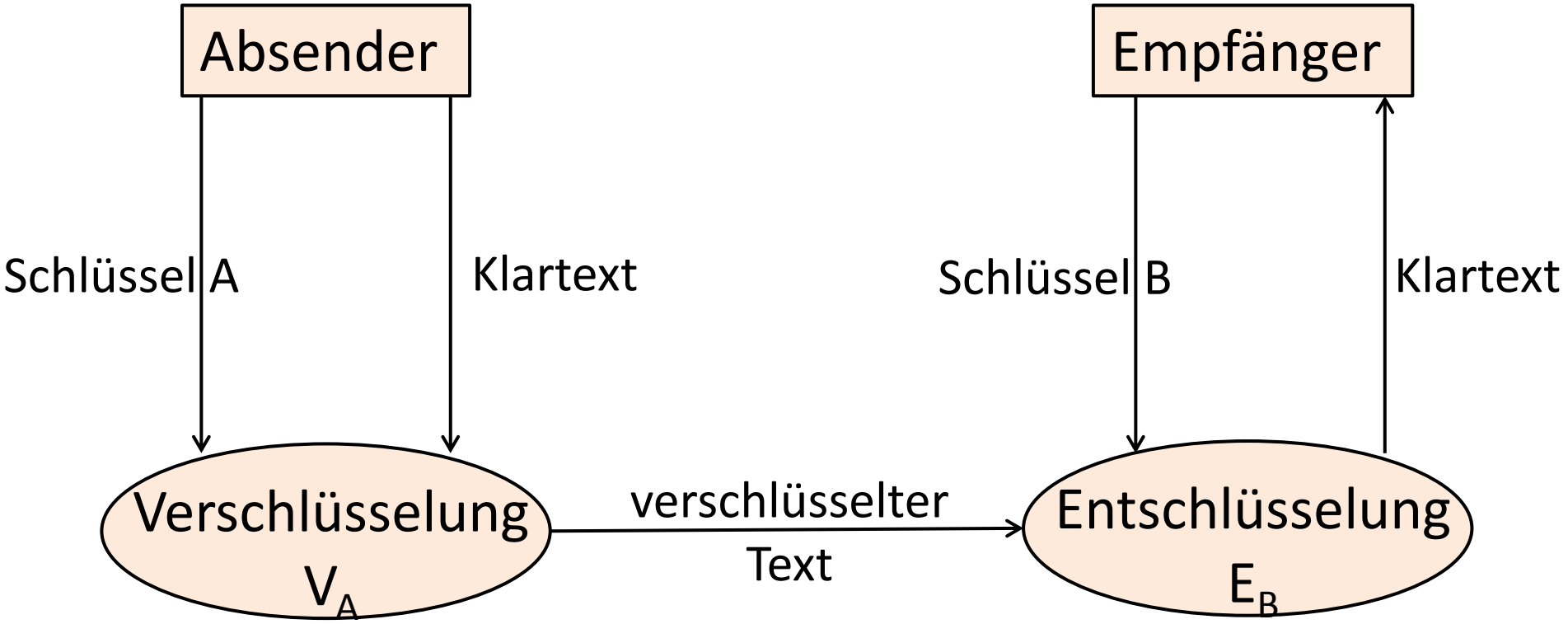
Annahme: Verschlüsselung sicher

Wurde mit dem Kommunikationspartner ein Schlüssel ausgetauscht, kann

- kein anderer die verschlüsselte Nachricht lesen,
- keiner die Nachricht verfälschen,
- keiner die Nachricht abfangen und durch eine eigene ersetzen.

Problem: Schlüsselaustausch
per Post?

Ziel:
Sichere Kommunikation mit unbekanntem Partner



Für die Nachricht N gilt: $E_B(V_A(N)) = N$

Wird zum Ver- und Entschlüsseln derselbe Schlüssel (oder ein leicht daraus berechenbarer) verwendet (A=B), spricht man von **symmetrischer** Verschlüsselung.

Asymmetrische Verschlüsselung: A ≠ B

Falls $E_B(V_A(N)) = N = V_A(E_B(N))$ gilt, heißt der Schlüssel **kommutativ**.

Jens Gallenbacher: Abenteuer Informatik
ASYM-Kodierer

Schlüssel A: EMU
Schlüssel B: FIR

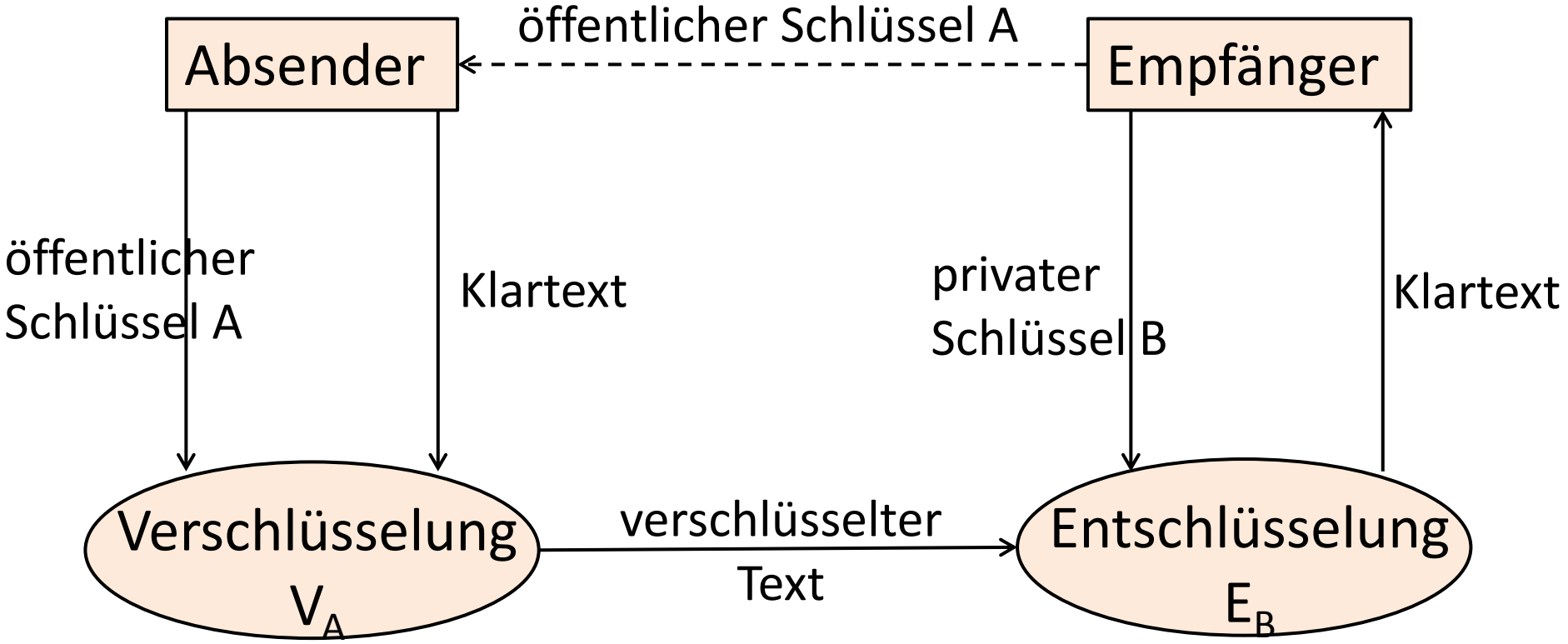
E	M	U	E	M	U	E	M	U	E
I	N	F	O	R	M	A	T	I	K
Y	J	U	C	Q	B	F	F	Q	H

Annahme:
Die asymmetrische Verschlüsselung ist so gut, dass aus einem Schlüssel und der verschlüsselten Nachricht nicht der passende Gegenschlüssel berechnet werden kann.

Einwegfunktionen:
In eine Richtung einfach zu berechnen, Umkehrung schwierig.

z.B. schwierige Richtung:
Zerlege 71302769 in Primzahlen
einfache Richtung: Berechne $7489 \cdot 9521$

Einwegfunktionen mit Falltür:
Umkehrung ist einfach, wenn man eine zusätzliche Information besitzt (Schlüssel).



Der öffentliche Schlüssel wird bekannt gegeben, der private dagegen keinesfalls.

Rollenspiel:
Nach Gallenbacher: Abenteuer Informatik
Kurt: Kunde, Anna: Anbieter, Bob: der Böse im Internet

- Wie kann mit asymmetrischer Verschlüsselung Kurt Nachrichten verschlüsselt übermitteln?
- Wie kann verhindert werden, dass Bob die Bestellung abfängt und eine fingierte Nachricht "Bestellung erhalten" an Kurt schickt?

Wenn jemand ein Schlüsselpaar besitzt und einen Schlüssel als öffentlichen Schlüssel bekannt macht, kann ihm jeder geheime Nachrichten schicken, er weiß aber nicht, ob der Absender echt ist.
Er selbst kann keine geheimen Nachrichten versenden, aber seine Nachrichten authentifizieren.

- Angriff:
  Statt des echten öffentlichen Schlüssels wird Kurt ein falscher öffentlicher Schüssel zugespielt, zu dem Bob den privaten Schlüssel besitzt. → Carl

Carl hat vorab allen Beteiligten seinen öffentlichen Schlüssel zukommen lassen. Er bietet an, die öffentlichen Schlüssel anderer auf Anfrage zu versenden.

Kurt fragt nun bei Carl nach dem Schlüssel von Anna.
Bob kann die Nachricht nicht lesen. Kurt wartet auf authentifizierte Antwort von Carl. Nun sicher?

- Angriff:
  Bob kann sich denken, dass die verschlüsselte Nachricht an Carl eine Schlüsselanfrage ist. Er wirft die Nachricht weg und fragt bei Carl nach seinem eigenen, öffentlichen Schlüssel. Dieser wird ihm – von Carl authentifiziert – zugeschickt. Er leitet die Nachricht weiter an Kurt.

Lösung:
Schlüssel und Schlüsseleigentümer werden immer zusammen übermittelt!

Zertifizierungsstellen (Certification Authority, CA)
geben digitale Zertifikate heraus, die einen öffentlichen Schlüssel einer Person oder Organisation zuordnen.
Der öffentliche Schlüssel der Zertifizierungsstelle ist bekannt (z.B. im Browser hinterlegt.)

Kurt kann nun geheime Nachrichten an Anna versenden, Anna kann authentifizierte Nachrichten an Kurt versenden, die aber jeder lesen kann.
Soll Anna ebenfalls verschlüsselte Nachrichten versenden können, muss Kurt ihr vorher einen verschlüsselten Schlüssel mitteilen.