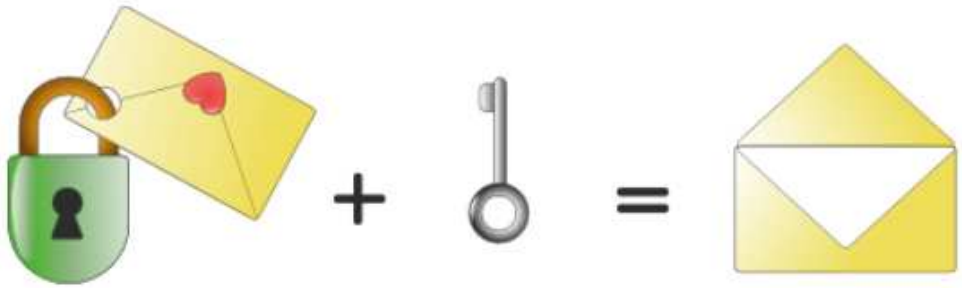


Verschlüsselung

Kleine „Schlüsselkunde"

Geheimnisse

- Bank: Kontostand
- Politik: Verträge über Unterstützung
- Know-How: Wie funktioniert …
- Liebesbriefe
- Wer wird der nächste OVV ?
- Geburtstags-Überraschung
- und so weiter …

Die 4 Ziele der Kryptographie

- **Vertraulichkeit der Nachricht:**
  Nur der Empfänger soll in der Lage sein,
  den Inhalt der Nachricht zu lesen.

- **Datenintegrität der Nachricht:**
  Der Empfänger soll in der Lage sein festzustellen,
  ob die Nachricht während ihrer Übertragung **verändert** wurde.

- **Authentifizierung:**
  Der Empfänger soll überprüfen können,
  ob die Nachricht tatsächlich vom angegebenen **Absender** stammt.

- **Verbindlichkeit:**
  Der Absender kann NICHT bestreiten,
  dass die Nachricht von **ihm** kommt.

Wolfgang sagt auf 2m: „Hallo Armin, hier ist Andreas(!) am Mikro:
Ich zahle Dir beim nächsten OV-Abend ein Bier.“

Was will der Hacker ?

- Wer schickt an wen ? Wer redet mit wem ? **Wann ?**
  Rolf Maier hat gestern 5 Mal mit dem Betriebsrat telefoniert.
- Welche Übertragung ?
  Reiter / Kurier / Brief im Kleid der Prinzessin /
  öffentliche Post / Telefon / Funk / Frequenz …
- Wie verschlüsselt ?
  Welches Verfahren wurde benutzt: Vertauschen, Enigma, …
- Das Chiffrat – besser den Klartext
  Die verschlüsselte Nachricht.
- Möglichst schnell !

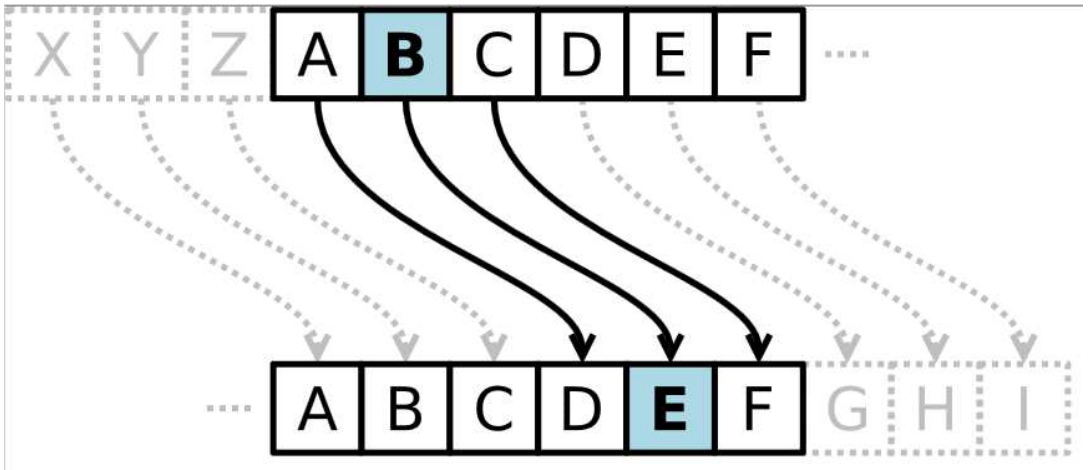
Symmetrische Verfahren

Substitution

wurde bereits vom Feldherrn Julius Cäsar angewandt:

- Buchstabe um 3 verschoben:
  A=D, B=E, C=F, …

  DL1WOL → GO4ZRO



- **Einfach zu knacken:**
  Häufigkeit der Buchstaben
  oder Inhalt: „…Wetterbericht…“

Symmetrische Verfahren

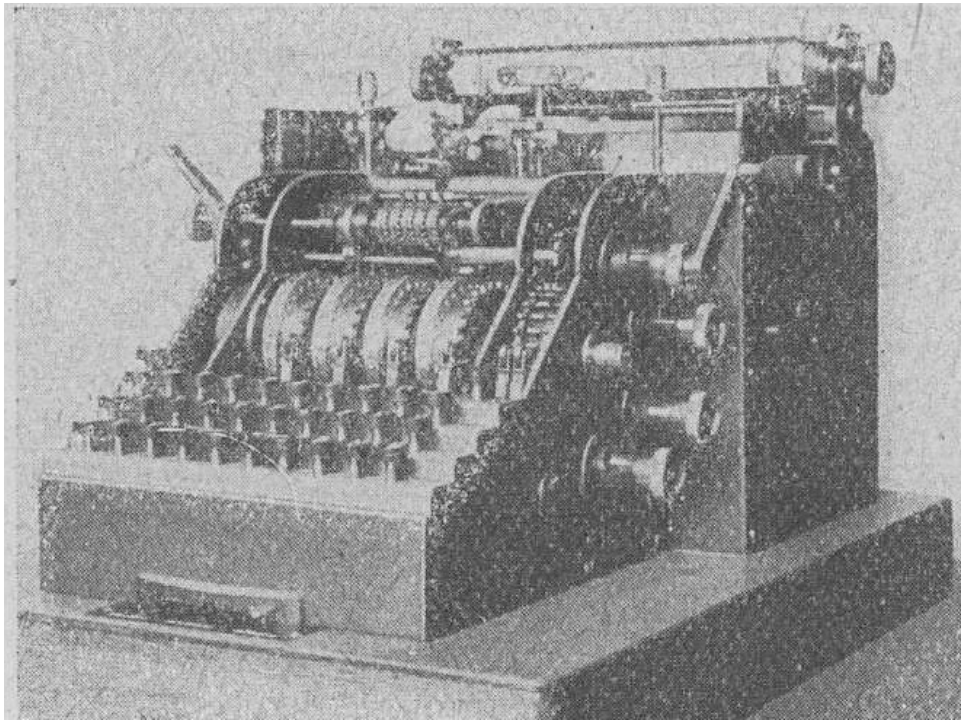
Substitution

Das Entschlüsseln benötigt etwas Zeit.

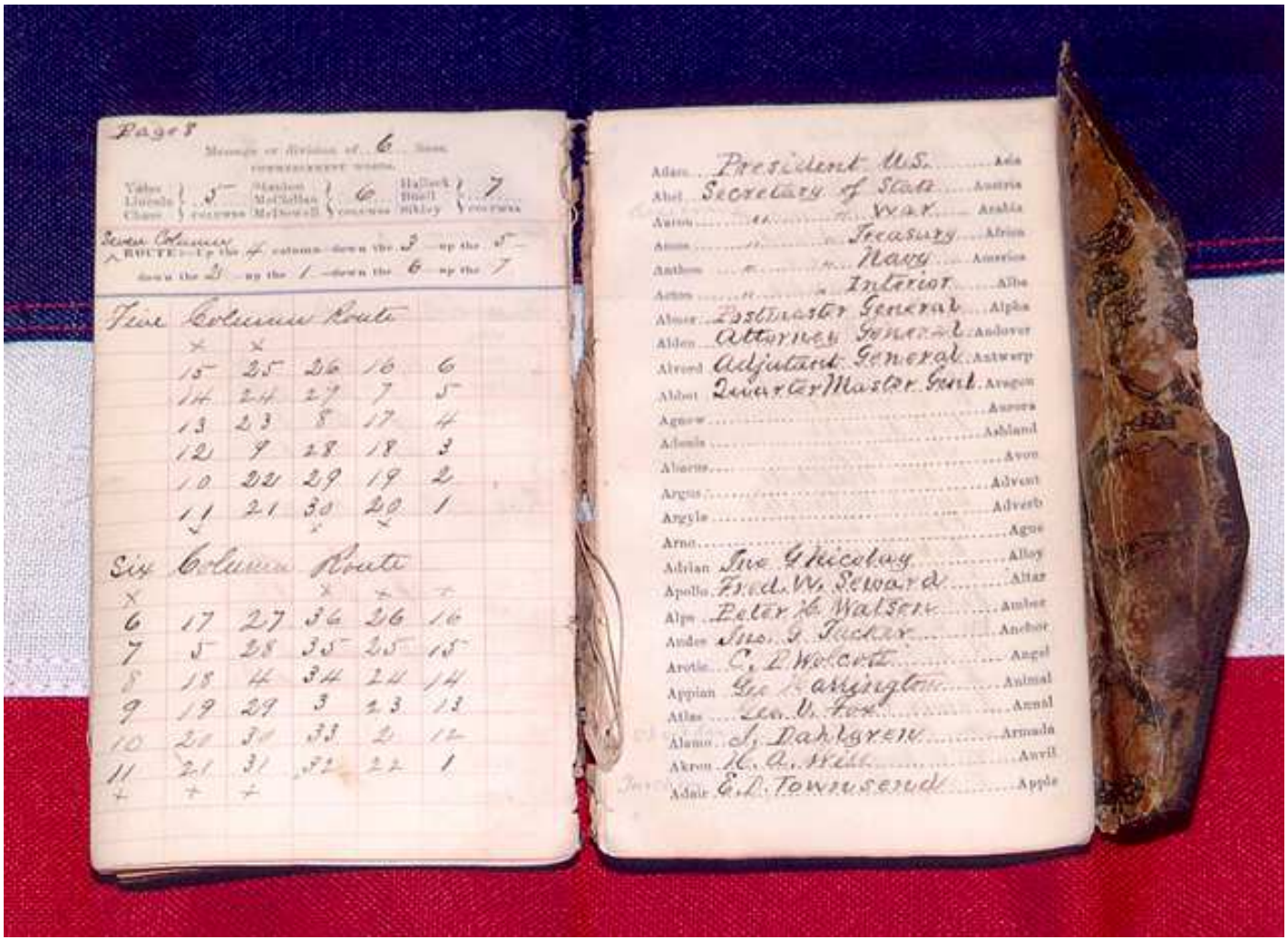
- Mein Empfänger soll meine Nachricht "sofort" lesen!
  (so bald wie nur möglich)

- Alle Anderen "niemals" !
  (oder zumindest NICHT in den nächsten 5 Jahren o.ä.).

→ Mehrfache Ersetzen /
Über(ver)schlüsselung
z. Bsp. Enigma



Kryptographisches Codebuch aus dem amerikanischen Bürgerkrieg



Transposition

Tabelle 8 * 6 Block:

Klartext (links → rechts):

„Bundesamt für Sicherheit in der Informationstechnik“

B	U	N	D	E	S	A	M
T	F	Ü	R	S	I	C	H
E	R	H	E	I	T	I	N
D	E	R	I	N	F	O	R
M	A	T	I	O	N	S	T
E	C	H	N	I	K		

Chiffrat (oben → unten):

„BTEDME UFREAC NÜHRTH DREIIN ESINOI SITFNK ACIOS MHNRT“

Heute

Kerckhoffs' Prinzip:

- das Verschlüsselungs-Verfahren kennt jeder.
- die verschlüsselte Nachricht ist offen (Postkarte).
- **Nur der Schlüssel ist geheim.**

Aber:

- Wie kommt der Schlüssel zum Empfänger ?

Ein Versuch dazu !

Praktische Versuche

a.) Ware in Kiste.
→ Ware wird geklaut.

b.) Ware in Kiste und absperren.
→ Geht nicht:
Empfänger hat keinen Schlüssel.

c.) Schlüssel an Empfänger:
→ Schlüssel wird kopiert.
→ Ware wird ausgetauscht !

d.) Das Zwei-Schloss-Verfahren:
→

Etwas Mathematik

Bitte mit dem Taschenrechner(!) ausrechnen:

5 * 7 = x	x = ?	
250 = a * a * a * b	a = ?	b = ?
247 = c * d	c = ?	d = ?
256793 = e * f	e = ?	f = ?

Etwas Mathematik

Hier die Lösung:

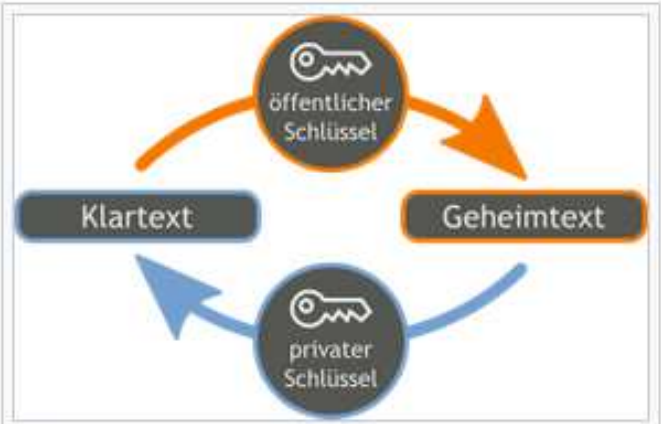
5 * 7 = x	x = 35		
250 = a * a * a * b	a = 5	b = 2	
247 = c * d	c = 13	d = 19	
256793 = e * f	e = 523	f = 941	

Lösung geht nur über ausprobieren !

Zwei Primzahlen (je 10 Stellen) ergeben 20 stellige Zahl.

Asymmetrisches Verfahren

Bei der symmetrischen Verschlüsselung dient der Schlüssel auch zur Entschlüsselung



Bei der asymmetrischen Verschlüsselung gibt es zwei unterschiedliche Schlüssel, den öffentlichen Schlüssel zur Verschlüsselung und den privaten Schlüssel zur Entschlüsselung

Zwei unterschiedliche Schlüssel:

Mit dem einen wird verschlüsselt.

Mit dem anderen entschlüsselt.

Asymmetrisches Verfahren

Bob:

hat einen öffentlichen Schlüssel
und hat einen privaten Schlüssel.

Alice:

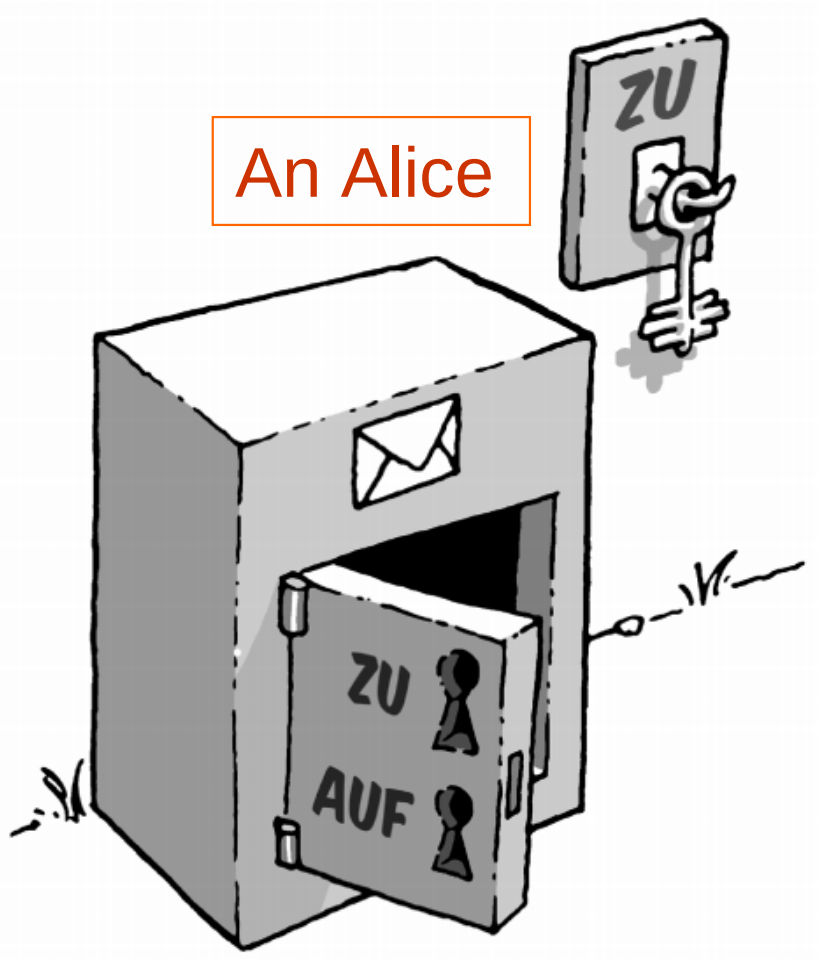
hat einen **öffentlichen** Schlüssel
und hat einen **privaten** Schlüssel.

Asymmetrisches Verfahren

Bob schreibt Alice eine E-Mail.

Er nimmt den
öffentlichen Schlüssel von Alice
und verschlüsselt seine E-Mail.

Er sendet die verschlüsselte
E-Mail an Alice.

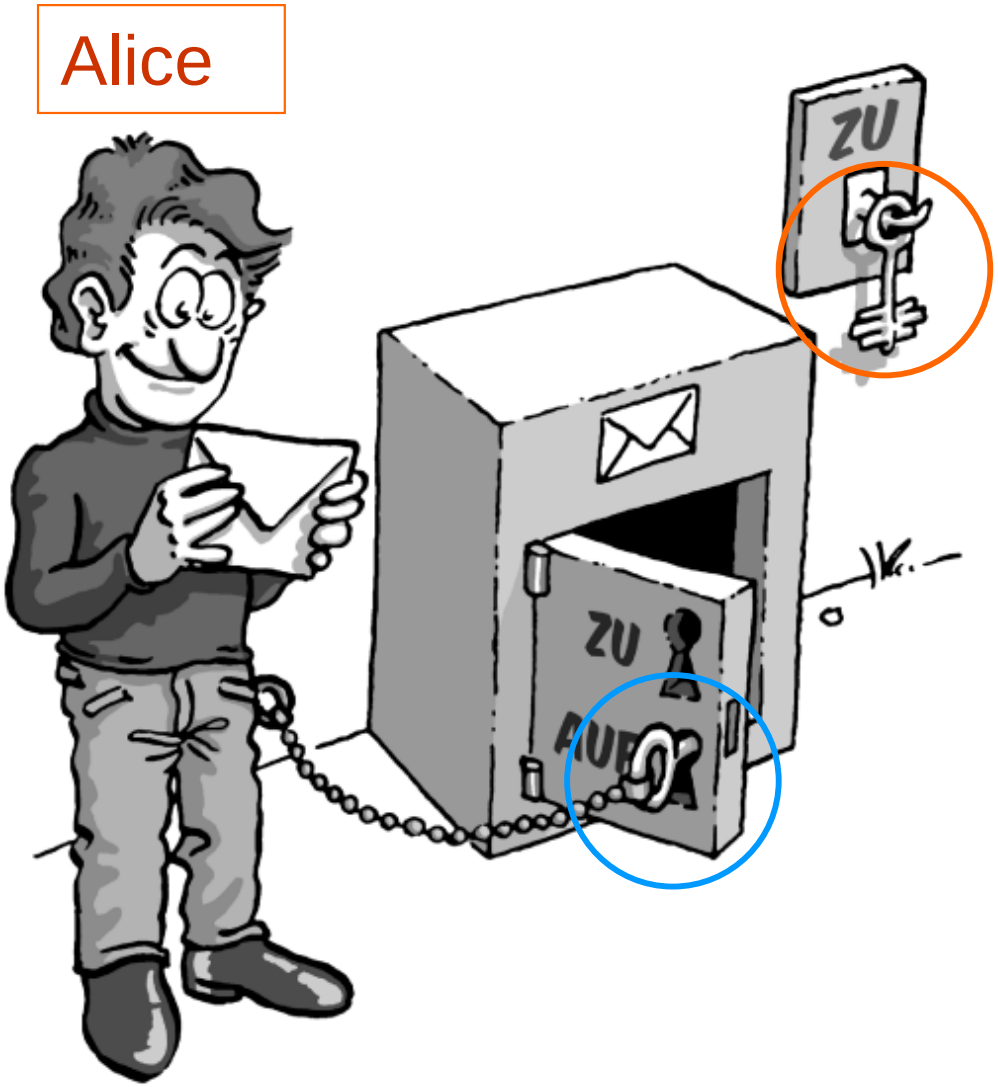


Asymmetrisches Verfahren

Alice

hat einen öffentlichen Schlüssel
und hat einen privaten Schlüssel.

Alice nimmt ihren privaten Schlüssel und entschlüsselt die E-Mail.

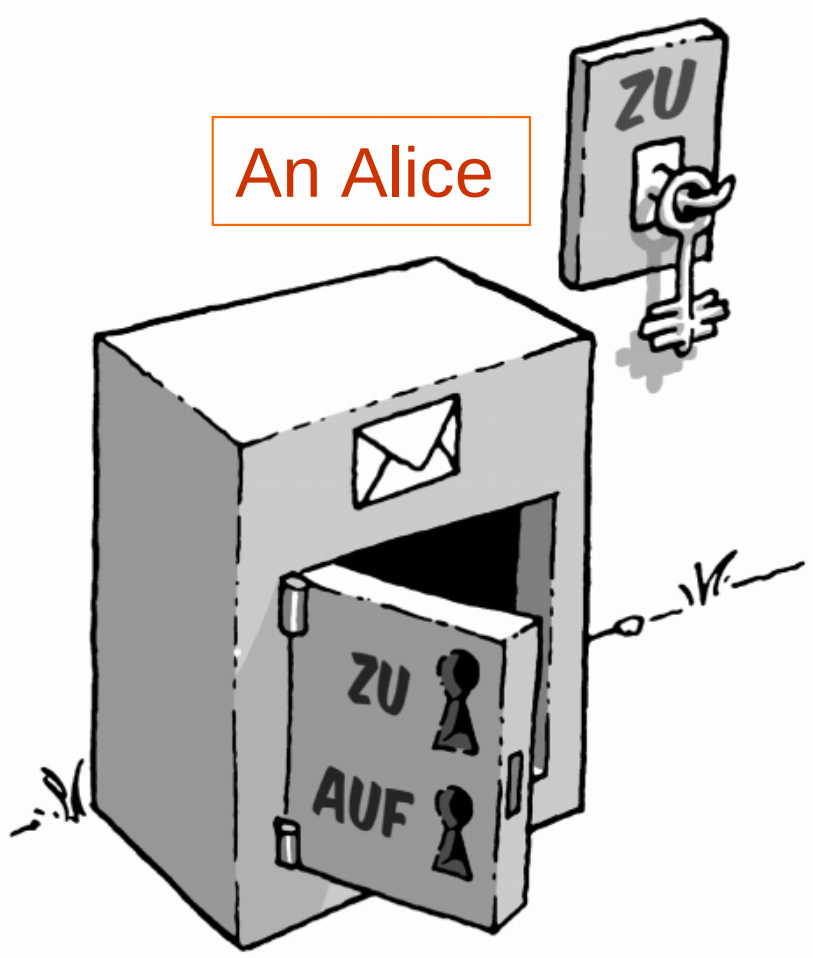


Asymmetrisches Verfahren

Wichtig dabei:

Möglichst viele Leute sollen den öffentlichen Schlüssel von Alice kennen!

Alice soll diesen überall verteilen. Dann kann niemand anderes sagen: Er sei Alice.



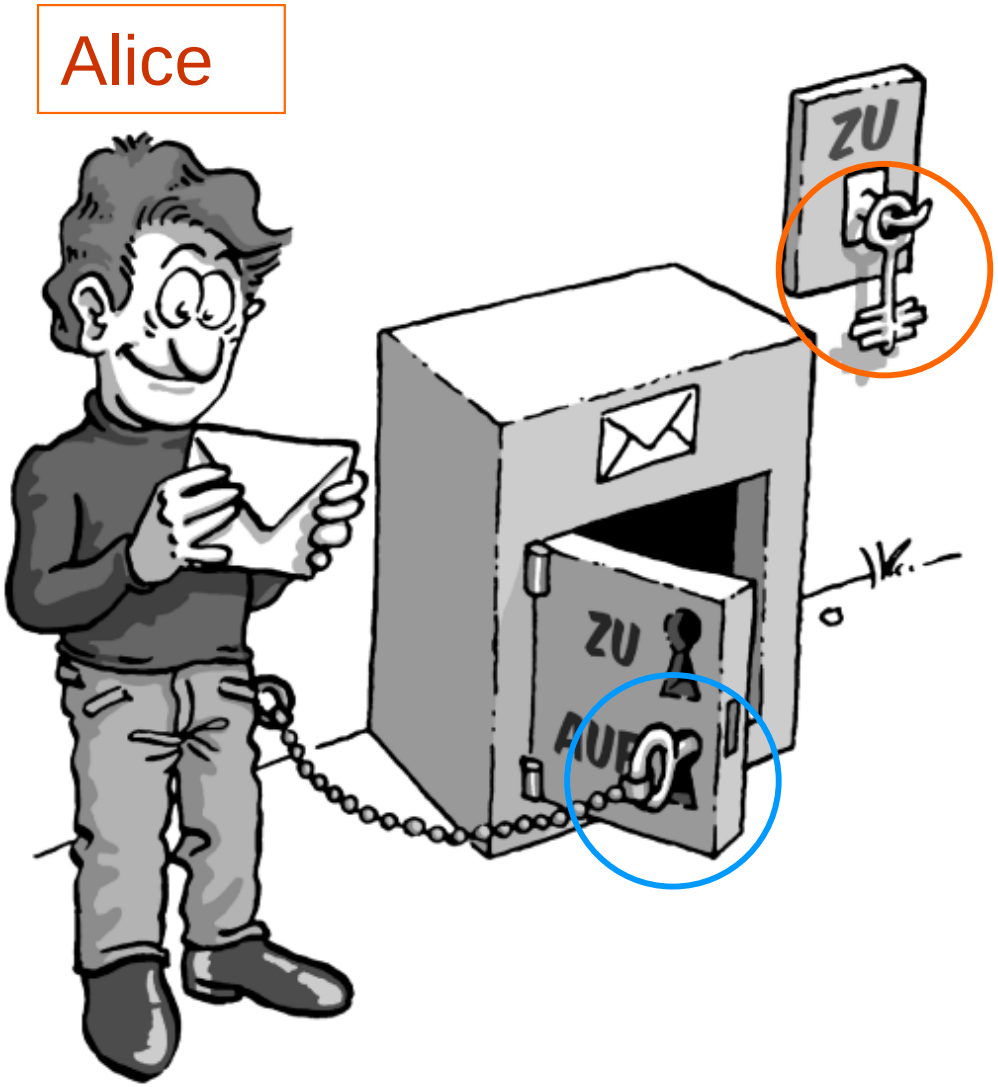
Asymmetrisches Verfahren

Alice

Der privaten Schlüssel von Alice kennt nur sie alleine**.**

Dieser ist mit einem Passwort geschützt.

Fragen hierzu?



Wie Unterschreiben?

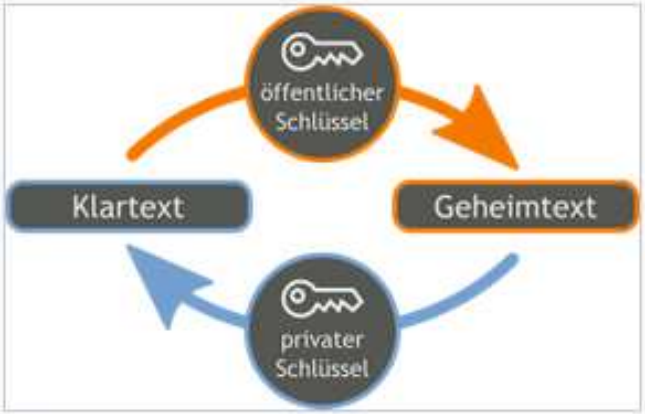
Zwei unterschiedliche Schlüssel:

Mit dem einen wird verschlüsselt.

Mit dem anderen entschlüsselt.

Das geht auch andersherum:

5 * 7 = 7 * 5



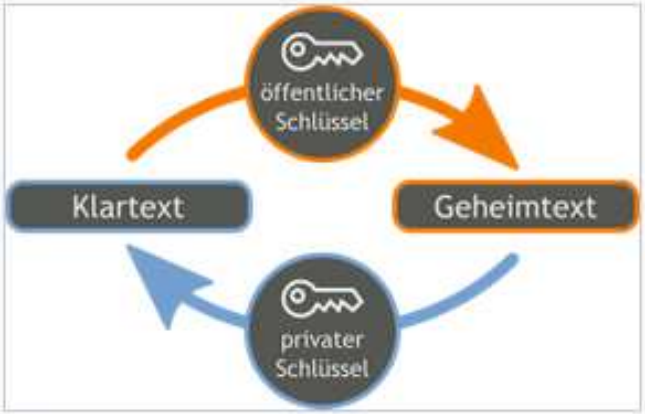
Bei der asymmetrischen Verschlüsselung gibt es zwei unterschiedliche Schlüssel, den öffentlichen Schlüssel zur Verschlüsselung und den privaten Schlüssel zur Entschlüsselung

Wie Unterschreiben?

Bob erklärt öffentlich, dass er Präsident werden will. Er schreibt eine (offene) E-Mail an alle seine Freunde.

Und er hängt eine kleine Datei an, mit seinem Namen, die er mit seinem privaten Schlüssel verschlüsselt!

Nun kann jeder mit Bobs öffentlichen Schlüssel diese Unterschrift überprüfen / entschlüsseln.



Bei der asymmetrischen Verschlüsselung gibt es zwei unterschiedliche Schlüssel, den öffentlichen Schlüssel zur Verschlüsselung und den privaten Schlüssel zur Entschlüsselung

Ende

Ach ja:

Das Verfahren nennt sich

Pretty Good Privacy / PGP

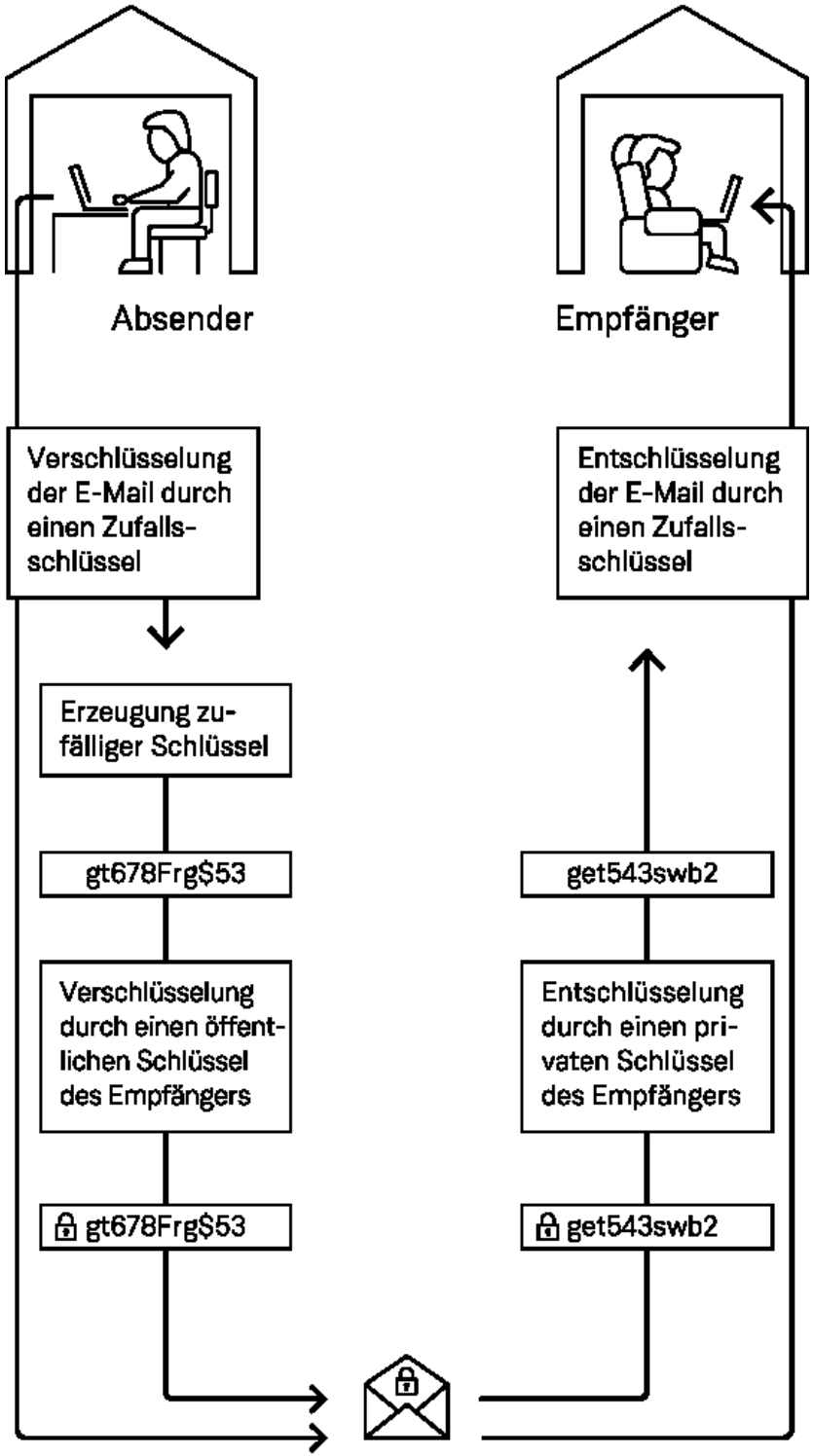
und wurde von einem

Philip R. Zimmermann in USA

* 12.02.1954

erfunden.

Phil Zimmermann


Absender
Empfänger
Verschlüsselung der E-Mail durch einen Zufalls-schlüssel
Entschlüsselung der E-Mail durch einen Zufalls-schlüssel
Erzeugung zu-fälliger Schlüssel
gt678Frg$53
get543swb2
Verschlüsselung durch einen öffent-lichen Schlüssel des Empfängers
Entschlüsselung durch einen pri-vaten Schlüssel des Empfängers
gt678Frg$53
get543swb2