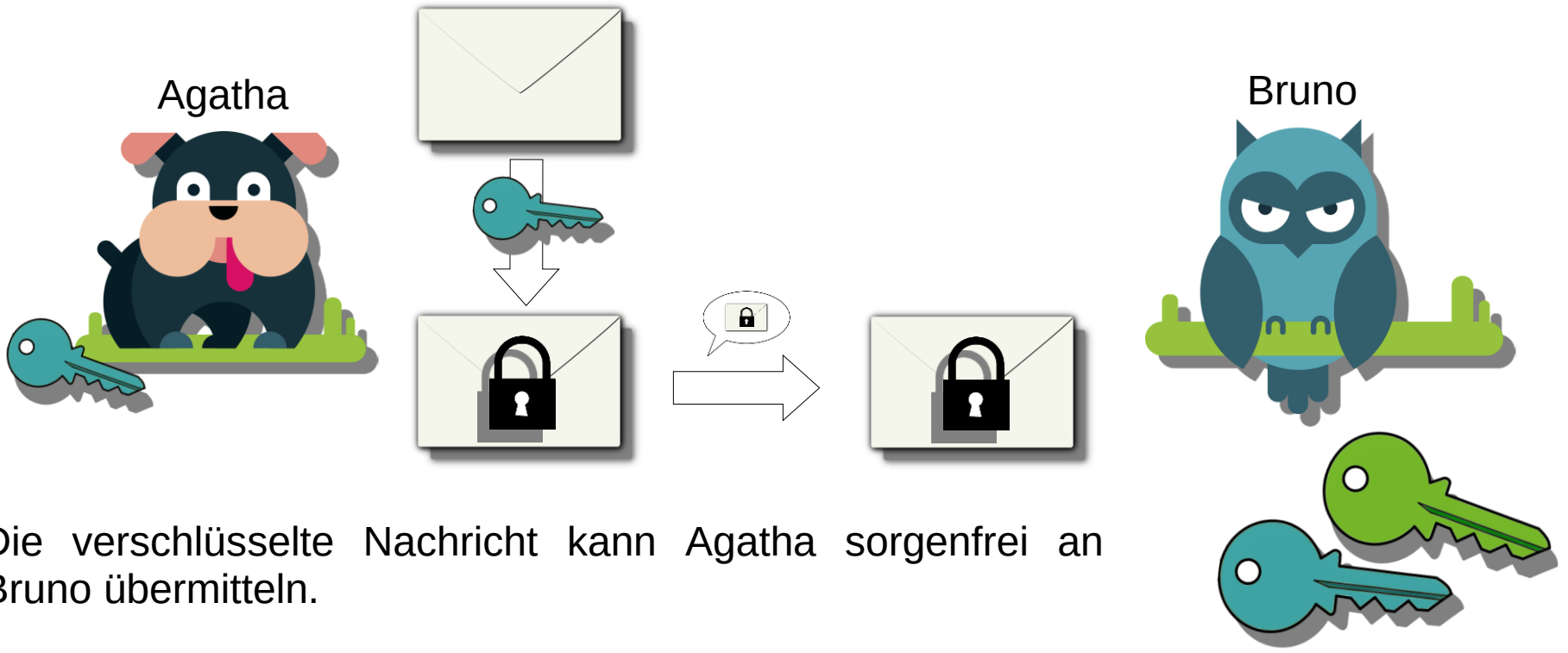
Bruno besitzt zwei Schlüssel.
Einen dieser Schlüssel teilt Bruno mit der Öffentlichkeit und damit auch mit Agatha.
Der zweite Schlüssel bleibt geheim!

Geheime und öffentliche Schlüssel



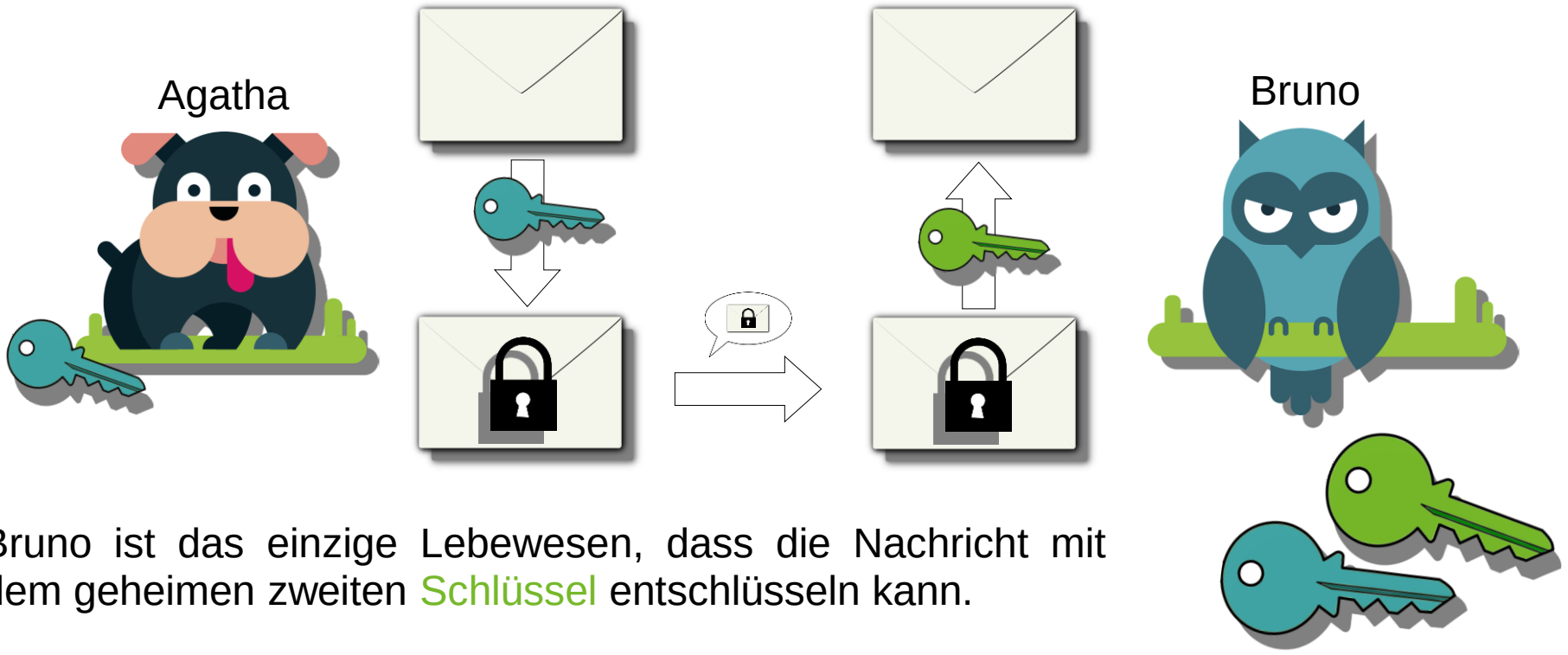
Mit Brunos öffentlichem Schlüssel kann Agatha Nachrichten für Bruno verschlüsseln, aber nicht mehr entschlüsseln.

Geheime und öffentliche Schlüssel



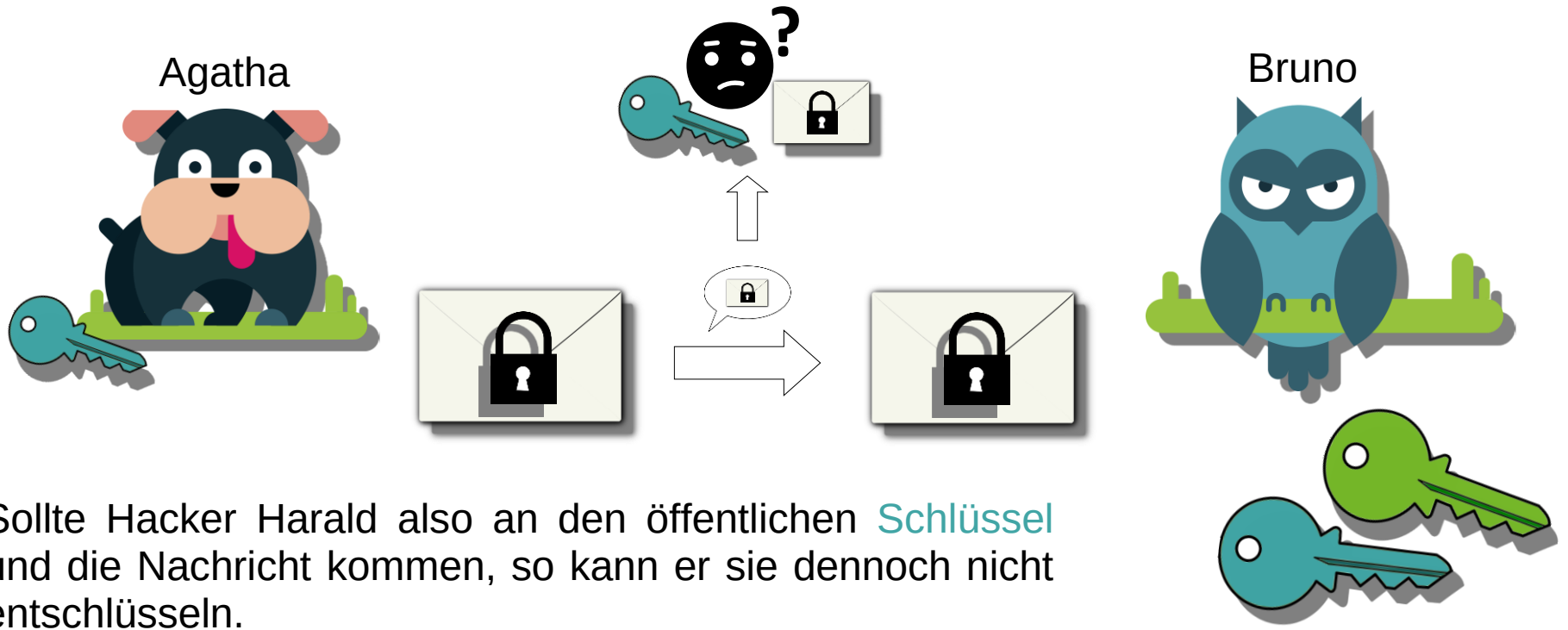
Die verschlüsselte Nachricht kann Agatha sorgenfrei an Bruno übermitteln.

Geheime und öffentliche Schlüssel



Bruno ist das einzige Lebewesen, dass die Nachricht mit dem geheimen zweiten Schlüssel entschlüsseln kann.

Geheime und öffentliche Schlüssel



Sollte Hacker Harald also an den öffentlichen Schlüssel und die Nachricht kommen, so kann er sie dennoch nicht entschlüsseln.

Schlüsselpaar?

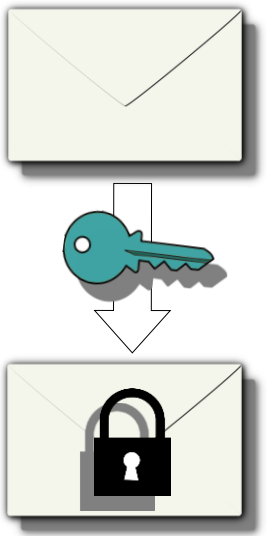
Wegen der Verschlüsselung mit einem öffentlichen Schlüssel, nennt man ein solches Verfahren „*Public-Key-Encryption*“

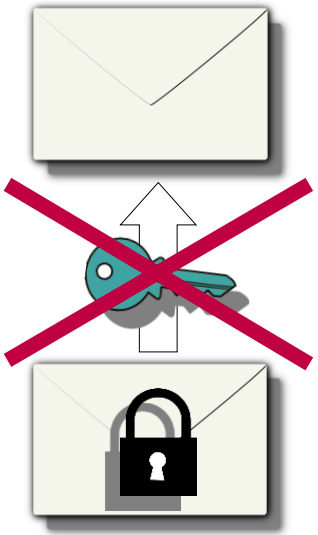
Weil für Ver- und Entschlüsselung unterschiedliche Schlüssel verwendet werden, spricht man auch von „*Asymmetrischer Verschlüsselung*“.

ABER: Gibt es überhaupt solche Schlüsselpaare?

Der öffentliche Schlüssel

Wir betrachten den öffentlichen Schlüssel genauer:
Wir brauchen einen Schlüssel, der verschlüsseln, aber nicht entschlüsseln kann.





Gibt’s sowas?!

AB
Einwegfunktionen und Primzahlen

Steidlinger, Walliser

Einwegfunktionen

Aufgabe 1: Einwegfunktionen im Alltag

...

Aufgabe 2 Produkte und ihre Faktoren

a) $19 \cdot 23 = 437$

b) $91 = 7 \cdot 13$

c) Durchprobieren? Dauert sehr lange! (Lösung: $3397 = 43 \cdot 79$)

d) Bei der Multiplikation zweier Primzahlen könnte es sich um eine Einwegfunktion handeln, da die Multiplikation schnell berechenbar ist, aber die Umkehrung (also die Faktorisierung) nicht.

Primfaktorzerwas?

„Bis heute ist kein Faktorisierungsverfahren bekannt, das nichttriviale Teiler und damit die Primfaktorzerlegung einer Zahl effizient berechnet! Das bedeutet, dass ein enormer Rechenaufwand notwendig ist, um eine Zahl mit mehreren hundert Stellen zu faktorisieren. Diese Schwierigkeit wird in der Kryptografie ausgenutzt“

(Wikipedia)

Mathematische Grundlagen

Aufgabe 3: Wie war das nochmal?

a) ggT(5, 15) = 5

b) ggT(36, 56) = 8

c) ggT(43, 71) = 1

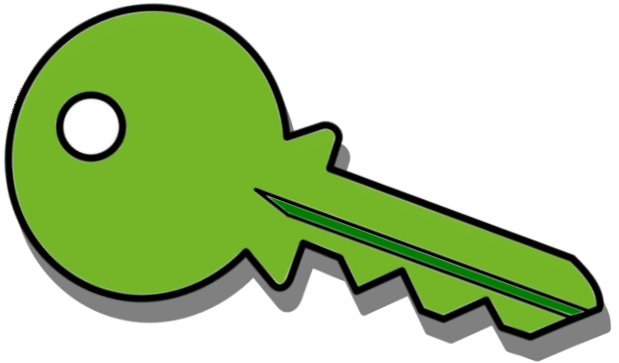
→ ggT(a,b) gibt den größten gemeinsamen Teiler der Zahlen a und b an.
Zwei verschiedene Zahlen a und b heißen teilerfremd, wenn sie nur „1“ als gemeinsamen Teiler haben.
→ Zwei verschiedene Primzahlen sind also immer teilerfremd!

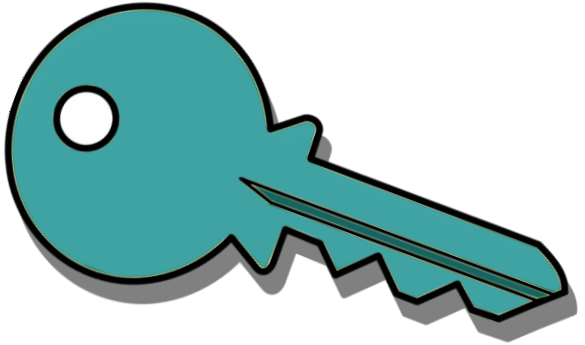
d) 53 mod 7 = 4

e) 121 mod 11 = 0

f) 4^3 mod 17 = 13

→ Der Modulo-Operator gibt den Rest einer Division zurück.





Das
RSA -Verfahren

(Rivest-Shamir-Adleman, 1983)

Steidlinger, Walliser

Berechnung der Schlüssel

1

- Wähle zwei Primzahlen p und q
- Berechne: n = p * q

Beispiel:

- Wähle p = 3 und q = 41
- Berechne: n = 3 * 41 = 123

Öffentlicher Schlüssel: (n, e)

Privater Schlüssel: (n, d)

Steidlinger, Walliser

Berechnung der Schlüssel

1
- Wähle zwei Primzahlen p und q
- Berechne: n = p * q

2
- Eulersche-φ-Funktion:
- Berechne: $\varphi(n)$ = (p - 1) * (q - 1)

Beispiel:
- Wähle p = 3 und q = 41
- Berechne: n = 3 * 41 = 123

- Eulersche-φ-Funktion:
- Berechne: $\varphi(n)$ = (3 - 1) * (41 - 1) = 80

Öffentlicher Schlüssel: (n, e)

Privater Schlüssel: (n, d)

Berechnung der Schlüssel

		Beispiel:
1	• Wähle zwei Primzahlen p und q • Berechne: n = p * q	• Wähle p = 3 und q = 41 • Berechne: n = 3 * 41 = 123
2	• Eulersche-φ-Funktion: • Berechne: $\varphi(n)$ = (p - 1) * (q - 1)	• Eulersche-φ-Funktion: • Berechne: $\varphi(n)$ = (3 - 1) * (41 - 1) = 80
3	• Suche natürliche Zahl e, die zu $\varphi(n)$ teilerfremd ist: • $ggT(e, \varphi(n))$ = 1	• Suche natürliche Zahl e, die zu $\varphi(n)$ teilerfremd ist: • $ggT(3, 80)$ = 1 => Wähle e = 3

Öffentlicher Schlüssel: (n, e)

Privater Schlüssel: (n, d)

Berechnung der Schlüssel

Beispiel:

1. • Wähle zwei Primzahlen p und q
   • Berechne: n = p * q

   • Wähle p = 3 und q = 41
   • Berechne: n = 3 * 41 = 123

2. • Eulersche-φ-Funktion:
   • Berechne: $\varphi(n)$ = (p - 1) * (q - 1)

   • Eulersche-φ-Funktion:
   • Berechne: $\varphi(n)$ = (3 - 1) * (41 - 1) = 80

3. • Suche natürliche Zahl e, die zu $\varphi(n)$ teilerfremd ist:
   • $ggT(e, \varphi(n))$ = 1

   • Suche natürliche Zahl e, die zu $\varphi(n)$ teilerfremd ist:
   • $ggT(3, 80)$ = 1 => Wähle e = 3

4. • Bestimme ganze Zahl d, sodass:
   • $d * e \ mod \ \varphi(n) = 1$

   • Berechne ganze Zahl d:
   • d = 27: 27 * 3 mod 80 = 1

Öffentlicher Schlüssel: (n, e)

Privater Schlüssel: (n, d)

Öffentlicher Schlüssel: (123, 3)

Privater Schlüssel: (123, 27)

Verschlüsseln / Entschlüsseln

Zerlege deine Nachricht in Stücke und schreibe ein Stück als Zahl m mit:

$$0 \leq m \leq n - 1$$

Beispiel:

- Wir möchten die Nachricht „s“ verschicken:
- ASCII: s = 115 mit $0 \leq 115 \leq n = 123$

Öffentlicher Schlüssel: (n, e)

Privater Schlüssel: (n, d)

Öffentlicher Schlüssel: (123, 3)

Privater Schlüssel: (123, 27)

Verschlüsseln / Entschlüsseln

Zerlege deine Nachricht in Stücke und schreibe ein Stück als Zahl m mit:

$$0 \leq m \leq n - 1$$

Verschlüsseln einer Nachricht m :

$$c = m^e \; mod \; n$$

Beispiel:

- Wir möchten die Nachricht „s“ verschicken:
- ASCII: s = 115 mit $0 \leq 115 \leq n = 123$

- Öffentlicher Schlüssel: (123, 3)
- Nachricht m = 115:

$$c = 115^3 \; mod \; 123 = 103$$

Öffentlicher Schlüssel: (n, e)

Privater Schlüssel: (n, d)

Öffentlicher Schlüssel: (123, 3)

Privater Schlüssel: (123, 27)

Verschlüsseln / Entschlüsseln

Zerlege deine Nachricht in Stücke und schreibe ein Stück als Zahl m mit:

$$0 \leq m \leq n - 1$$

Verschlüsseln einer Nachricht m :

$$c = m^e \; mod \; n$$

Entschlüsseln der Nachricht c :

$$m = c^d \; mod \; n$$

Beispiel:

- Wir möchten die Nachricht „s“ verschicken:
- ASCII: s = 115 mit $0 \leq 115 \leq n = 123$

- Öffentlicher Schlüssel: (123, 3)
- Nachricht m = 115:

$$c = 115^3 \; mod \; 123 = 103$$

- Privater Schlüssel: (27)
- Nachricht c = 64:

$$m = 103^{27} \; mod \; 123 = 115$$

Öffentlicher Schlüssel: (n, e)

Privater Schlüssel: (n, d)

Öffentlicher Schlüssel: (123, 3)

Privater Schlüssel: (123, 27)

H5P Übungen zum RSA-Verfahren

Steidlinger, Walliser

Übungen zum RSA-Verfahren mit dem RSA-Tool

Steidlinger, Walliser

RSA - Tool

<u>Aufgaben RSA-Tool:</u>

1) …

2) „E“ entspricht in ASCII: 69 → c1 = 69^3 mod 123 = 99
„i“ entspricht in ASCII: 105 → c2 = 105^3 mod 123 = 72
„s“ entspricht in ASCII: 115 → c3 = 115^3 mod 123 = 103

Verschlüsselte Nachricht: (99, 72, 103)
(oder mit ASCII als Buchstaben dargestellt: (c, H, g))

3) …

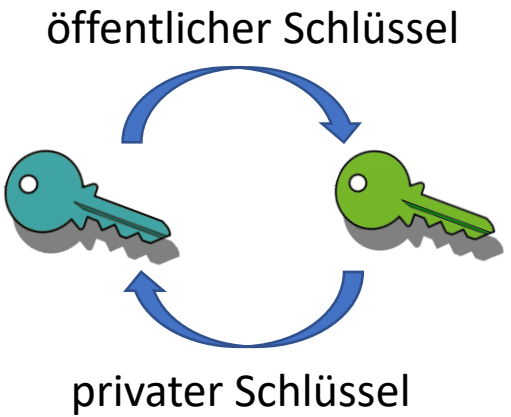
Fazit

Vorteile symmetrischer Verschlüsselung	Vorteile asymmetrischer Verschlüsselung
- Niedrige Rechenzeit - Einfache Algorithmen	- Hohe Sicherheit - Digitale Signaturen
Nachteile symmetrischer Verschlüsselung	**Nachteile asymmetrischer Verschlüsselung**
- Schlüsselübergabe ist sehr unsicher - Jeder Teilnehmer muss für jeden seiner Kontakte einen Schlüssel anfertigen, was bei vielen Kontakten **sehr** viele Schlüssel erfordert Beispiel: 1000 Teilnehmer => 499 500 Schlüssel	- Hohe Rechenzeit: c.a. 1000 Mal langsamer - Komplexere Algorithmen, mehr Aufwand - Die Sicherheit ist nicht bewiesen. Es könnte eine einfache Lösung für Einwegfunktionen geben!

Die Erfindung des RSA-Verfahrens war ein Meilenstein der Verschlüsselung!

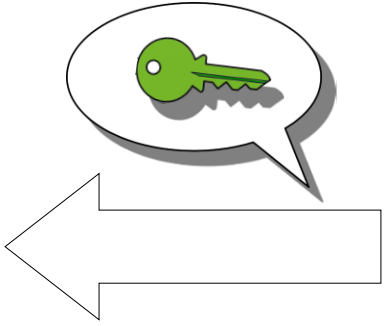
Digitale Signatur

Wie könnten wir sicherstellen, dass ein signiertes Dokument (z.B. ein Vertrag) nicht gefälscht werden kann?
Wir vertauschen einfach die Rollen der beiden Schlüssel!



Digitale Signatur

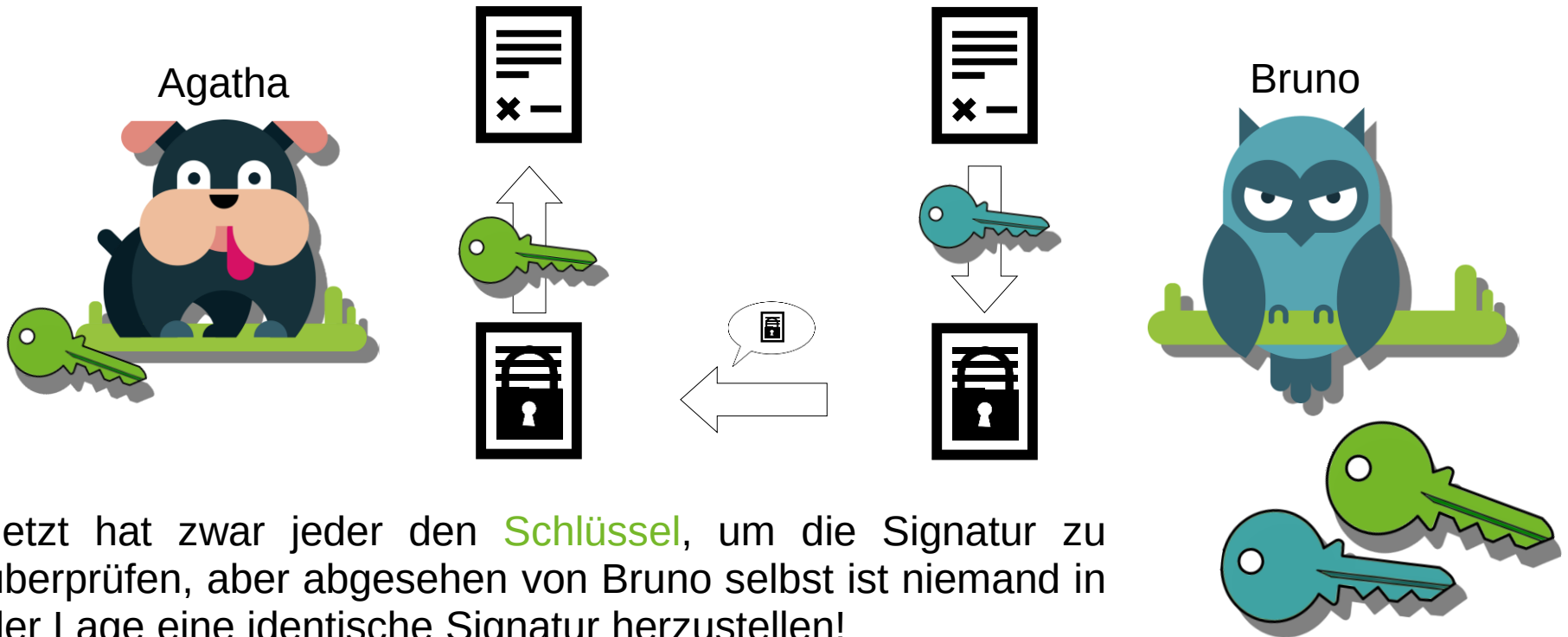
Agatha



Bruno

Nun teilen wir den Schlüssel zum Entschlüsseln mit der Öffentlichkeit.
Der Schlüssel zum Verschlüsseln bleibt geheim!

Digitale Signatur



Jetzt hat zwar jeder den Schlüssel, um die Signatur zu überprüfen, aber abgesehen von Bruno selbst ist niemand in der Lage eine identische Signatur herzustellen!