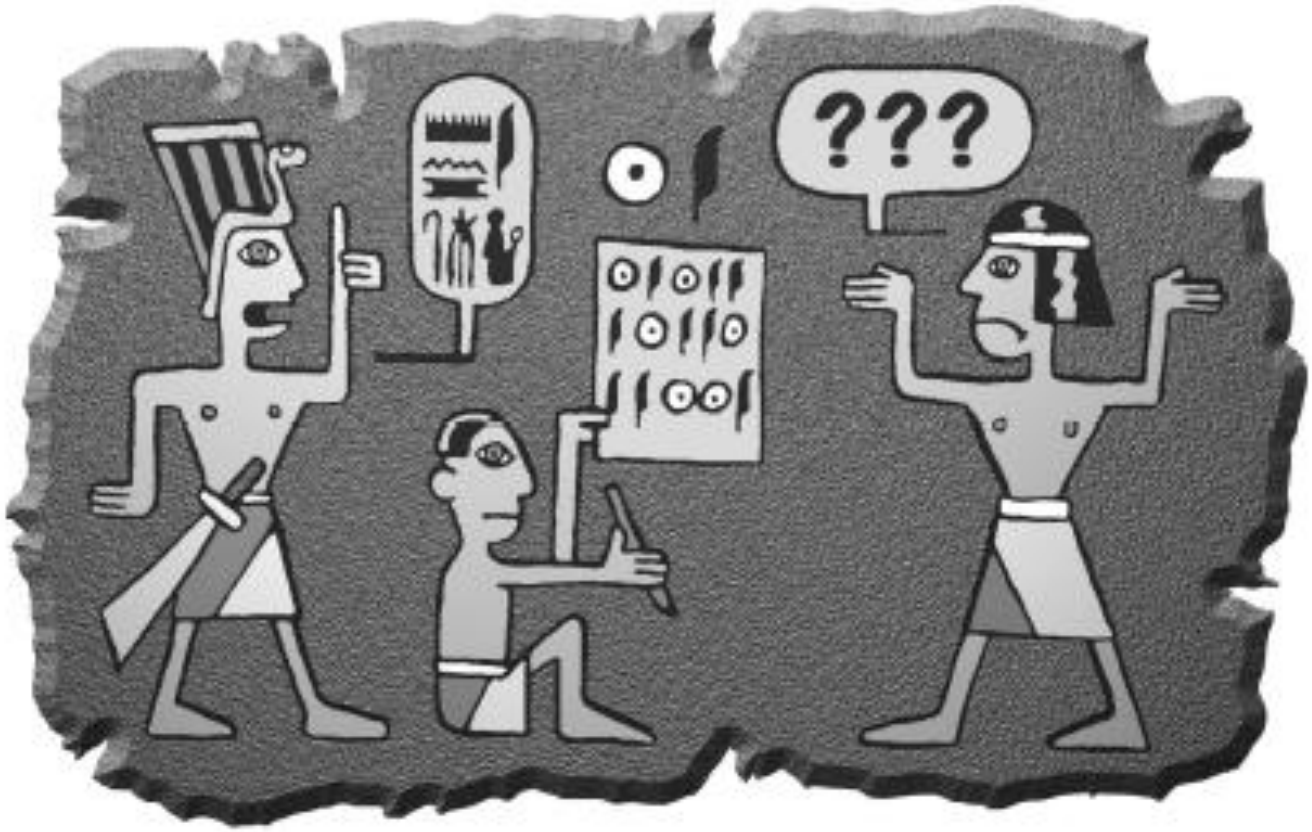
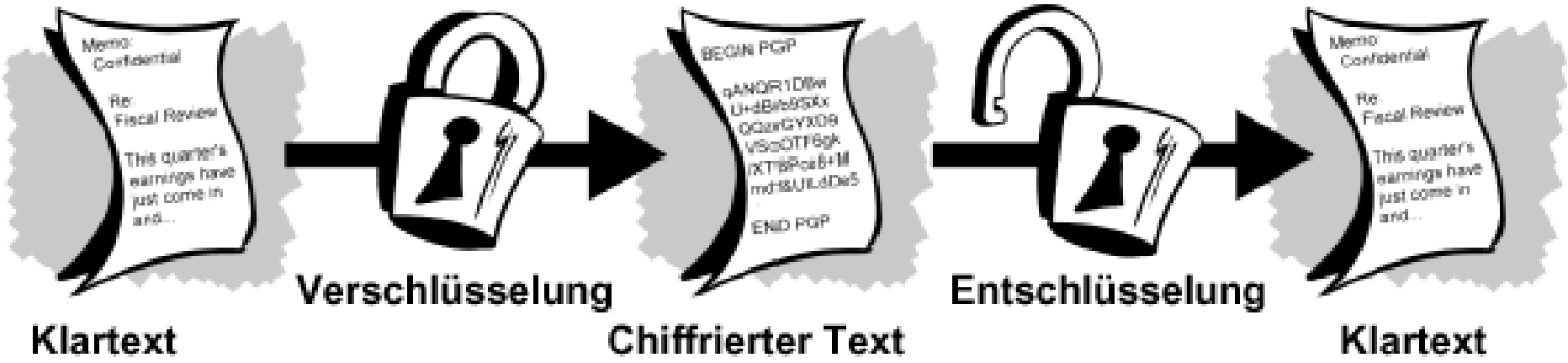
Verschlüsselung

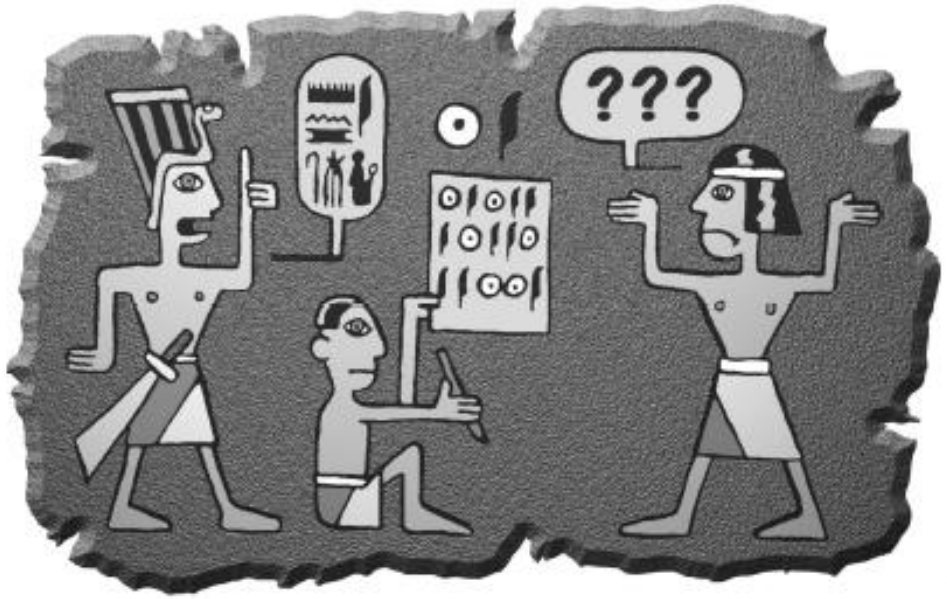


Nur eine Handvoll Menschen braucht es angeblich als Vermittler, um jeden Erdenbürger mit einem beliebigen anderen bekannt zu machen: Beispielsweise könnte die Tochter Ihres Metzgers mit einem Bekannten der Cousine des Friseurs Ihres zuständigen Finanzbeamten am selben Fließband arbeiten. Würden Sie dieser `Menschenkette´ Ihre Steuererklärung anvertrauen? In einer Klarsichthülle als Umschlag? Wohl nicht.

Nicht viel anders funktioniert das Internet: Ihr Provider ist mit irgendwem verbunden, der eine Leitung zu einem Rechner hat ... Wer auch immer - mehr oder weniger zufällig - an einem Knotenpunkt zwischen Absender und Empfänger einer EMail sitzt, kann Nachrichten abfangen, mitlesen oder verändern.

Quelle: c't 12/99, S. 212





Quelle: IntroToCrypto.pdf aus dem PGP-SW-Paket
www.gnupp.org -> durchblicker1.1.pdf

Verschlüsselung !

Ein „Schlüssel“ ist eine Zeichenfolge, die verwendet wird, um andere Zeichenfolgen zu verfälschen (zu verschlüsseln).

z.B.: fg+5svbRf4&lO+*0Rdf35EDcbt628/hjzt%rdfE

Hierfür muss eine Verknüpfungsoperation zwischen den Zeichenfolgen definiert werden.

a	1
b	2
c	3
d	4
e	5
f	6
g	7
h	8
i	9
j	10
k	11
l	12
m	13
n	14
o	15
p	16
q	17
r	18
s	19
t	20
u	21
v	22
w	23
x	24
y	25
z	26

Information: Fachbereich Seefahrt
= 6 1 3 8 2 5 18 5 9 3 8 19 5 5 6 1 8 18 20

Operation: +

Schlüssel: 7

Ergebnis: 13 8 10 15 9 12 25 12 16 10 15 26 12 12 13 8 15 25 1
= mhjoilylpjozllmhoya

Wer den Schlüssel hat und die Operation kennt, kann die verschlüsselte Information wieder entschlüsseln :

m -> 13 -> 6 -> f
h -> 8 -> 1 -> a
... usw.

Wer den Schlüssel hat und die Operation kennt, kann die verschlüsselte Information wieder entschlüsseln.

Also:

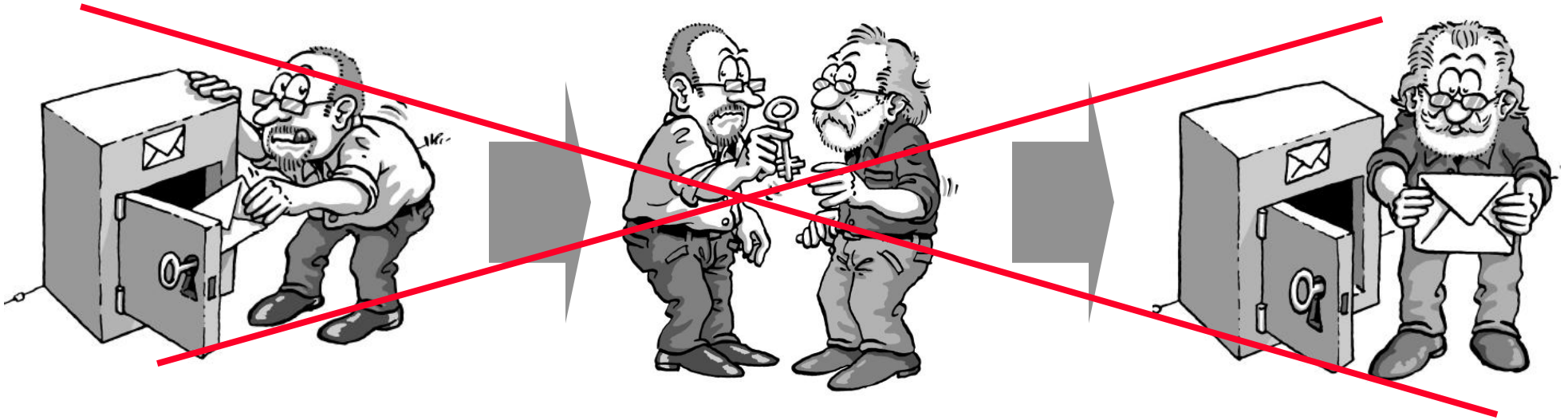
(1) komplizierte Operationen

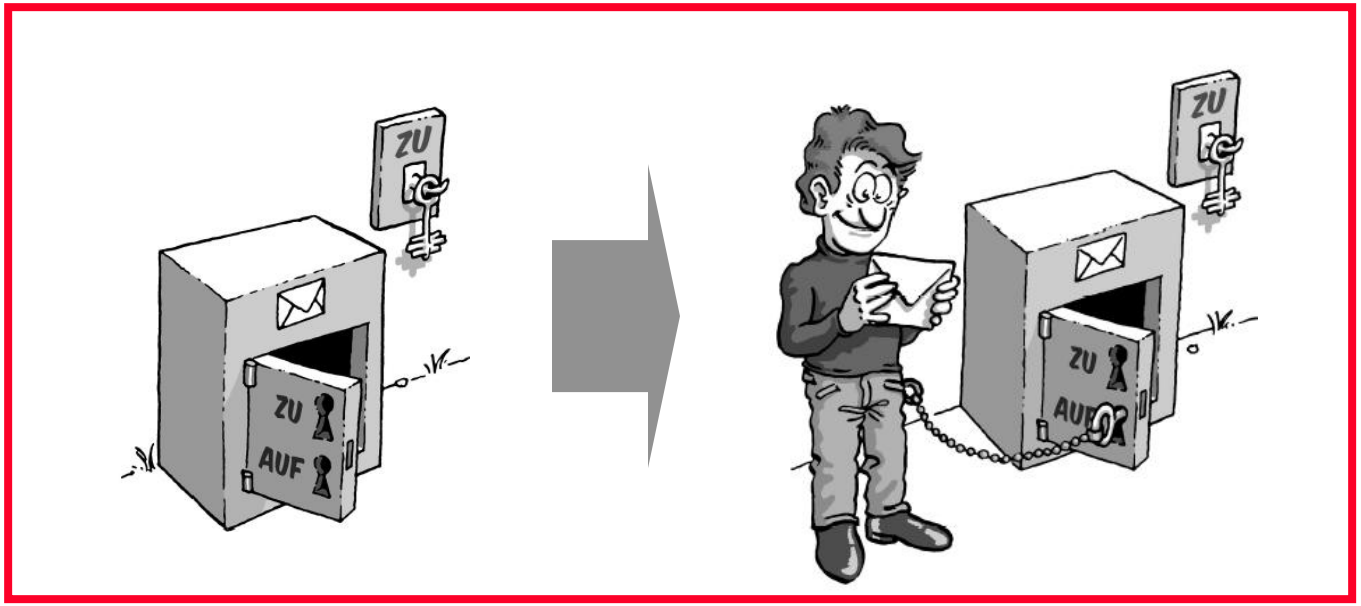
(2) geheimer Schlüsselaustausch (über einen „sicheren Kanal“, z.B. mündlich, Diskette)

Das ist das Problem !

-> Sichere Übermittlung eines Schlüssels über einen unsicheren Kommunikationskanal !!

Das public key Verfahren im Überblick

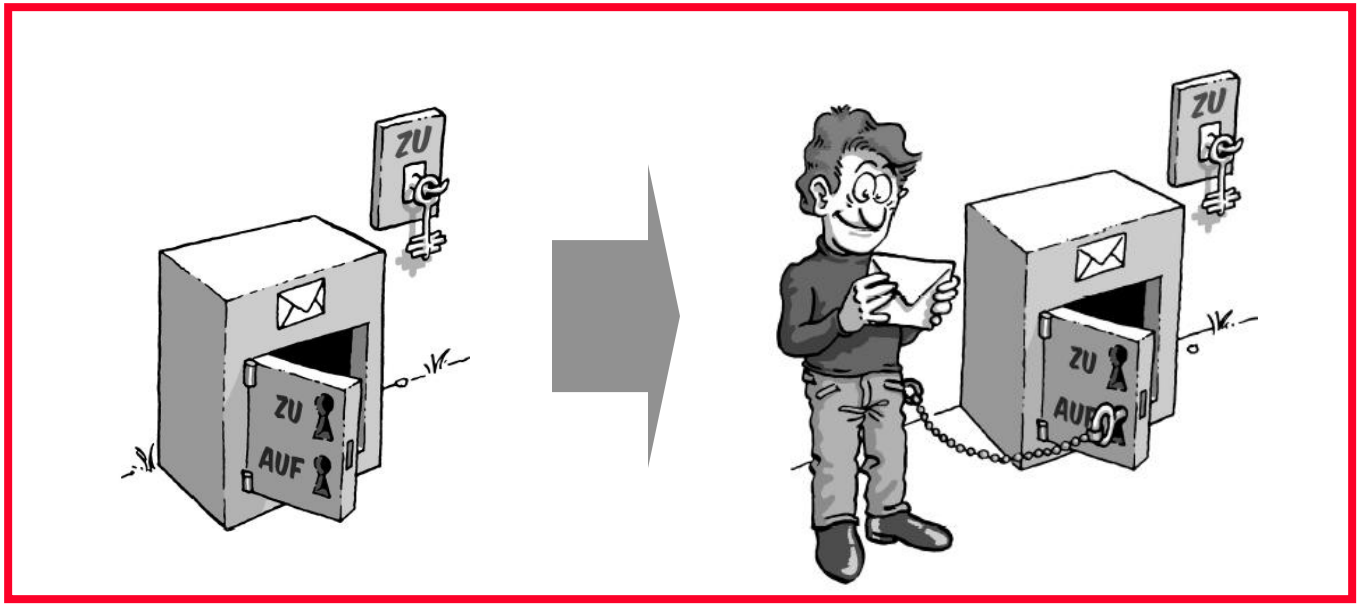




Quelle: www.gnupp.org -> durchblicker1.1.pdf

public key / private key

Jeder kann mit einem öffentlich verfügbaren Schlüssel etwas einschliessen. Aber mit diesem Schlüssel kann man den Kasten NICHT wieder öffnen. Das kann nur der Empfänger der Nachricht mit seinem privaten Schlüssel.



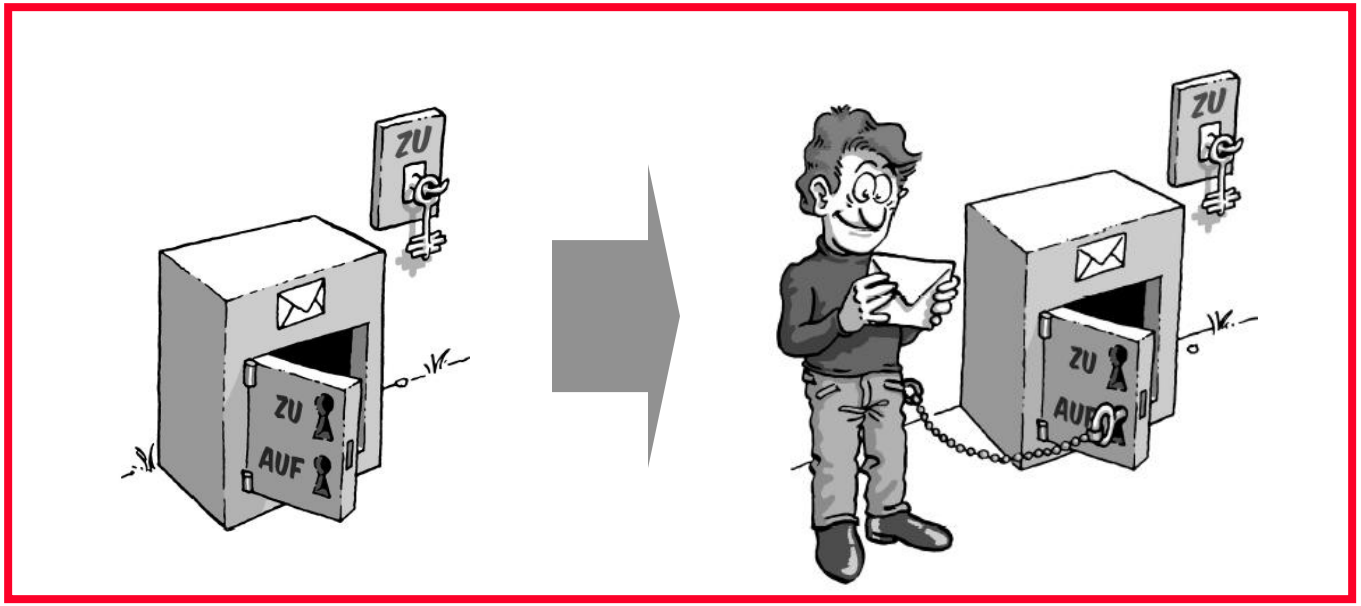
Quelle: www.gnupp.org -> durchblicker1.1.pdf

public key / private key

Ihren privaten Schlüssel kennen und benutzen nur Sie selbst. Er wird niemals einem Dritten mitgeteilt – die Notwendigkeit einer geheimen Vereinbarung entfällt, sie verbietet sich sogar.

Es muss überhaupt nichts Geheimes mehr zwischen Absender und Empfänger ausgetauscht werden – weder eine geheime Vereinbarung noch ein geheimes Codewort.

Das ist – im wahrsten Sinne des Wortes - der Knackpunkt: alle „alten“ Verschlüsselungs-verfahren wurden geknackt, weil ein Dritter sich beim Schlüsselaustausch in den Besitz des Schlüssels bringen konnte.



Quelle: www.gnupp.org -> durchblicker1.1.pdf

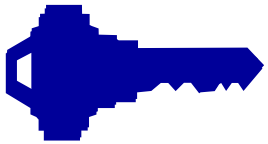
public key / private key

A

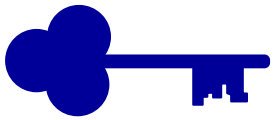
~~Passwort~~

„Passphrase“

Am Brunnen vor dem Tore



A‘s öffentlicher Schlüssel



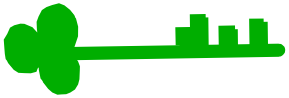
A‘s geheimer Schlüssel

~~Passwort~~

„Passphrase“

Hoch auf dem gelben Wagen

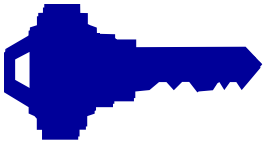
B‘s öffentlicher Schlüssel



B‘s geheimer Schlüssel

B

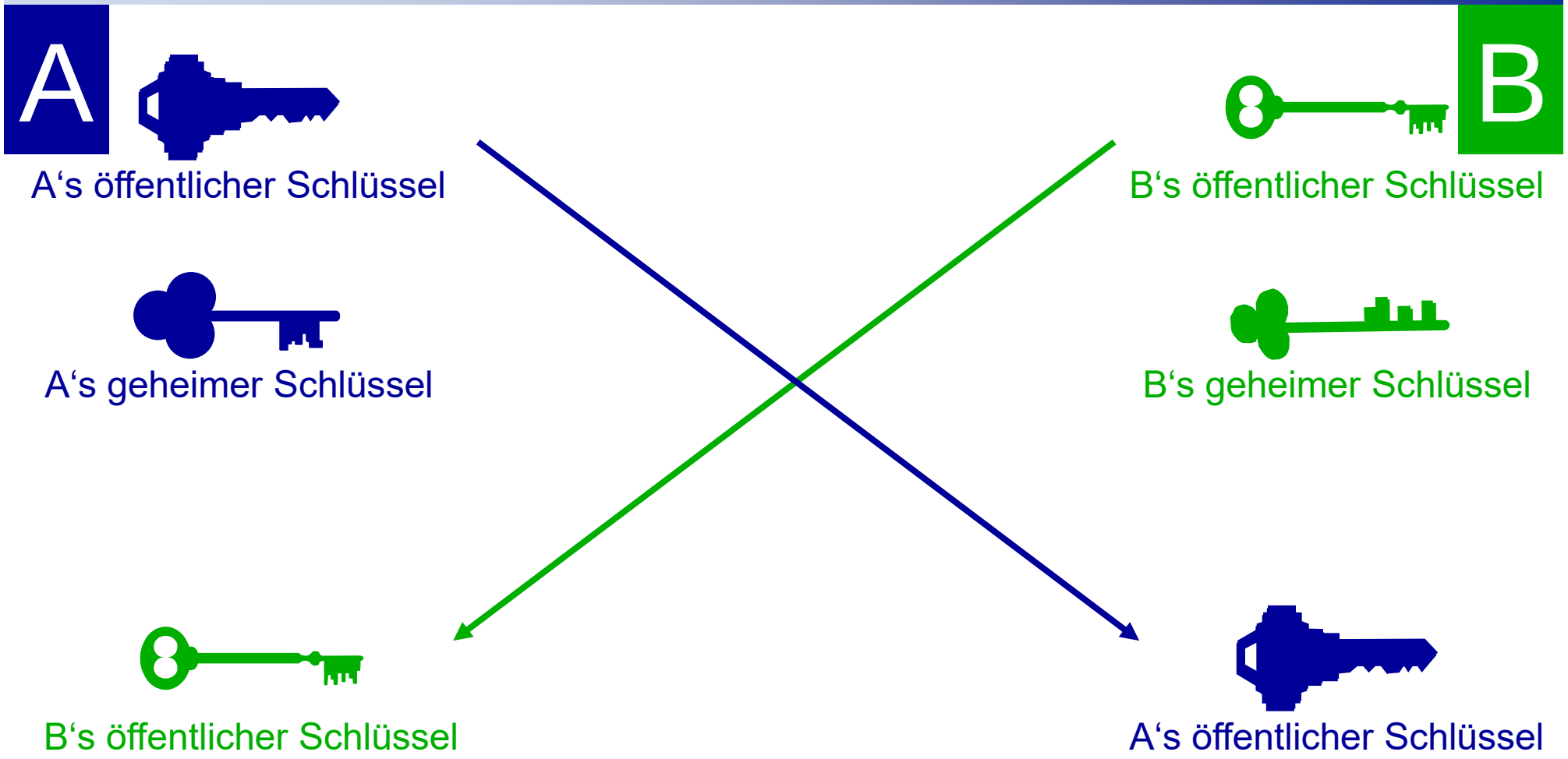
Schlüsselgenerierung



```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1.0.6 (MingW32)
Comment: Weitere Infos: siehe http://www.gnupg.org

mQGiBD7D3QsRBACFJHtw7MYAGSWKZk0kxqqWHvvqfFAoqr/9DlP2Mh8kSpW+DY8E
vbWL99YZ153q7yxAz2tGPTh6DVyjxWmhFOiCymZCDyiM8z8koEllXrtlFvoH6xcR
/yK/N5k5GDM8qcs9sfWXK+2uVvUfpIEgc4X+4x2vCextOgr4b4xVsoY5lwCgjGDD
v66vLVQr6v5Rt4psJQNEC08D/iAmFblHiwZ9NCi02CAwMy/Sbe/I4+gKKfAhfxPS
Lp3ebwOHVU5xe0xCBaGHyStikP9fsJQG4eSTRC7DsBaquDRrDaNfHh4Z5ZLJjQ45
W0zUWRIoSxkLGz8g8FMuhDpIjJOhzamVY0KMZpX3JiPF9XkmkYlOFWRB/O8YH23I
fz/UA/9c8HFRgcJsjOgnPIitQGel/vTlfchWRFq6Pw/m61rXFA7l8mZ7+EKDqt22
WmyGy0txznzE+BOfRP3g1mowf52FITKAib0kDkkcq+zW1OBdmMDAJ3tj7UUnETEN
HMcBNQdRC+oSC9oyeAOqKpIXFiRlKSTskqCNEHj/i+5oQOUwArQsRnJpdHogTXVz
dGVybWFubiA8ZnJpdHoubXVzdGVybWFubkBmaXJtYS5kZT6IVwQTEQIAFwUCPsPd
CwULBwoDBAMVAwIDFgIBAheAAAoJENYsMsuPikin8uEAoIM4UOQVRIFJ/S3CoyjO
pXaD/TUkAJ9J5ZTnxc0hSX0okj3zJ30LLXUMYbkBDQQ+w90NEAQAh6806iwW4rgU
sbS5WU0Zun5Yk9vYgqfMIyoKD5mWmHXN/cdR0NaS54FFrQYbblSgelJ0Cr0ibUmj
32KT6n3FK/MKb6WXv5NJCVk0hLkzddSta6oEaE8joiOAC9o1EeqPm8+xDNMSKtGl
gNphEadCzYQNnGCAwVV9zYLbFXkUg8MAAwUD/jYPuiO+nb66zfJQUdjanajdBQjI
3sztN2P3ZcLvQBQwalZu780lR3qUVZrviaJrFFCWsBdGDoJCyPlHhL+ipDca45/d
gWfSn8zTLq7lvsVXwCP/t6gEihOWe1rH1F0x9aCdxghCDPkC98++x9cM07S7Rw96
decmC5zsf/F3nh7eiEYEGBECAAYFAj7D3Q0ACgkQ1iwyy4+KScO8QCdFOkdrlpi
ZyAxopu2iKnwXGCj5Z4An04nHTqWqEz1rxA35JTP+bEkVZ62
=6PPu
-----END PGP PUBLIC KEY BLOCK-----
```

ein Schlüssel



Schlüsselaustausch

A

B

B‘s öffentlicher Schlüssel

+

Wir treffen uns heute um 15 Uhr.
A.

=

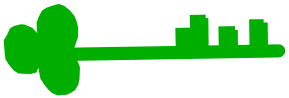
eR7/uk350kMbG8
(l=#*bfR3$2bG5%

eR7/uk350kMbG8
(l=#*bfR3$2bG5%

Nachrichtenverschlüsselung

A

B‘s öffentlicher Schlüssel



B

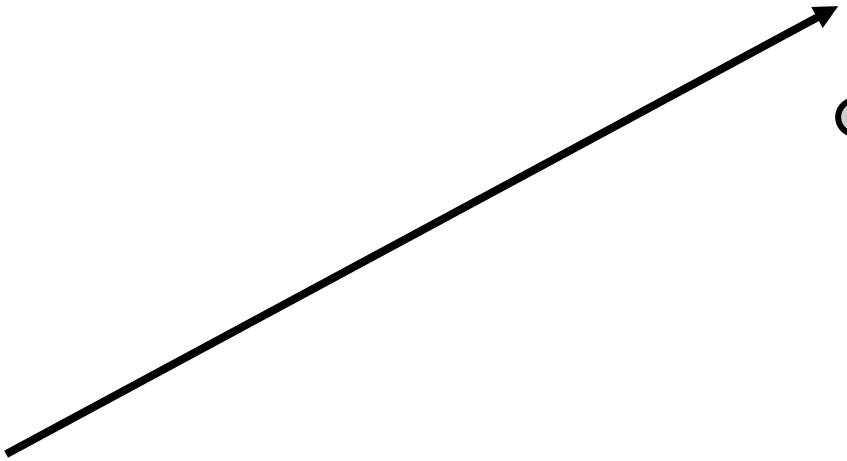
B‘s geheimer Schlüssel

+

Wir treffen uns
heute um 15 Uhr.
A.

=

eR7/uk350kMbG8
(l=#*bfR3$2bG5%



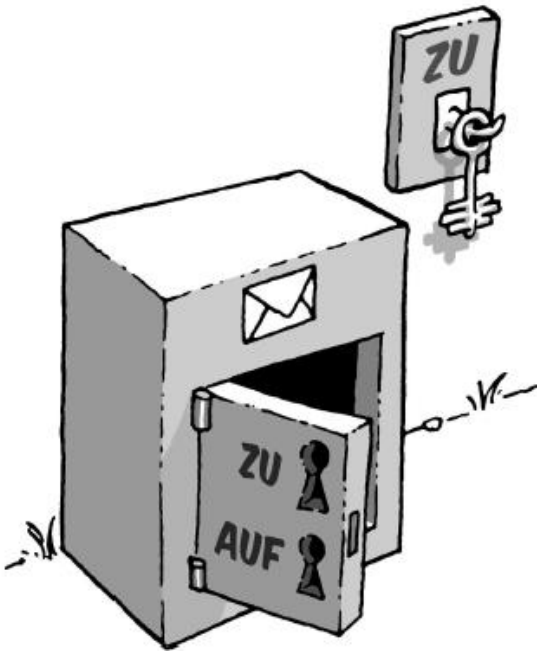
+

eR7/uk350kMbG8
(l=#*bfR3$2bG5%

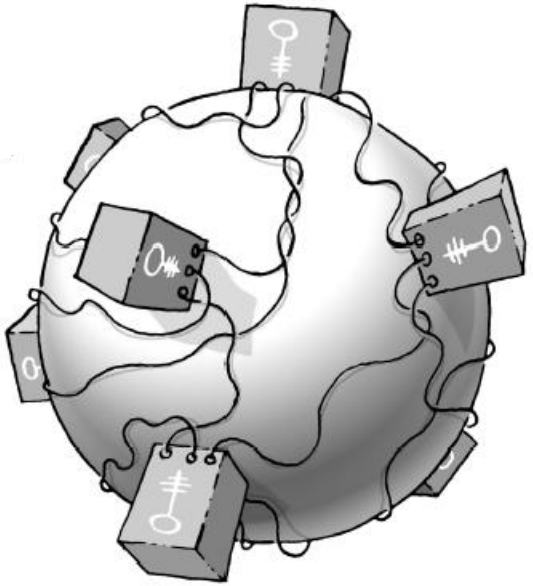
=

Wir treffen uns
heute um 15 Uhr.
A.

Nachrichtenentschlüsselung



- als Mailanhang
- auf der eigenen Webseite
- persönlich auf Diskette
- über öffentliche Schlüsselserver (z.B. www.keyserver.net)



Quelle: www.gnupp.org -> durchblicker1.1.pdf

Verbreitung des öffentlichen Schlüssels

Symmetrische und Asymmetrische Verschlüsselung

a	1
b	2
c	3
d	4
e	5
f	6
g	7
h	8
i	9
j	10
k	11
l	12
m	13
n	14
o	15
p	16
q	17
r	18
s	19
t	20
u	21
v	22
w	23
x	24
y	25
z	26

Information: Fachbereich Seefahrt
= 6 1 3 8 2 5 18 5 9 3 8 19 5 5 6 1 8 18 20

Operation: +

Schlüssel: 7

Ergebnis: 13 8 10 15 9 12 25 12 16 10 15 26 12 12 13 8 15 25 1
= mhjoilylpjozllmhoya

Wer den Schlüssel hat und die Operation kennt, kann die verschlüsselte Information wieder entschlüsseln :

m -> 13 -> 6 -> f
h -> 8 -> 1 -> a
... usw.

„&“

Asymmetrische Verschlüsselung

„Verzerrung“ von Schlüsseln, damit sie über unsichere Verbindungen übertragen werden können.

Der Empfänger entschlüsselt nicht, sondern führt dieselbe Verzerrung durch und überprüft die Gleichheit der Ergebnisse.

„+“

Symmetrische Verschlüsselung

Umkehrbare Verschlüsselung von Informationen.

Der Sender verschlüsselt – der Empfänger entschlüsselt.

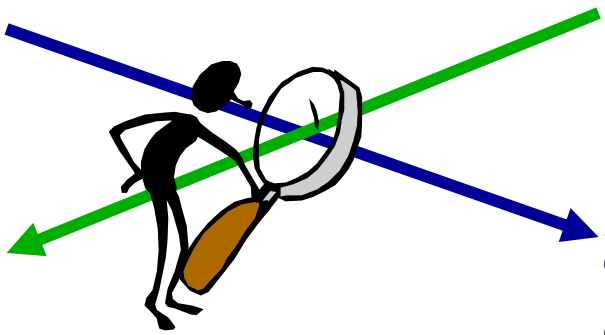
Alice

general key p:
8

Bob

private key a:
12
&
8
=
20 (= a & p = A)

14 (= B = b & p)
&
12 (= a)
=
26 (= S = b & p & a)



private key b:
6
&
8
=
14 (= b & p = B)

20 (= A = a & p)
&
6 (= b)
=
26 (= S = a & p & b)

Alice

general key p:
8

Bob

private key a:
12
&
8
=
20 (= a & p =)

te key b:

14 (= B = b & p)
&
12 (= a)
=
26 (= S = b & p & a)

=)

= b)

26 (= S = a & p & b)

Entscheidend ist, dass beide Partner zum SELBEN Ergebnis kommen, das aber NICHT zwischen ihnen ausgetauscht wurde !!

Alice

general key p:
8

Bob

private key a:
12
&
8
=
20 (= a & p =

te key b:

Aber der Horcher in der Mitte kann sich doch die private keys rückwärts ausrechnen ???????

14 (= B = b & p)
&
12 (= a)
=
26 (= S = b & p & a)

= b)

26 (= S = a & p & b)

Exkurs: Reste-Arithmetik

Definition: $a \;\&_m\; b = c$ = **„der Rest, der bleibt, wenn man a+b durch m teilt“**

z.B.:

$13 \;\&_7\; 8 = 0$

$17 \;\&_7\; 5 = 1$

$22 \;\&_7\; 8 = 3$

$11 \;\&_7\; 7 = 4$

$17 \;\&_7\; 12 = ?$

$15 \;\&_7\; 23 = ?$

$28 \;\&_7\; 9 = ?$

$19 \;\&_7\; 31 = ?$

Definition: $a \;\&_m\; b = c$ = **„der Rest, der bleibt, wenn man a+b durch m teilt“**

z.B.:

$13 \;\&_7\; 8 = 0$ $\quad$ $17 \;\&_7\; 12 = 1$

$17 \;\&_7\; 5 = 1$ $\quad$ $15 \;\&_7\; 23 = 3$

$22 \;\&_7\; 8 = 3$ $\quad$ $28 \;\&_7\; 9 = 6$

$11 \;\&_7\; 7 = 4$ $\quad$ $19 \;\&_7\; 31 = 1$

Definition: $a \;\&_m\; b = c$ = **„der Rest, der bleibt, wenn man a+b durch m teilt“**

ACHTUNG: **Aus der Kenntnis von b,m und c kann man a NICHT berechnen ! („Falltür-Funktion“)**

z.B.:

$a \;\&_7\; 8 = 3$

-> a = 2 ? a = 9 ? a = 16 ? a = 23 ? ...

Die Falltürfunktion muß kommutativ sein, d.h.

$$\mathbf{a \ \&_m b = b \ \&_m a}$$

z.B.:

$$13 \ \&_7 \ 8 = 8 \ \&_7 \ 13 = 0$$
$$17 \ \&_7 \ 5 = 5 \ \&_7 \ 17 = 1$$

Dann ist nämlich

$$\mathbf{a \ \&_m b \ \&_m c = b \ \&_m a \ \&_m c}$$

Nocheinmal: Symmetrische und Asymmetrische Verschlüsselung

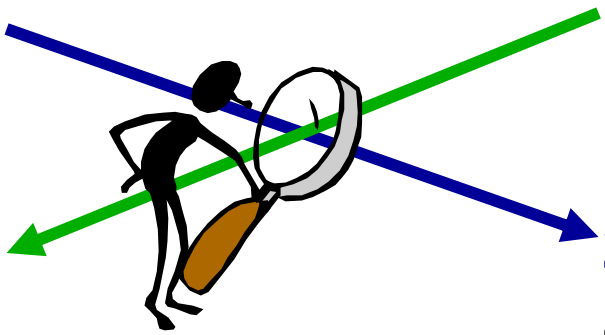
Alice

general key p:
8

Bob

private key a:
12
&
8
=
20 (= a & p = A)

14 (= B = b & p)
&
12 (= a)
=
26 (= S = b & p & a)



private key b:
6
&
8
=
14 (= b & p = B)

20 (= A = a & p)
&
6 (= b)
=
26 (= S = a & p & b)

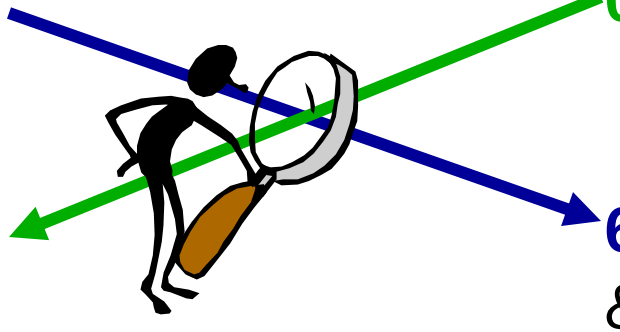
Alice

general key p:
8 - 3 - 11

Bob

private key a:
12 - 4 - 9
$\&_7$
8 - 3 - 11
=
6 - 0 - 6 (= a $\&_7$ p = A)

0 - 6 - 2 (= B = b $\&_7$ p)
$\&_7$
12 - 4 - 9 (= a)
=
5 - 3 - 4 (= S = b $\&_7$ p $\&_7$ a)



private key b:
6 - 10 - 5
$\&_7$
8 - 3 - 11
=
0 - 6 - 2 (= b $\&_7$ p = B)

6 - 0 - 6 (= A = a $\&_7$ p)
$\&_7$
6 - 10 - 5 (= b)
=
5 - 3 - 4 (= S = a $\&_7$ p $\&_7$ b)

Quelle: T. Beth, "Sichere offene Datennetze", Spektrum der Wissenschaft, Mai 1995, S. 46-55

Beispiel für asymmetrische Verschlüsselung

Alice

general key p:
8 - 3 - 11

Bob

private key a:
12 - 4 - 9
$\&_7$
8 - 3 - 11
=
6 - 0 - 6 (= a

geheime Schlüssel

Schlüsselpaar !!

öffentliche Schlüssel

private key b:
6 - 10 - 5
$\&_7$
8 - 3 - 11
=
0 - 6 - 2 (= b $\&_7$ p = B)

0 - 6 - 2 (= B = b $\&_7$ p)
$\&_7$
12 - 4 - 9 (= a)
=
5 - 3 - 4 (= S = b $\&_7$ p $\&_7$ a)

6 - 0 - 6 (= A = a $\&_7$ p)
$\&_7$
6 - 10 - 5 (= b)
=
5 - 3 - 4 (= S = a $\&_7$ p $\&_7$ b)

Quelle: T. Beth, "Sichere offene Datennetze", Spektrum der Wissenschaft, Mai 1995, S. 46-55

Sichere Übermittlung eines Schlüssels über einen unsicheren Kommunikationskanal

Was könnte jemand, der p und die Operation „$\&_7$“kennt, mit dem abgehörten A anfangen ?

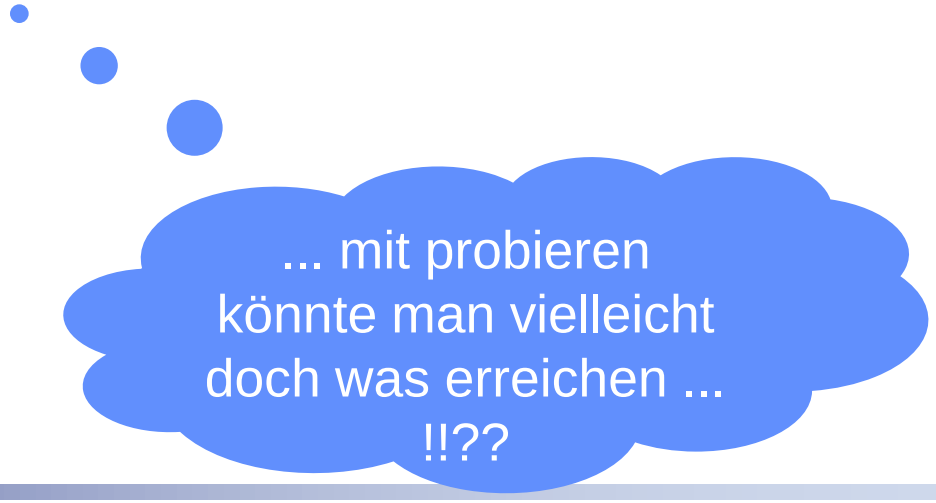
a = 12 – 4 – 9
p = 8 – 3 – 11
A = 6 – 0 – 6

$A = a \&_7 p$
$6 = a \&_7 8$
a = ?
a = 5, 12, 19, 26, 33, ...

... mit probieren
könnte man vielleicht
doch was erreichen ...
!!??

-> Operationen mit sehr komplizierten Umkehr-Operationen
-> lange Schlüssel

=> Knacken des Schlüssels prinzipiell möglich – aber nicht mit vertretbarem Zeitaufwand



$$A = a \&_n p$$

Nicht so, ... sondern so!

$$A = (a+p) \bmod n$$

$$A = p^a \bmod n$$

a = 12
p = 8
n = 7

A = 20 mod 7
= 6

a = 12
p = 1745263857352738 4...9597
n = 8253749573626748 4...7881

z.B. 1024 bit = 307 Dezimalstellen

$$A = 17452638573527384...9597^{12} \bmod 8253749573626748 4...7881$$
$$= 6419284652627804947...3561$$

Quelle: K. Fuhrberg “Internetsicherheit”, Hanser-Verlag 1998, S. 86

Sichere Übermittlung eines Schlüssels über einen unsicheren Kommunikationskanal

Beispiel mit kleinen Zahlen

$A = p^a \bmod n$

$a = 22$

$p = 17452638573527384...9597$

$n = 82537495736267484...7881$

z.B. 1024 bit = 307 Dezimalstellen

$A = 17452638573527384...9597^{22} \bmod 82537495736267484...7881$

$= 641928465262780494 7...3561$

$a = 22$

$p = 3$

$n = 17$

$A = 3^{22} \bmod 17$

$= 31381059609 \bmod 17$

$= 15$

Knacken durch Probieren:

- 3^x ausrechnen
- durch 17 teilen
- Rest gleich 15 ?

(siehe Verschluesselung.xls)

Angenommen man würde einen Chip entwickeln, der in einer Sekunde eine Milliarde Schlüssel durchprobieren könnte - was auch heute noch jenseits aktueller Computerleistung liegt. Weiter vorausgesetzt, man hätte 1 Milliarde dieser Chips zur Verfügung, so würde die Berechnung aller möglichen Schlüssel dennoch circa 10 Billionen Jahre dauern. Zum Vergleich: Unser Universum ist selbst erst 15 bis 20 Milliarden Jahre alt. Um einen kompletten Schlüsselraum zu durchsuchen, würde man also unter den genannten Voraussetzungen noch einmal 1500- bis 2000-mal das Alter des Universums benötigen. Zugegeben: Im statistischen Mittel findet man den richtigen Schlüssel bereits nach der Hälfte der Zeit.

Eine Zusammenschaltung von 10^{24} Chips könnte rein theoretisch den gesamten Schlüsselraum in einem Tag berechnen. Der Haken ist nur, dass es im gesamten Universum - nach heutigem Wissensstand - nicht genügend Siliziumatome gibt, um alle diese Chips zu fertigen.

Quelle: c't 21/99, S. 314ff.

Alice

general key p:
5 - 13 - 9

Bob

private key a:
12 - 4 - 9
$\&_7$
5 - 13 - 9
=
__ - __ - __ (= a $\&_7$ p = A)

__ - __ - __ (= B = b $\&_7$ p)
$\&_7$
12 - 4 - 9 (= a)
=
__ - __ - __ (= S = b $\&_7$ p $\&_7$ a)

private key b:
6 - 10 - 5
$\&_7$
5 - 13 - 9
=
__ - __ - __ (= b $\&_7$ p = B)

__ - __ - __ (= A = a $\&_7$ p)
$\&_7$
6 - 10 - 5 (= b)
=
__ - __ - __ (= S = a $\&_7$ p $\&_7$ b)

Quelle: T. Beth, "Sichere offene Datennetze", Spektrum der Wissenschaft, Mai 1995, S. 46-55

Übungsaufgabe zum public key Verfahren

Alice

general key p:
5 - 13 - 9

Bob

private key a:
12 - 4 - 9
$\&_7$
5 - 13 - 9
=
3 - 3 - 4 (= a $\&_7$ p = A)

4 - 2 - 0 (= B = b $\&_7$ p)
$\&_7$
12 - 4 - 9 (= a)
=
2 - 6 - 2 (= S = b $\&_7$ p $\&_7$ a)

private key b:
6 - 10 - 5
$\&_7$
5 - 13 - 9
=
4 - 2 - 0 (= b $\&_7$ p = B)

3 - 3 - 4 (= A = a $\&_7$ p)
$\&_7$
6 - 10 - 5 (= b)
=
2 - 6 - 2 (= S = a $\&_7$ p $\&_7$ b)

Quelle: T. Beth, "Sichere offene Datennetze", Spektrum der Wissenschaft, Mai 1995, S. 46-55

Übungsaufgabe zum public key Verfahren (Lösung)

general key p

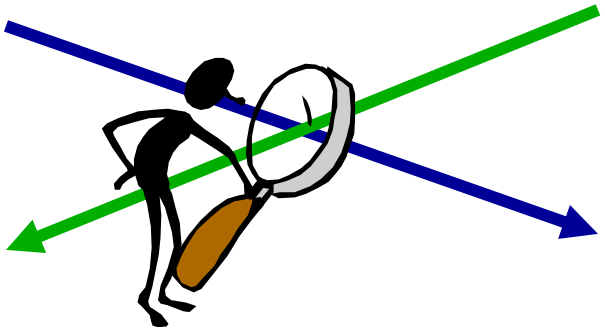
Alice

private key a

$A = a \,\&\, p$

B

$S_{a,b} = B \,\&\, a = b \,\&\, p \,\&\, a$



Bob

private key b

$B = b \,\&\, p$

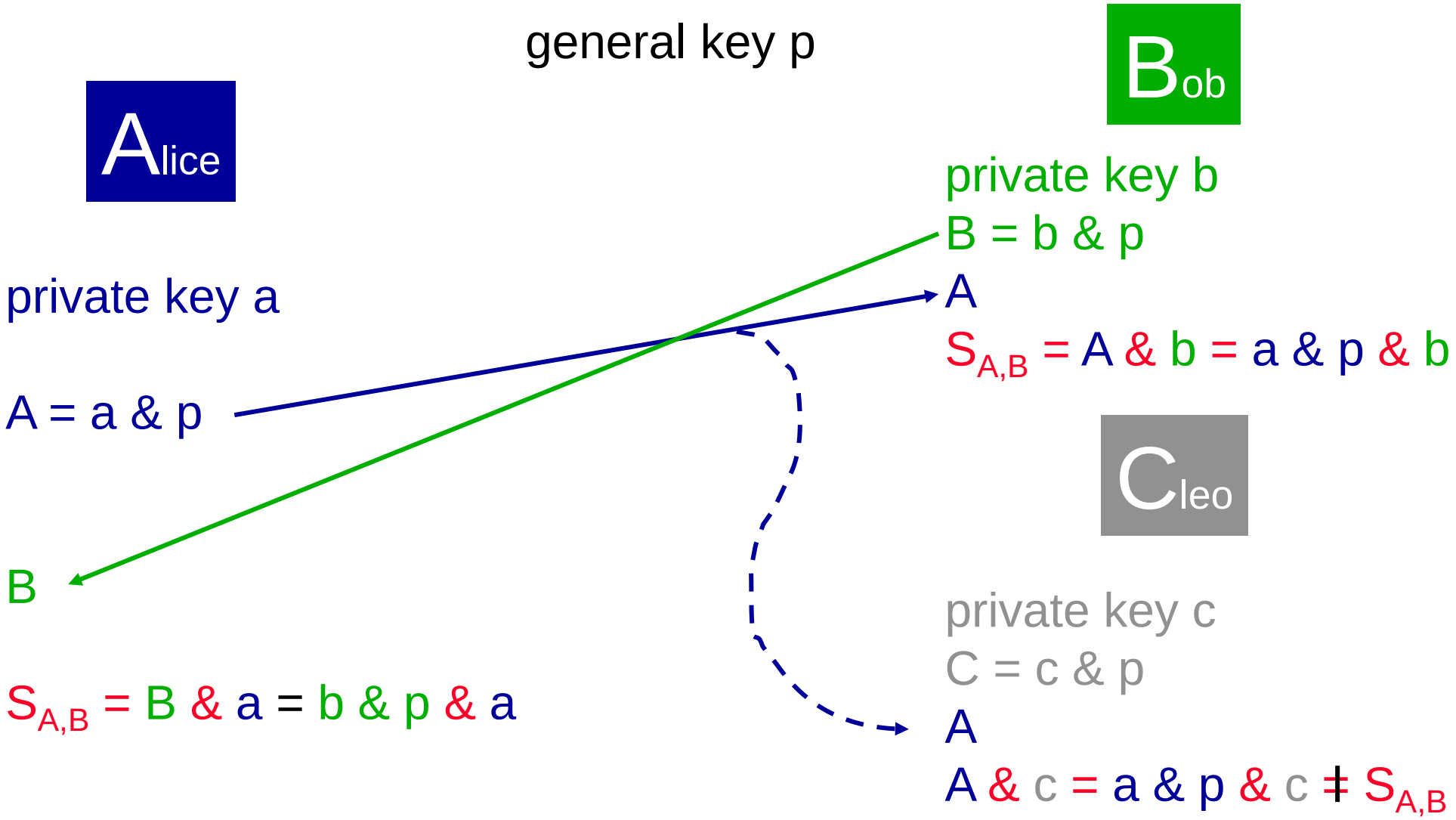
A

$S_{a,b} = A \,\&\, b = a \,\&\, p \,\&\, b$

Quelle: T. Beth, "Sichere offene Datennetze", Spektrum der Wissenschaft, Mai 1995, S. 46-55
Diffie/Hellman 1976
K. Fuhrberg "Internetsicherheit", Hanser-Verlag 1998, S. 86

& = „Falltürfunktion"

Sichere Übermittlung eines Schlüssels über einen unsicheren Kommunikationskanal



& = „Falltürfunktion“

Quelle: T. Beth, ”Sichere offene Datennetze”, Spektrum der Wissenschaft, Mai 1995, S. 46-55

C kann den Schlüssel von A und B mit seinem privaten Schlüssel c nicht erzeugen !

general key p

Alice

Bob

private key b

B = b & p

A

$S_{A,B}$ = A & b = a & p & b

private key a

A = a & p

Cleo

B,C

private key c

C = c & p

A

$S_{A,C}$ = A & c = a & p & c

$S_{A,B}$ = B & a = b & p & a

$S_{A,C}$ = C & a = c & p & a

& = „Falltürfunktion“

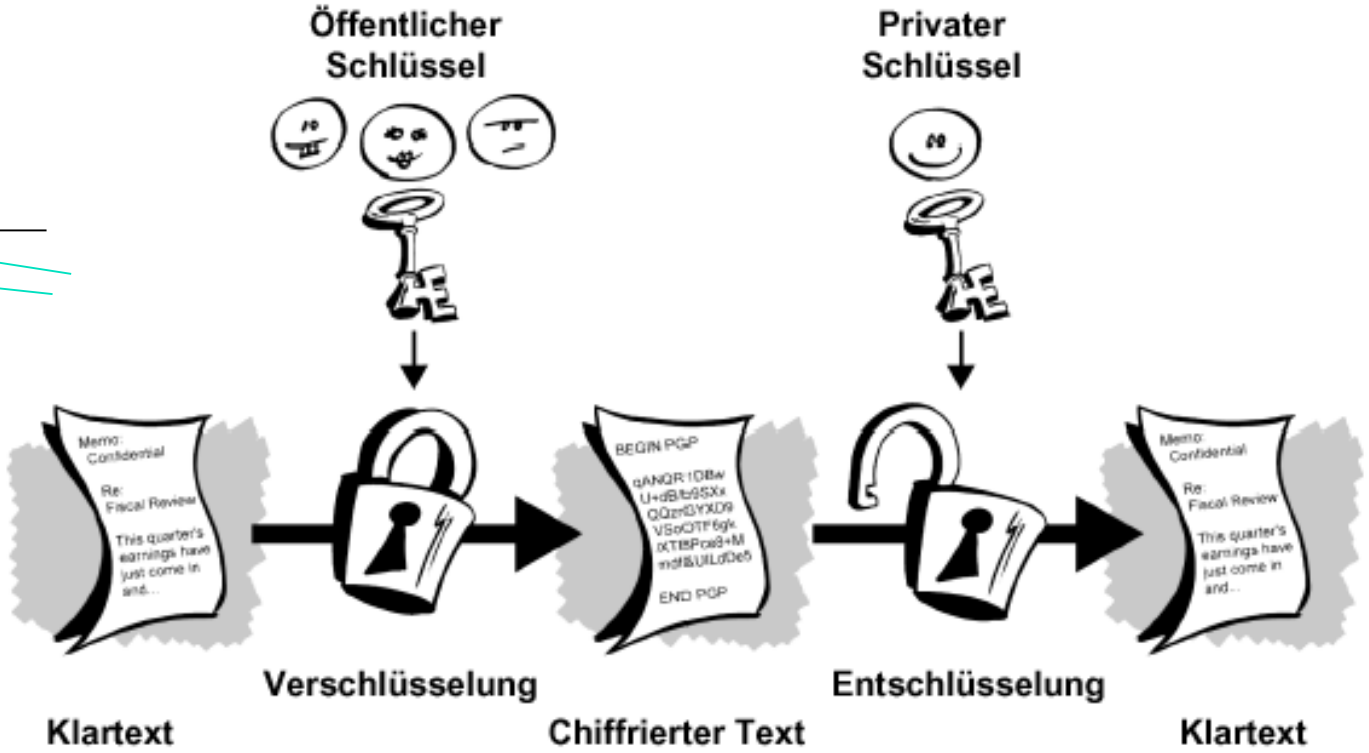
Quelle: T. Beth, ”Sichere offene Datennetze”, Spektrum der Wissenschaft, Mai 1995, S. 46-55

A und B sowie A und C haben jeweils einen gemeinsamen Schlüssel

Wir haben jetzt also ein Verfahren, nach dessen Anwendung zwei Kommunikationspartner über DIESELBE Information verfügen. Diese Information ist dabei NICHT zwischen ihnen ausgetauscht worden !!

Das public key Verfahren im Detail

„Mit einem öffentlichen Schlüssel werden Daten verschlüsselt, und mit dem dazugehörigen privaten Schlüssel werden Daten entschlüsselt.“



Quelle: IntroToCrypto.pdf aus dem PGP-SW-Paket

???

„Eine Nachricht wird nicht mehr mit ein und dem gleichen Schlüssel ver- und entschlüsselt, sondern mit zwei unterschiedlichen, einander zugeordneten Schlüsseln. Einen dieser Schlüssel bezeichnet man als öffentlichen Schlüssel, da er öffentlich bekannt sein kann. Der öffentliche Schlüssel einer Person wird verwendet, um eine Nachricht an diese Person zu verschlüsseln. Der private Schlüssel hingegen wird zur Decodierung der verschlüsselten Nachricht verwendet und steht nur dem Empfänger zur Verfügung. Der Besitz des öffentlichen Schlüssels einer Person ermöglicht lediglich das Versenden einer verschlüsselten Nachricht an diese Person. Mit Hilfe des öffentlichen Schlüssels kann diese Nachricht jedoch nicht gelesen werden!“

(Quelle: Hansen, „Wirtschaftsinformatik“, S. 453)

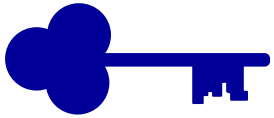
???

A

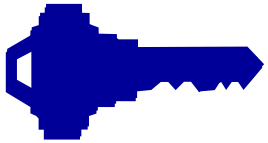
~~Passwort~~

„Passphrase“

Am Brunnen vor dem Tore



A‘s geheimer Schlüssel

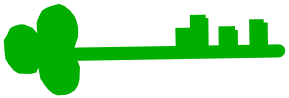


A‘s öffentlicher Schlüssel

~~Passwort~~

„Passphrase“

Hoch auf dem gelben Wagen



B‘s geheimer Schlüssel

B‘s öffentlicher Schlüssel

B

Schlüsselgenerierung

A

B

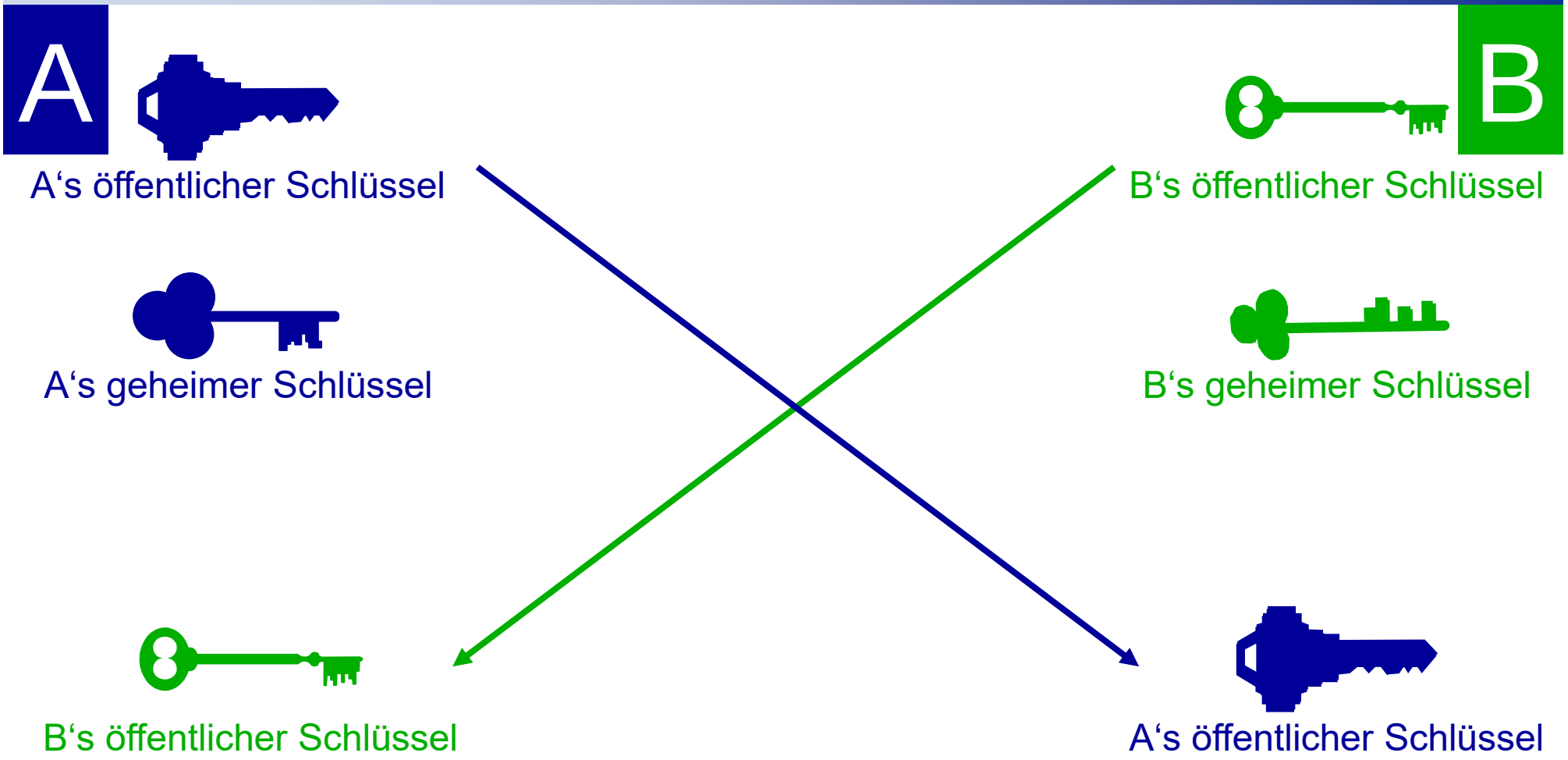
allgemeiner Schlüssel:
p

Hoch auf dem gelben Wagen

B‘s geheimer Schlüssel:
b

B‘s öffentlicher Schlüssel
B = b & p

Der öffentliche Schlüssel ist in Wirklichkeit der mit einem allgemeinen Schlüssel verzerrte geheime Schlüssel !



Schlüsselaustausch

A

B

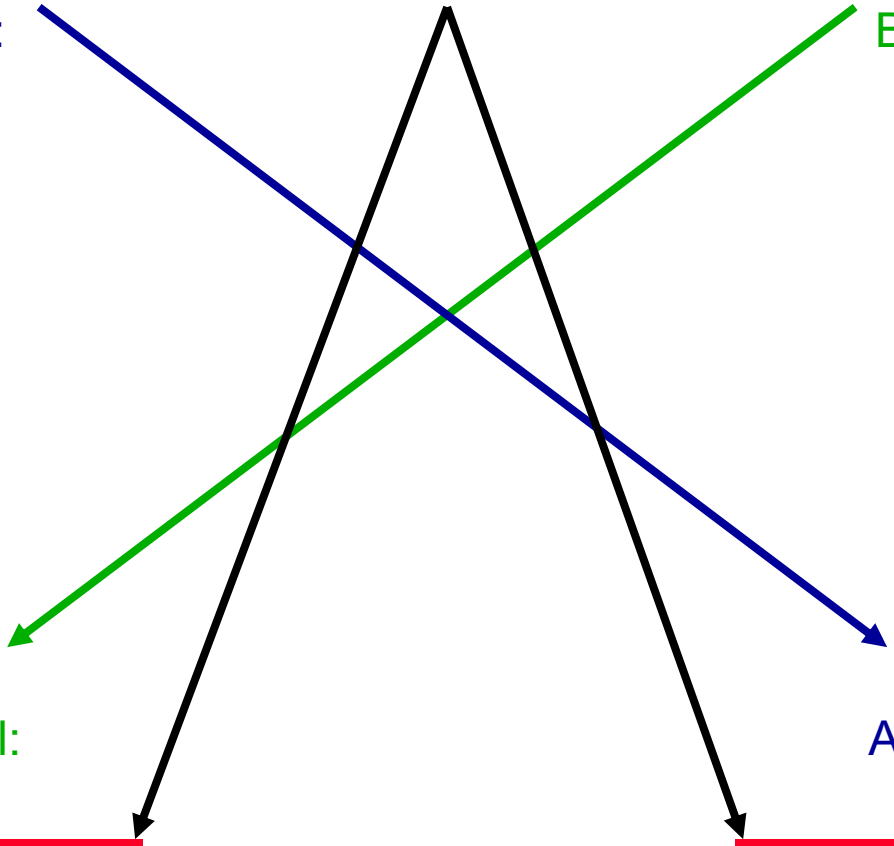
allgemeiner Schlüssel:
p

A‘s öffentlicher Schlüssel:
A = a & p

B‘s öffentlicher Schlüssel
B = b & p

A‘s geheimer Schlüssel
a

B‘s geheimer Schlüssel:
b



B‘s öffentlicher Schlüssel:
B = b & p

A‘s öffentlicher Schlüssel:
A = a & p

GEMEINSAMER SCHLÜSSEL:

$S_{a,b} = a \& B = a \& b \& p$

GEMEINSAMER SCHLÜSSEL:

$S_{a,b} = b \& A = b \& a \& p$

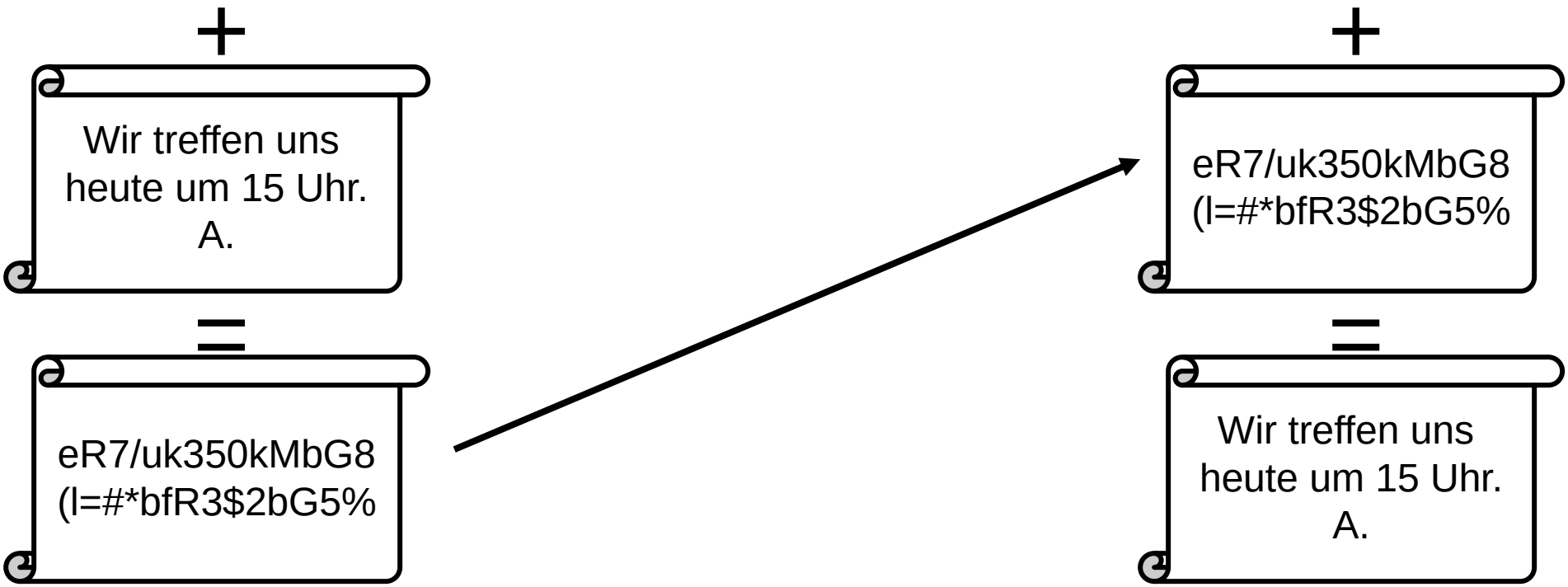
Schlüsselaustausch im Detail

A

B

B‘s öffentlicher Schlüssel

B‘s geheimer Schlüssel



Nachrichtenver- und entschlüsselung

A

A‘s geheimer Schlüssel a
&
B‘s öffentlicher Schlüssel B

B‘s geheimer Schlüssel b
&
A‘s öffentlicher Schlüssel A

B

GEMEINSAMER SCHLÜSSEL:

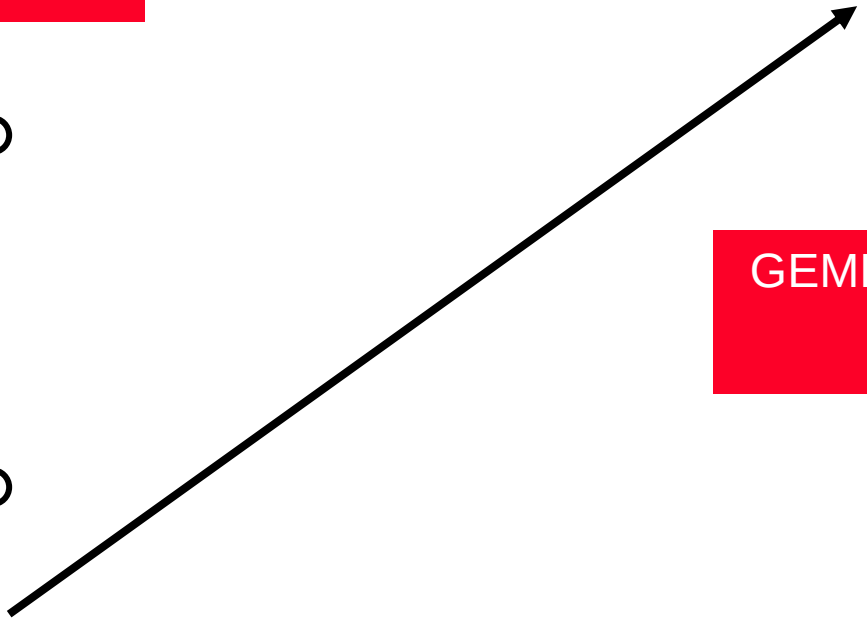
$S_{a,b}$ = a & B = a & b & p

+

Wir treffen uns
heute um 15 Uhr.
A.

=

eR7/uk350kMbG8
(l=#*bfR3$2bG5%



eR7/uk350kMbG8
(l=#*bfR3$2bG5%

-

GEMEINSAMER SCHLÜSSEL:

$S_{a,b}$ = b & A = b & a & p

=

Wir treffen uns
heute um 15 Uhr.
A.

Nachrichtenver- und entschlüsselung im Detail

A

B‘s öffentlicher Schlüssel B
&
A‘s geheimer Schlüssel a

B‘s geheimer Schlüssel b
&
A‘s öffentlicher Schlüssel A

B

GEMEINSAMER SCHLÜSSEL:

$S_{a,b} = a \& B = a \& b \& p$

+

eR7/uk350kMbG8
bfR3$2bG5%

Wir
heu

(l=#*bfR3

EL:
p

en uns
um 15 Uhr.
A.

Das Verfahren „&“ der Schlüsselverzerrung ist nicht oder nur sehr schwer umkehrbar.

Das Verfahren „+“ der Nachrichtenverschlüsselung mit dem gemeinsamen Schlüssel dagegen muss natürlich umkehrbar sein (-> Entschlüsselung) !!

„&“
Asymmetrische Verschlüsselung

„+“
Symmetrische Verschlüsselung

Das Verfahren „&“ der Schlüsselverzerrung ist nicht oder nur sehr schwer umkehrbar.

Das Verfahren „+“ der Nachrichtenverschlüsselung mit dem gemeinsamen Schlüssel dagegen muss natürlich umkehrbar sein (-> Entschlüsselung) !!

„&“

Asymmetrische Verschlüsselung

„+“

Symmetrische Verschlüsselung

A = a & p
B = b & p

$S_{a,b}$ = b & A = b & a & p
$S_{a,b}$ = a & B = a & b & p

GEMEINSAMER SCHLÜSSEL:

$S_{a,b}$ = a & B = a & b & p

+

Wir treffen uns heute um 15 Uhr.

=

eR7/uk350kMbG8
(l=#*bfR3$2bG5%

„&“
Asymmetrische Verschlüsselung

„Verzerrung“ von Schlüsseln, damit sie über unsichere Verbindungen übertragen werden können.

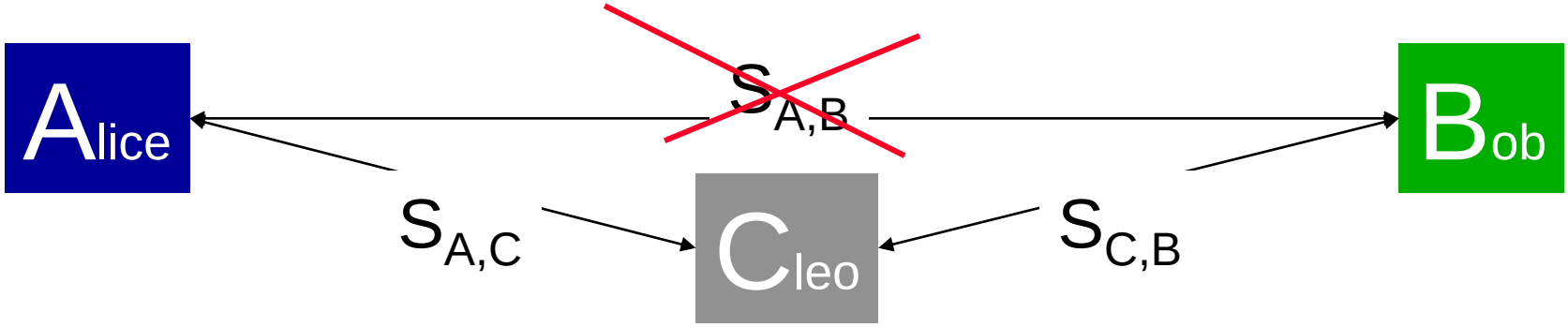
Der Empfänger entschlüsselt nicht, sondern führt dieselbe Verzerrung durch und überprüft die Gleichheit der Ergebnisse.

„+“
Symmetrische Verschlüsselung

Umkehrbare Verschlüsselung von Informationen.

Der Sender verschlüsselt – der Empfänger entschlüsselt.

man-in-middle attack

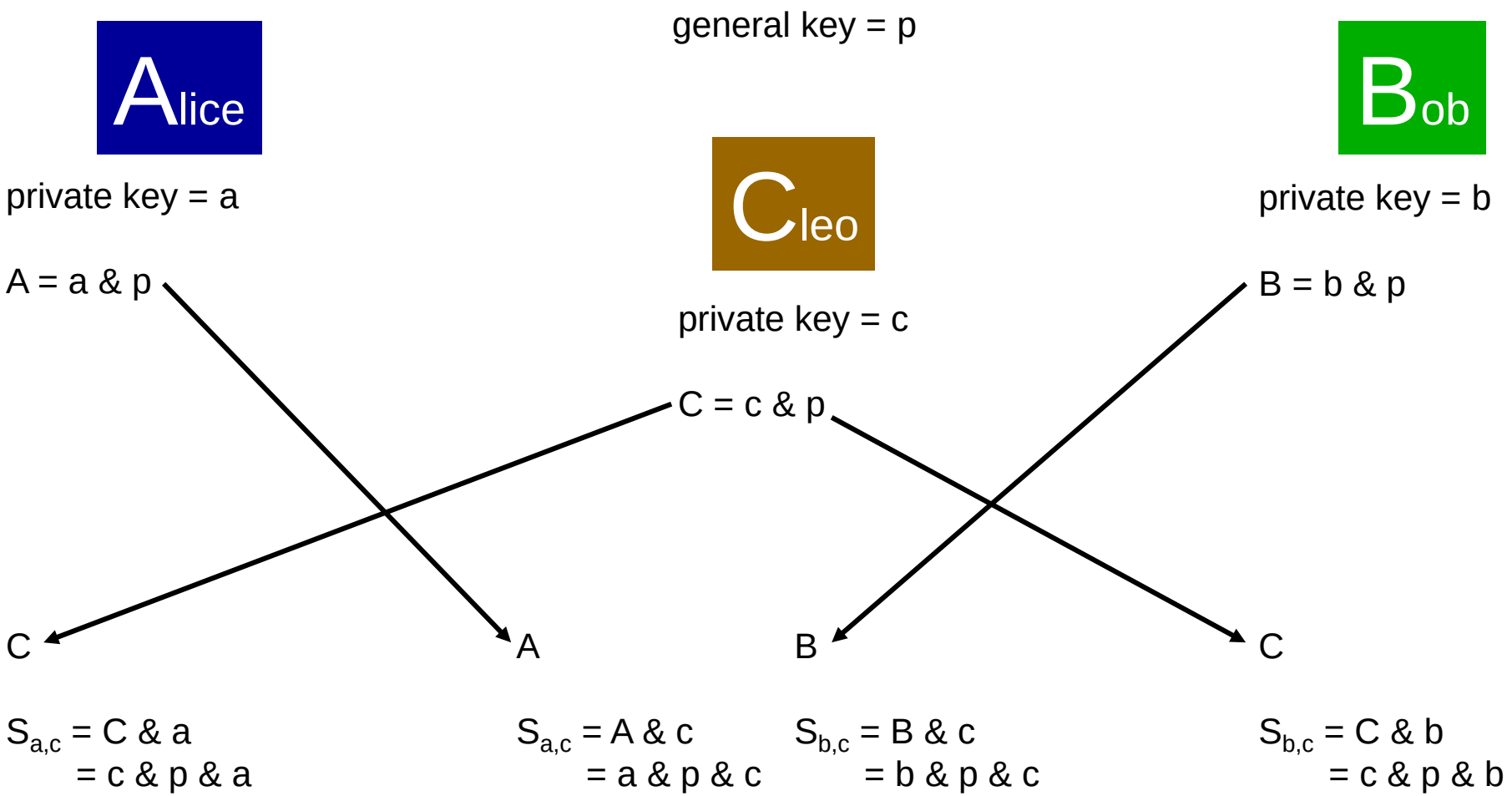


Ein Angreifer („Cleo“) klinkt sich in den Datenverkehr zwischen A und B ein und

1. fängt die zwischen A und B ausgetauschten öffentlichen Schlüssel ab
2. sendet A und B jeweils seinen eigenen öffentlichen Schlüssel zu
3. hat jetzt einen gemeinsamen Schlüssel mit A und einen anderen mit B
4. fängt den verschlüsselten Datenverkehr von A an B ab
5. entschlüsselt ihn mit seinem Schlüssel $S_{A,C}$
6. verschlüsselt ihn wieder mit seinem Schlüssel $S_{C,B}$
7. sendet die (ggf. verfälschten) Daten an B

Quelle: T. Beth, ”Sichere offene Datennetze”, Spektrum der Wissenschaft, Mai 1995, S. 46-55

„man-in-the-middle“ attack



Quelle: T. Beth, "Sichere offene Datennetze", Spektrum der Wissenschaft, Mai 1995, S. 46-55

„man-in-the-middle“ attack

general key p:
8 - 3 - 11

private key a:
12 - 4 - 9

private key c:
17 - 3 - 25

private key b:
6 - 10 - 5

general key p:
8 - 3 - 11

Alice

private key a:
12 - 4 - 9
$\&_7$
8 - 3 - 11
=
6 - 0 - 6 (= a $\&_7$ p = A)

Cleo

private key c:
17 - 3 - 25
$\&_7$
8 - 3 - 11
=
4 - 6 - 1 (= c $\&_7$ p = C)

Bob

private key b:
6 - 10 - 5
$\&_7$
8 - 3 - 11
=
0 - 6 - 2 (= b $\&_7$ p = B)

4 - 6 - 1 (= C = c $\&_7$ p)
$\&_7$
12 - 4 - 9 (= a)
=
2 - 3 - 3 (= $S_{a,c}$ = c $\&_7$ p $\&_7$ a)

4 - 6 - 1 (= C = c $\&_7$ p)
$\&_7$
6 - 10 - 5 (= b)
=
3 - 2 - 6 (= $S_{b,c}$ = c $\&_7$ p $\&_7$ b)

6 - 0 - 6 (= A = a $\&_7$ p)
$\&_7$
17 - 3 - 25 (= c)
=
2 - 3 - 3 (= $S_{a,c}$ = a $\&_7$ p $\&_7$ c)

0 - 6 - 2 (= B = b $\&_7$ p)
$\&_7$
17 - 3 - 25 (= c)
=
3 - 2 - 6 (= $S_{b,c}$ = b $\&_7$ p $\&_7$ c)

Quelle: T. Beth, "Sichere offene Datennetze", Spektrum der Wissenschaft, Mai 1995, S. 46-55

„man-in-the-middle" attack

Authentifizierung

=

Vergewisserung über die Identität des Partners

§2 „Begriffsbestimmungen:

„Zertifizierungsdiensteanbieter“

↓

„qualifizierte Zertifikate“

↓

„Signaturprüfschlüssel“

↓

„elektronische Signatur“ → „qualifizierte elektronische Signatur“

der handschriftlichen Unterschrift juristisch gleichgestellt !

„elektronische Signatur“ → „fortgeschrittene elektronische Signatur“

Quelle: Bundesgesetzblatt 2001, Teil1, Nr. 22 vom 21.5.2001

general key p:
8 - 3 - 11

Alice

Z

Bob

a = 12 - 4 - 9
p = 8 - 3 - 11
ap = 6 - 0 - 6

z = 15 - 2 - 7
p = 8 - 3 - 11
zp = 2 - 5 - 4

zp = 2 - 5 - 4
ap = 6 - 0 - 6
apzp = 1 - 5 - 3

persönliche Übergabe und Identifizierung der Person

ap = 6 - 0 - 6 - Name - ...
z = 15 - 2 - 7
apz = 0 - 2 - 6 - Name - ...

Chipkarte

apz = 0 - 2 - 6 - Name - ...
p = 8 - 3 - 11
apzp = 1 - 5 - 3 - Name - ...

OK

apzp = 1 - 5 - 3 - Name - ...

Quelle: T. Beth, "Sichere offene Datennetze", Spektrum der Wissenschaft, Mai 1995, S. 46-55

Authentifizierung durch eine Signatur

general key p:
8 - 3 - 11

Alice

a = 12 -4 - 9
p = 8 -3 - 11
ap = 6 -0 - 6

Z

z = 15 - 2 - 7
p = 8 - 3 - 11
zp = 2 - 5 - 4

Bob

persönliche Übergabe und Identifizierung der Person

ap = 6 - 0 - 6 - Name - ...
z = 15 - 2 - 7
apz = 0 - 2 - 6 - Name - ...

Chipkarte

Cleo

c = 17 - 3 - 25
p = 8 - 3 - 11
cp = 4 - 6 - 1

zp = 2 - 5 - 4
cp = 4 - 6 - 1
cpzp = 6 - 4 - 5

nicht OK

apz = 0 - 2 - 6 - Name - ...
p = 8 - 3 - 11
apzp = 1 - 5 - 3 - Name - ...

apzp = 1 - 5 - 3 - Name - ...

Quelle: T. Beth, "Sichere offene Datennetze", Spektrum der Wissenschaft, Mai 1995, S. 46-55

Abwehr einer man-in-the-middle attack mit Hilfe einer Signatur

Trustcenter überprüfen zunächst die Identität des Nutzers (z.B. Ausweiskontrolle) und generieren ein elektronisches Zertifikat. Dieses beinhaltet u.a. (siehe §7 Signaturgesetz)

- den Namen des Ausstellers,
- Informationen über die Identität des Inhabers,
- Mail-Adresse sowie
- die digitale Signatur des Ausstellers.

Vor allem aber bestätigt das Zertifikat, dass der öffentliche Schlüssel wirklich der Person gehört. Er ist ein eindeutiges Merkmal zur Identifizierung.

(praktischer Ablauf: siehe Funkschau 23/2001, S. 26/27)

Das Trustcenter erzeugt das Signaturschlüsselpaar und lädt es auf eine Chipkarte. Diese wird anschließend an den Antragsteller übergeben. Zusätzlich erhält er eine zur Chipkarte gehörende Geheimnummer (PIN). Diese Chipkarte nutzt der Kunde bei rechtsverbindlichen Erklärungen auf elektronischem Wege.

Quelle: Funkschau 1/2002, S. 30 und Funkschau 23/2001, S. 24ff
siehe auch: K. Fuhrberg „Internetsicherheit“, Hanser-Verlag 1998, S. 92ff

Soll ein Dokument digital signiert werden, verknüpft der Absender das zu versendende Dokument mit seinem privaten Schlüssel, indem er die Chipkarte in den Chipkartenleser steckt und in der entsprechenden Software den Befehl „Signieren" anklickt. Das so erzeugte Dokument dient als digitale Signatur und wird an das ursprüngliche Dokument angehängt. Die beiden Teile werden anschließend zusammen übermittelt.

Der Empfänger des so signierten Dokuments kann den Inhalt sofort im Klartext lesen. Allerdings besteht noch keine Gewähr für den richtigen Absender und den korrekten Inhalt des Dokuments. Um dies zu prüfen, muss der Empfänger die digitale Signatur mit dem öffentlichen Schlüssel des Absenders entschlüsseln. Dazu muss er im Besitz des öffentlichen Schlüssels des Absenders sein, der beispielsweise künftig in einem Verzeichnis, ähnlich dem Telefonbuch, eingesehen werden kann.

Quelle: Funkschau 1/2002, S. 30
siehe auch: K. Fuhrberg „Internetsicherheit“, Hanser-Verlag 1998, S. 92ff

- Signatur am besten auf einer Karte, die jeder schon hat -> EC-Karte !
- Bei der nächsten Umstellung der EC-Karten Ende 2004 sollen alle Karten mit einem signaturfähigen Chip versehen werden.
- gleiche Planung in Österreich
- dort sind ca. 10 Cent pro Transaktion vorgesehen
- Bundesinnenministerium entwickelt Geschäftsmodell für die Abwicklung von Behörden-Aktionen

Quelle: c't 12/2003, S. 42