Wie bleibt unser Geheimnis geheim?

MuT, Wintersemester 2009/10

Jan Tobias Mühlberg & Johannes Schwalb
muehlber@swt-bamberg.de

Lehrstuhl: Prof. Lüttgen, Softwaretechnik und Programmiersprachen
http://swt-bamberg.de/

04. November 2009

Motivation

- . . . bestimmt hast du ein Geheimnis, das niemand erfahren darf . . .

- Themen rund um die *Kryptographie*:
  - Geheime Nachrichten verschicken
  - Codes knacken
  - Echtheit von Nachrichten

Skytale

- Vor 2500 Jahren von Lysander eingesetzt (Peloponnesischer Krieg)
- Stab senkrecht halten, Nachricht von oben nach unten schreiben
- Band abwickeln: fertig

Begriffe

- **Klartext**:
- **Geheimtext**:
- **Schlüssel**:
- **Chiffre**:
- **Verschlüsseln**:
- **Entschlüsseln**:

Begriffe

- **Klartext**: *„SUSI IST VERLIEBT“*
- **Geheimtext**:
- **Schlüssel**:
- **Chiffre**:
- **Verschlüsseln**:
- **Entschlüsseln**:

Begriffe

- **Klartext**: *„SUSI IST VERLIEBT“*
- **Geheimtext**: *„svuesril iiesbtt “*
- **Schlüssel**:
- **Chiffre**:
- **Verschlüsseln**:
- **Entschlüsseln**:

Begriffe

- **Klartext**: *„SUSI IST VERLIEBT“*
- **Geheimtext**: *„svuesril iiesbtt “*
- **Schlüssel**: der Stab bzw. dessen Umfang
- **Chiffre**:
- **Verschlüsseln**:
- **Entschlüsseln**:

Begriffe

- **Klartext**: *„SUSI IST VERLIEBT“*
- **Geheimtext**: *„svuesril iiesbtt “*
- **Schlüssel**: der Stab bzw. dessen Umfang
- **Chiffre**: das Verfahren
- **Verschlüsseln**: Text schreiben und abwickeln
- **Entschlüsseln**: aufwickeln und lesen

Caesar-Chiffre

- *„. . . wenn etwas Geheimes zu überbringen war, schrieb er in Zeichen, das heißt, er ordnete die Buchstaben so, daß kein Wort gelesen werden konnte: Um diese zu lesen, tauscht man den vierten Buchstaben, also D für A aus und ebenso mit den restlichen.“*

  — Sueton, um 100

Caesar-Chiffre

- Klar- und Geheimtextalphabete für die Caesar-Chiffre:

Klartext:	a	b	c	d	e	f	g	h	i	j	k	l	m
Geheimtext:	D	E	F	G	H	I	J	K	L	M	N	O	P
Klartext:	n	o	p	q	r	s	t	u	v	w	x	y	z
Geheimtext:	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

- Ein Beispiel:

DQJULIILPPRUJHQJUDXHQ $\approx$ angriffimmorgengrauen

Kryptoanalyse

- Entschlüsseln von verschlüsselten Nachrichten ohne den Schlüssel zu kennen:

  ☞ *Durchprobieren* aller Schlüssel

  ☞ *Statistische* Methoden

☞ Oft noch einfacher: *Social Engineering*

Kryptoanalyse: Durchprobieren

- Wie groß ist denn der *Schlüsselraum* der Skytale und der Caesar-Chiffre?
- Moderne Chiffren: zwischen 10^{40} und 10^{80} Möglichkeiten, je nach Anwendungsgebiet auch mal mehr

Kryptoanalyse: Statistik

- Aufgabe: MYHUG BUK ZBZP ZPUK PT RPUV.

Kryptoanalyse: Statistik

- Aufgabe: MYHUG BUK ZBZP ZPUK PT RPUV.
- Buchstaben haben im Deutschen unterschiedliche Häufigkeit
- Erst kurze Worte untersuchen, dann schauen ob sich lange Worte entschlüsseln lassen

Kryptoanalyse: Statistik

- Aufgabe: MYHUG BUK ZBZP ZPUK PT RPUV.
- Buchstaben haben im Deutschen unterschiedliche Häufigkeit
- Erst kurze Worte untersuchen, dann schauen ob sich lange Worte entschlüsseln lassen
- Lösung: Caesar mit 7; *„franz und susi sind im kino.“*

Social Engineering

- Geburtstage und Namen sind schlechte Schlüssel!

- *„Hallo, ich bin Franz Mustermann und ich habe mein Passwort vergessen. Können Sie mir bitte ein neues geben?“*
- *„Hallo, ich bin von der Firma X und wir brauchen mal Ihr Passwort um ihren Telefonanschluss zu überprüfen.“*

Vigenère-Chiffre

- Nach Blaise de Vigenère, frz. Diplomat, 1523–1596
- Polyalphabetische Chiffre: jeder Buchstabe wird anders verschoben $\longrightarrow$ es gibt mehrere Geheimtextalphabete
- Schlüssel ist eine Buchstabengruppe beliebiger Länge

Vigenère-Chiffre

- Schlüsselbuchstaben = Zeile, Klartextbuchstaben = Spalte
- Beispiel: Klartext ist *„cafe“*, Schlüssel ist *„bad“*
- Geheimtext ist:

A	B	C	D	E	F	G	H
B	C	D	E	F	G	H	I
C	D	E	F	G	H	I	J
D	E	F	G	H	I	J	K
E	F	G	H	I	J	K	L
F	G	H	I	J	K	L	M
G	H	I	J	K	L	M	N
H	I	J	K	L	M	N	O

Vigenère-Chiffre

- Schlüsselbuchstaben = Zeile,
  Klartextbuchstaben = Spalte
- Beispiel: Klartext ist „*cafe*“,
  Schlüssel ist „*bad*“
- Geheimtext ist: D. . .

A	B	C	D	E	F	G	H
B	C	D	E	F	G	H	I
C	D	E	F	G	H	I	J
D	E	F	G	H	I	J	K
E	F	G	H	I	J	K	L
F	G	H	I	J	K	L	M
G	H	I	J	K	L	M	N
H	I	J	K	L	M	N	O

Vigenère-Chiffre

- Schlüsselbuchstaben = Zeile,
  Klartextbuchstaben = Spalte
- Beispiel: Klartext ist „*cafe*“,
  Schlüssel ist „*bad*“
- Geheimtext ist: DA. . .

A	B	C	D	E	F	G	H
B	C	D	E	F	G	H	I
C	D	E	F	G	H	I	J
D	E	F	G	H	I	J	K
E	F	G	H	I	J	K	L
F	G	H	I	J	K	L	M
G	H	I	J	K	L	M	N
H	I	J	K	L	M	N	O

Vigenère-Chiffre

- Schlüsselbuchstaben = Zeile,
  Klartextbuchstaben = Spalte
- Beispiel: Klartext ist „*cafe*“,
  Schlüssel ist „*bad*“
- Geheimtext ist: DAI. . .

A	B	C	D	E	F	G	H
B	C	D	E	F	G	H	I
C	D	E	F	G	H	I	J
D	E	F	G	H	I	J	K
E	F	G	H	I	J	K	L
F	G	H	I	J	K	L	M
G	H	I	J	K	L	M	N
H	I	J	K	L	M	N	O

Vigenère-Chiffre

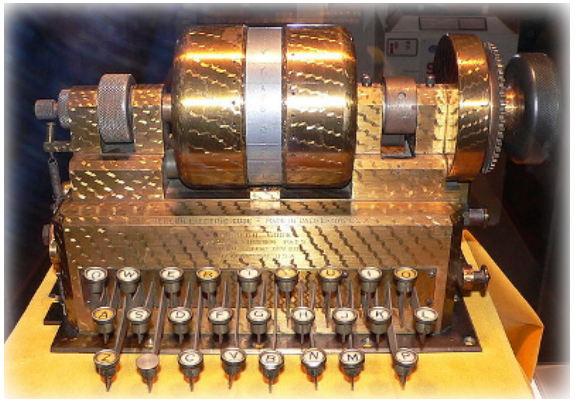
- Schlüsselbuchstaben = Zeile,
  Klartextbuchstaben = Spalte
- Beispiel: Klartext ist „*cafe*“,
  Schlüssel ist „*bad*“
- Geheimtext ist: DAIF

A	B	C	D	E	F	G	H
B	C	D	E	F	G	H	I
C	D	E	F	G	H	I	J
D	E	F	G	H	I	J	K
E	F	G	H	I	J	K	L
F	G	H	I	J	K	L	M
G	H	I	J	K	L	M	N
H	I	J	K	L	M	N	O

Pause!

Mechanische Verschlüsselung

Kryha, etwa 1920, Deutschland



Hebern-Maschine, 1917, USA

M-209, etwa 1930, Schweden und USA

Enigma, 1. und 2. Weltkrieg, Deutschland

Und was kann man noch so damit machen?

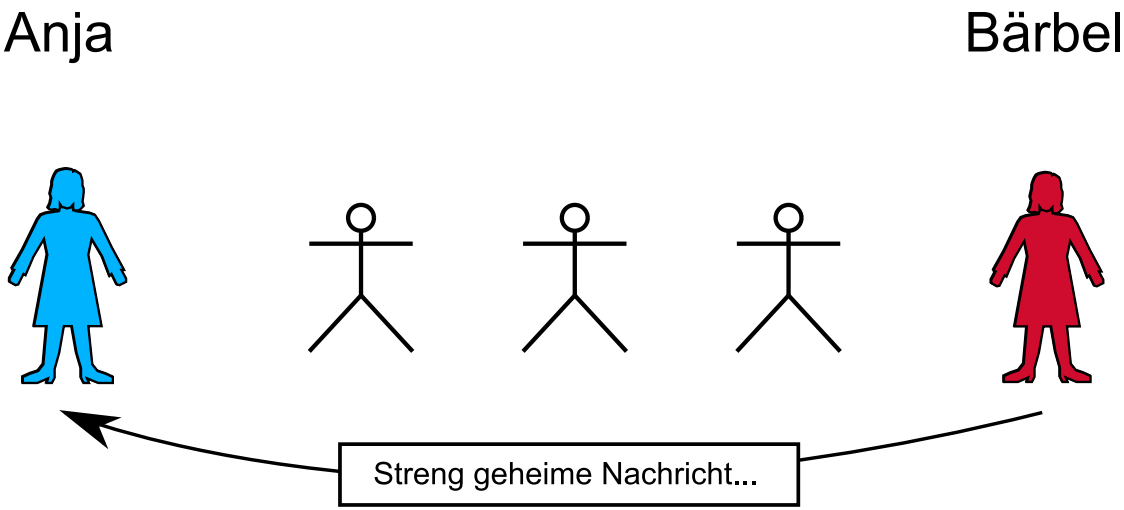
Und was kann man noch so damit machen?

- ☞ Schlüssel austauschen
- ☞ *„Echtheit“* von Nachrichten
- ☞ Wissen, mit wem man redet

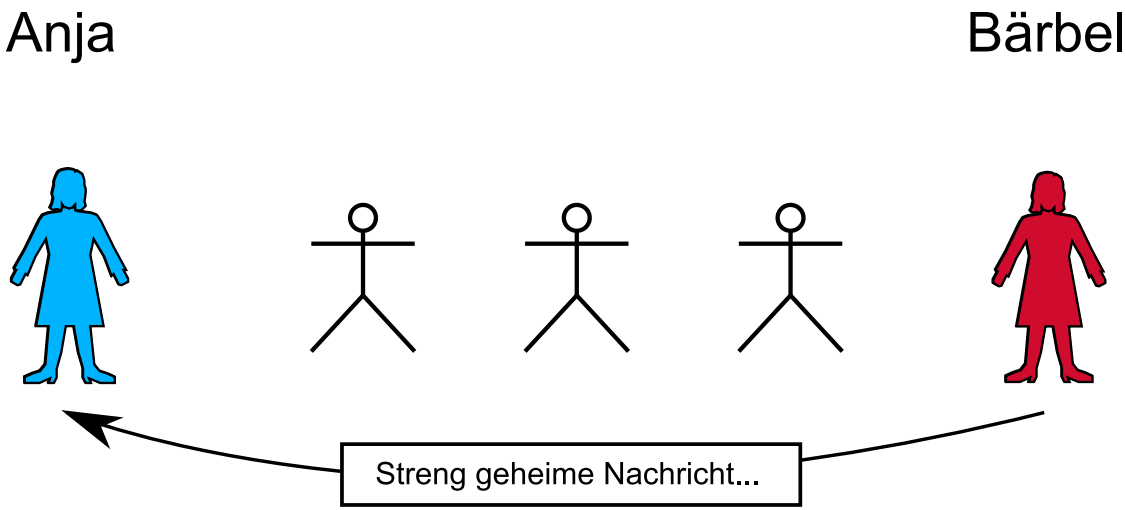
Authentifizierung

- Rede ich mit der *„richtigen“* Person?
- Stammt eine Nachricht tatsächlich vom angegebenen Absender?
- Traditionell:
  - Wissen (Losung)
  - Besitz (Schlüssel)
  - Biometrie (Fingerabdruck, Unterschrift)
- Aber: Über weite Entfernungen?

Authentifizierung



Authentifizierung

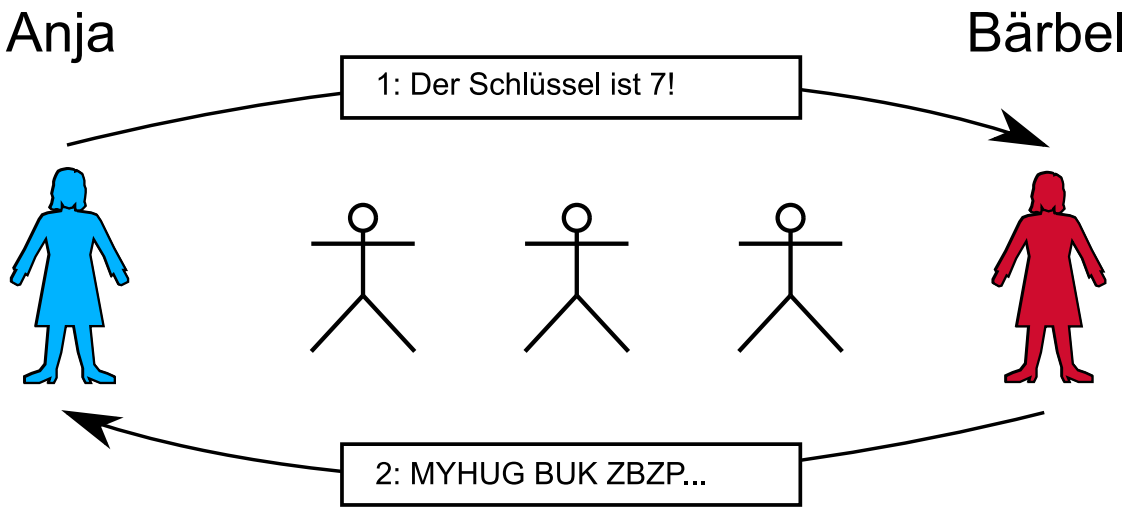


- Nachricht ist unverschlüsselt

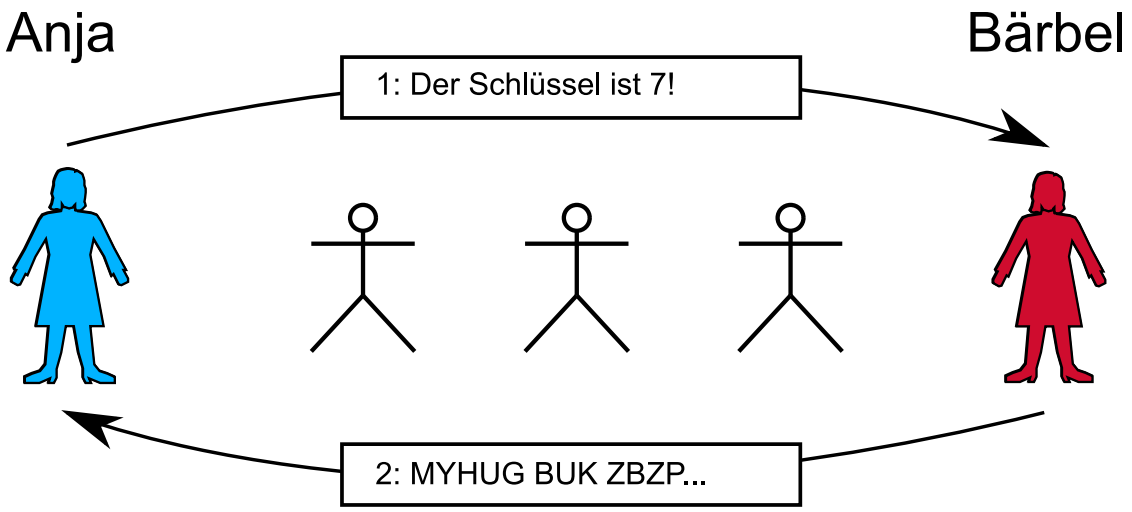
☞ Jeder kennt Inhalt der Nachricht

☞ Nachricht kann verändert worden sein

Authentifizierung



Authentifizierung



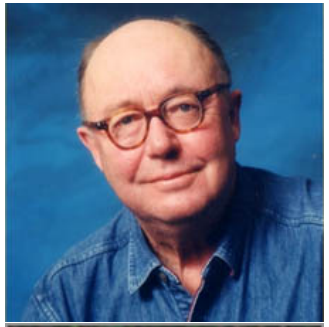
- Jeder kennt den Schlüssel

☞ Jeder kennt Inhalt der Nachricht

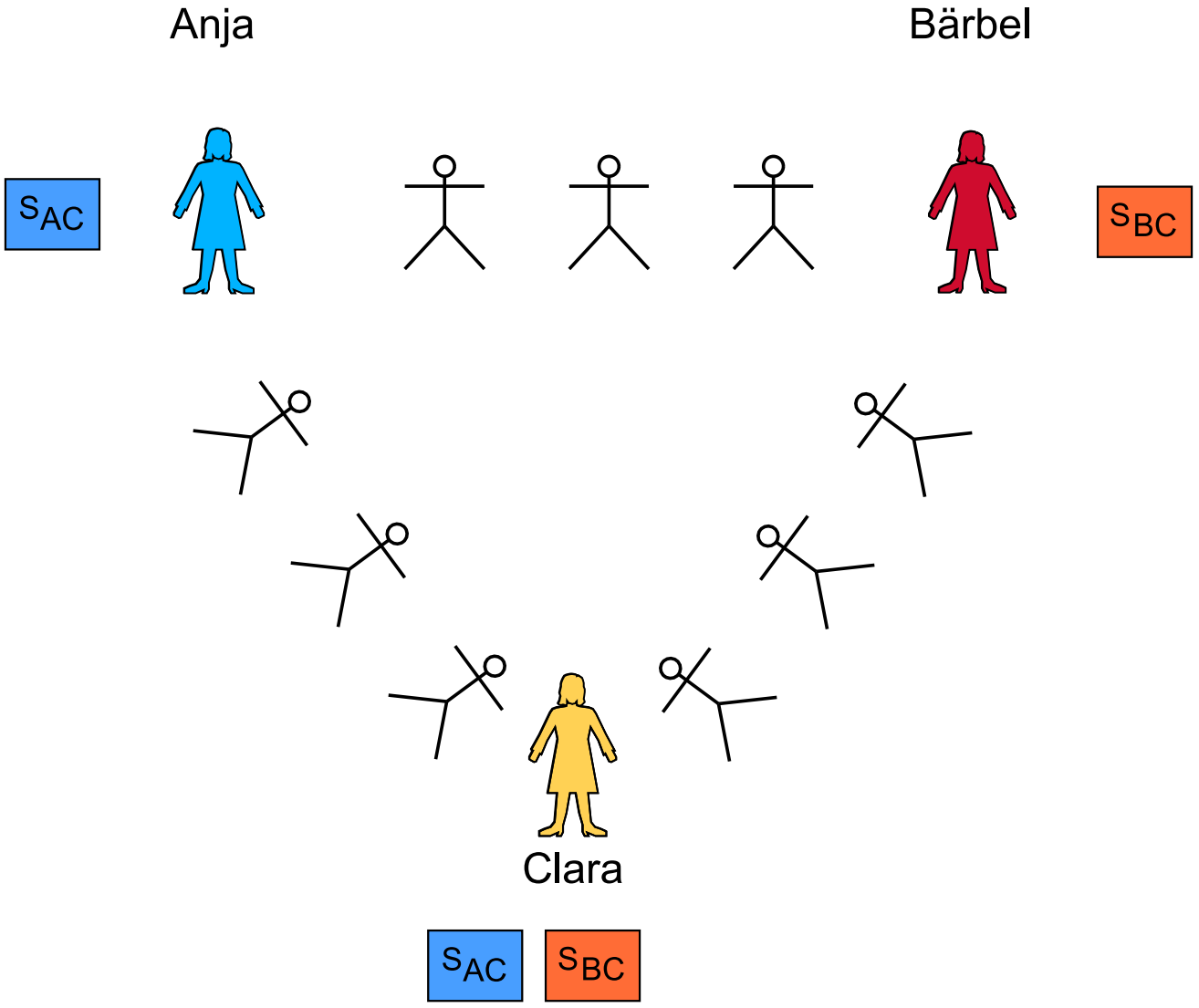
☞ Nachricht kann verändert worden sein

Needham-Schroeder

- Von Roger Needham und Michael Schroeder, 1978
- Personen Anja, Bärbel und Clara
- A und B wollen sicher miteinander kommunizieren
- C ist ein vertrauenswürdiger Dritter
- Schlüssel: S_{AC} und S_{BC}; geheim und nur A und C bzw. B und C bekannt



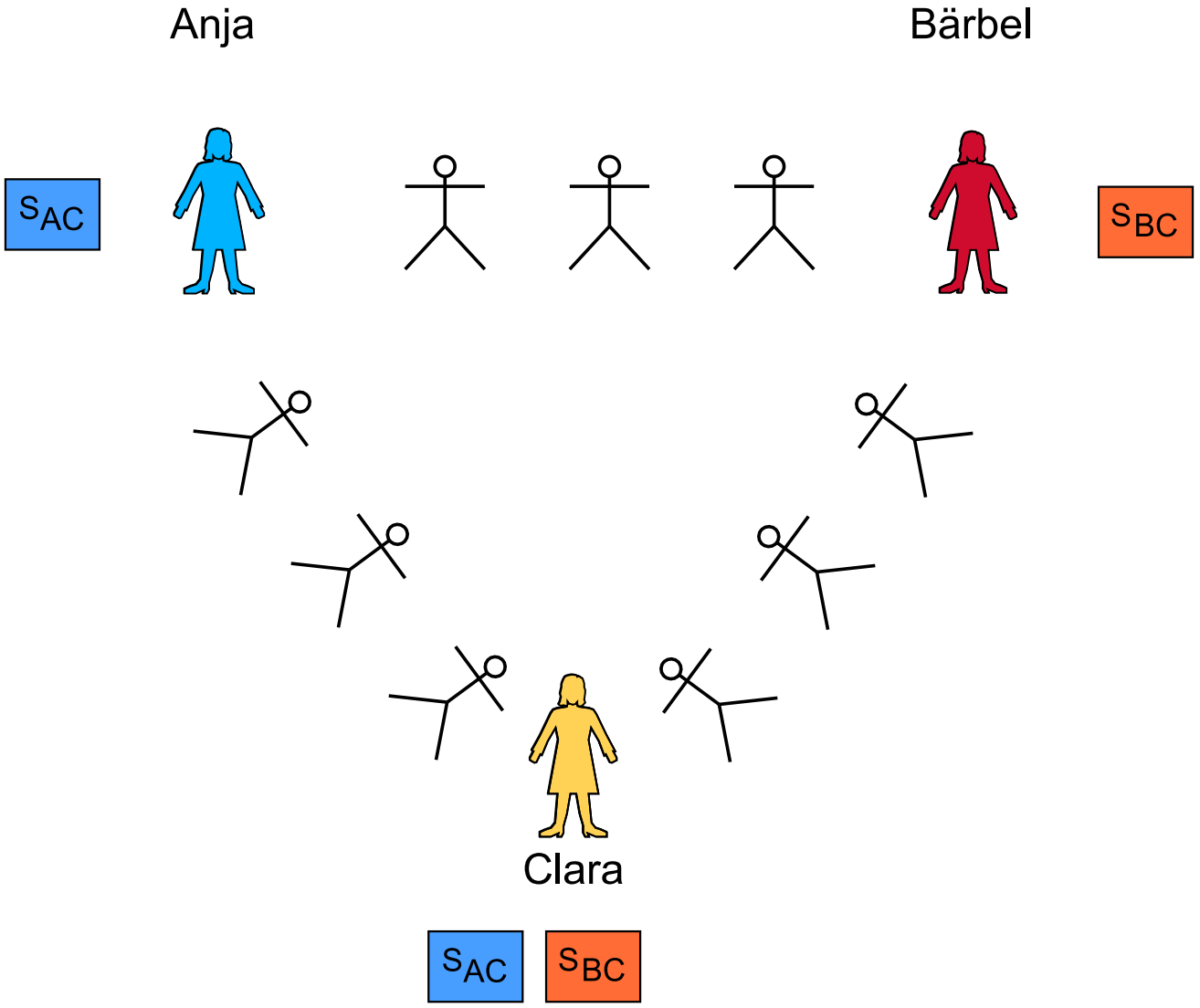
Needham-Schroeder



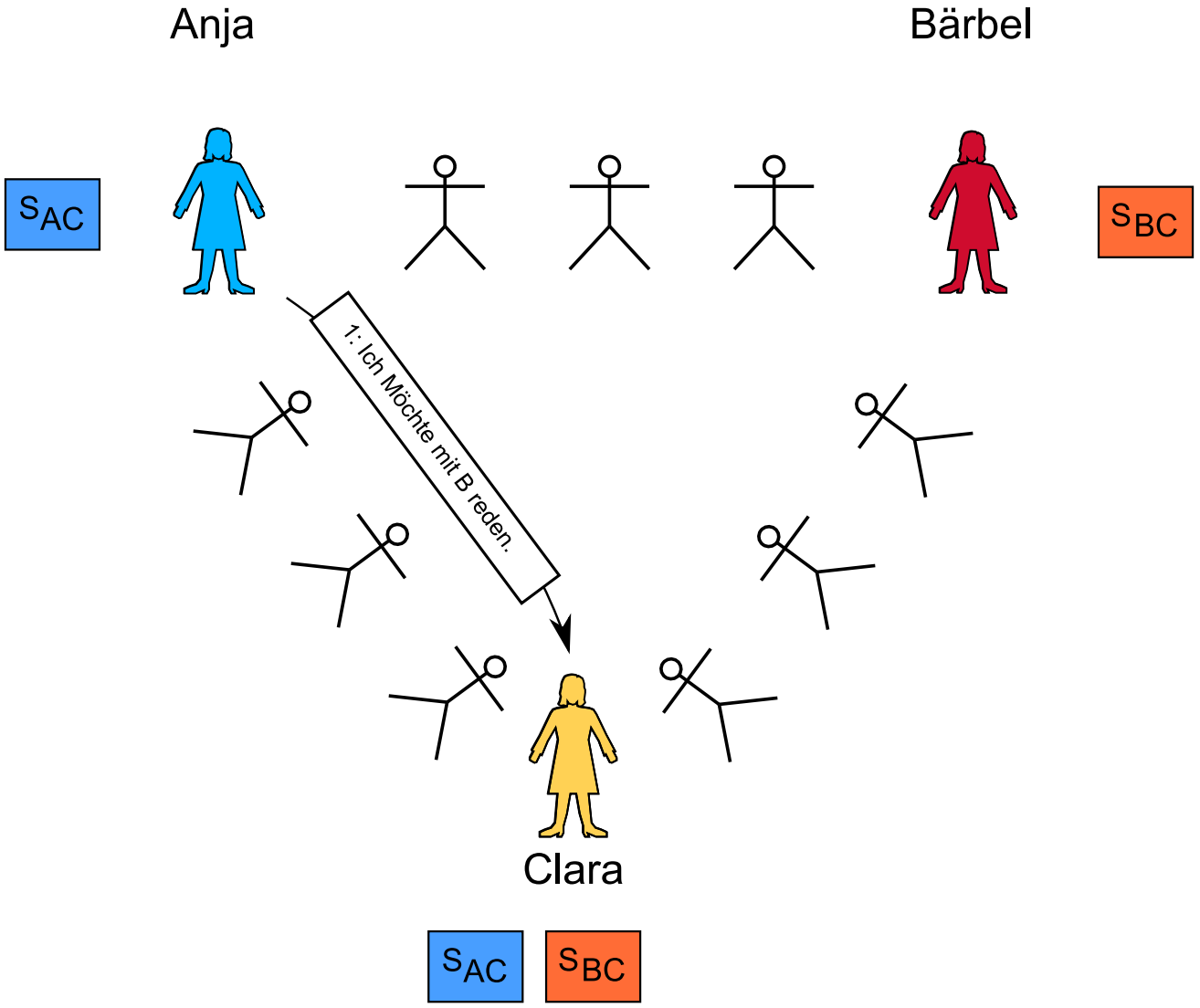
Needham-Schroeder

- Schritt 1:
  - A sendet *„Ich möchte mit B reden.“*, verschlüsselt mit S_{AC} an C
- Schritt 2:
  - C erzeugt einen Schlüssel S_{AB}
  - C verschlüsselt S_{AB}, einmal mit S_{AC} und einmal mit S_{BC}
  - C sendet die Chiffrate an A

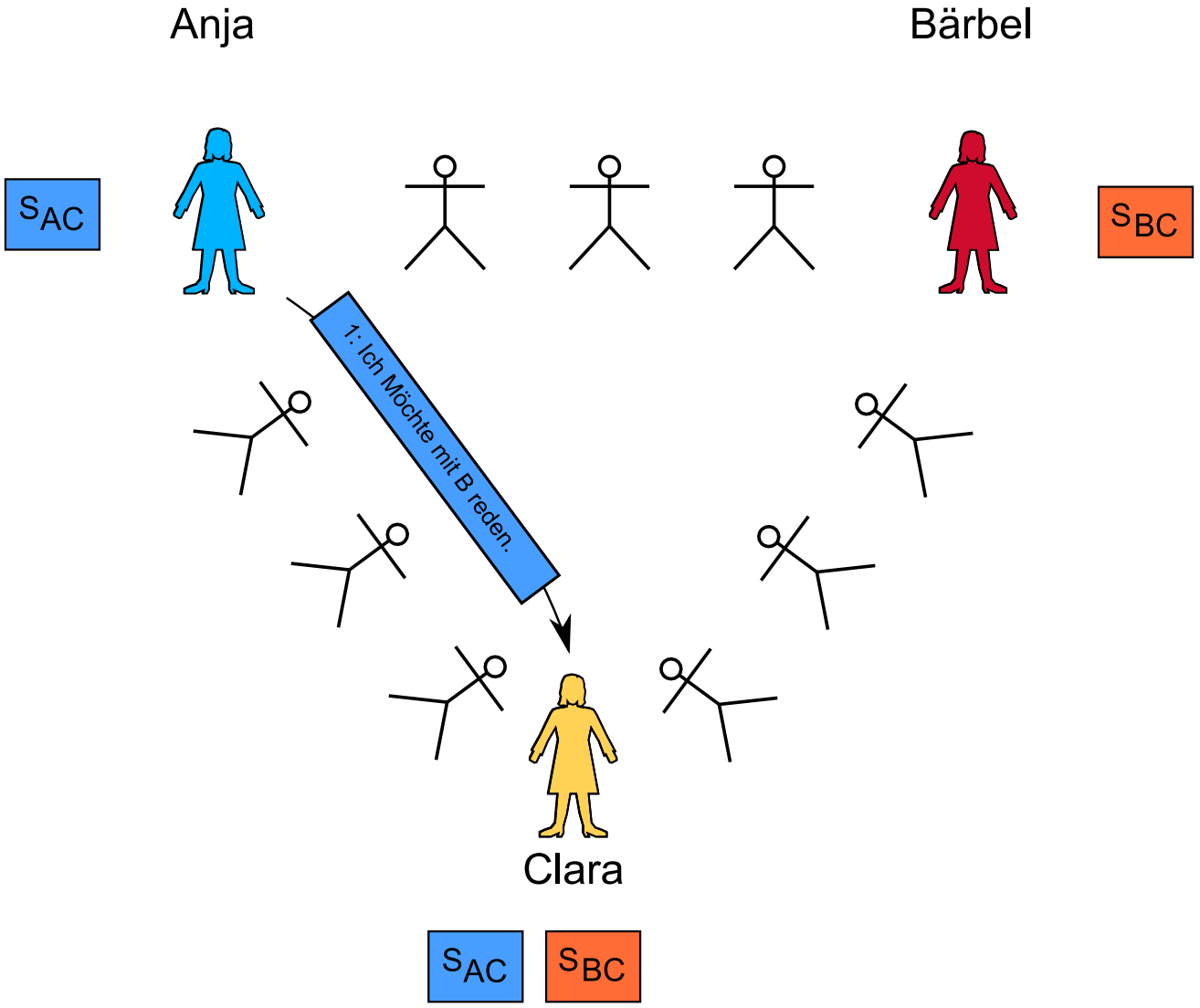
Needham-Schroeder



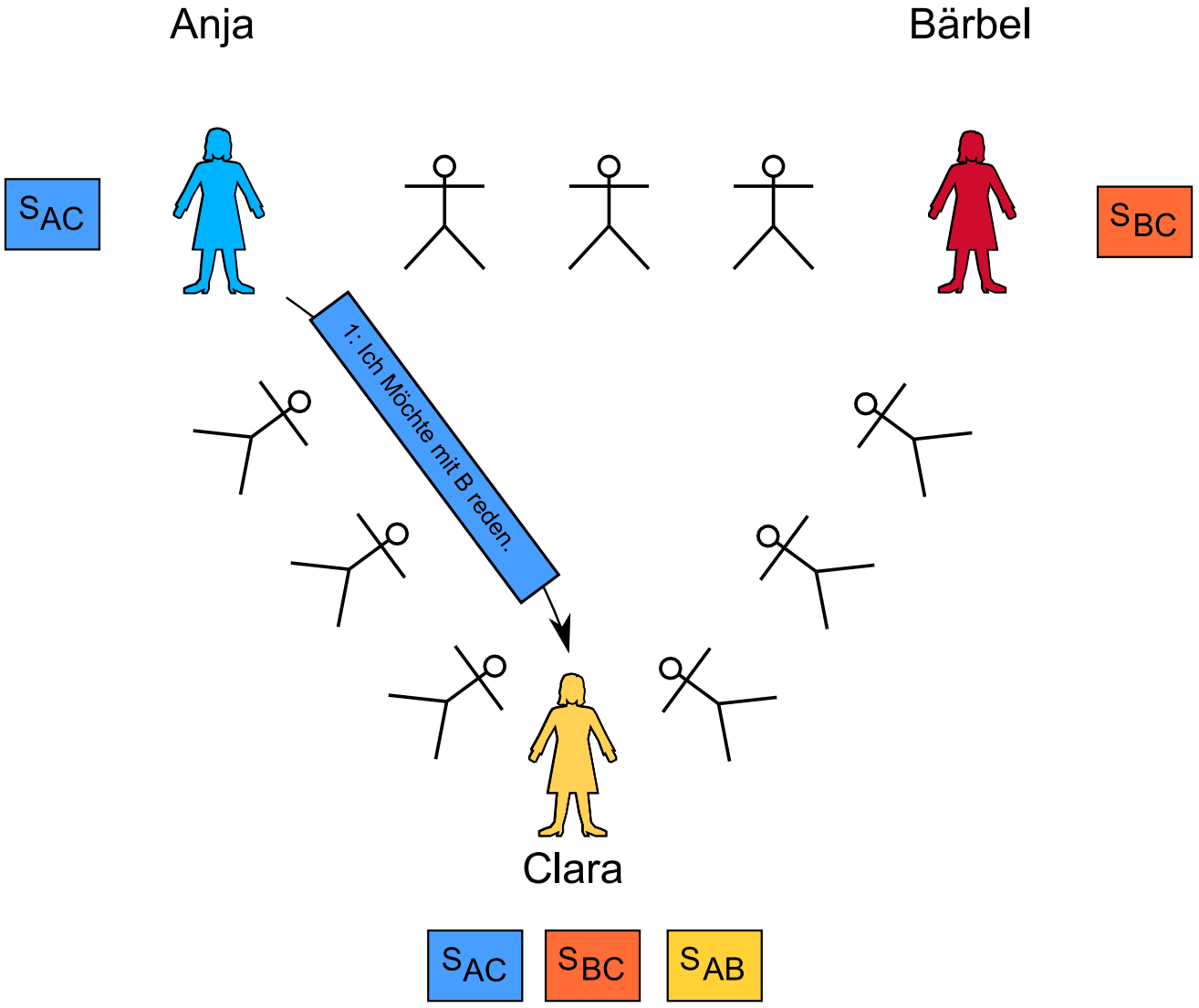
Needham-Schroeder



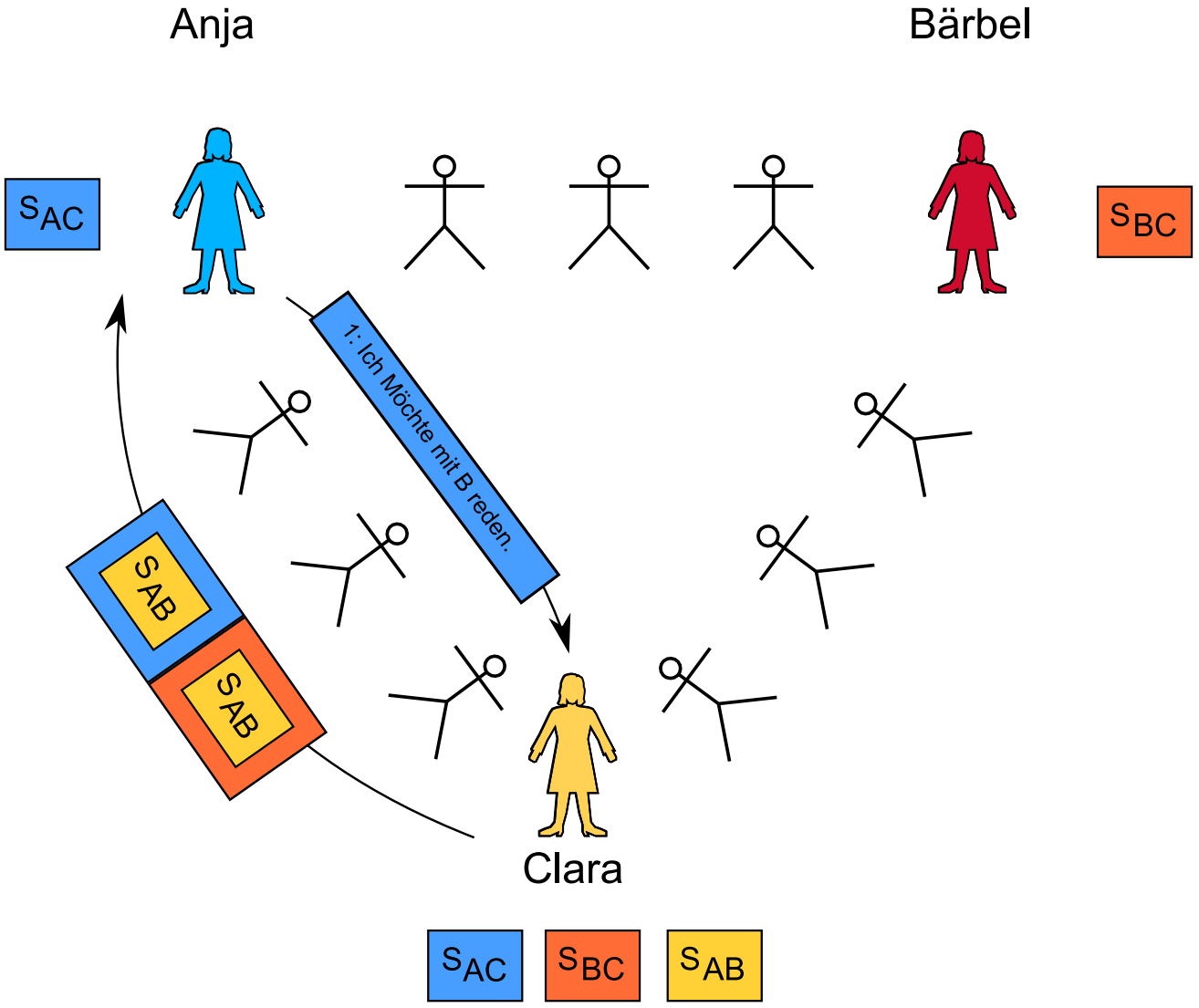
Needham-Schroeder



Needham-Schroeder



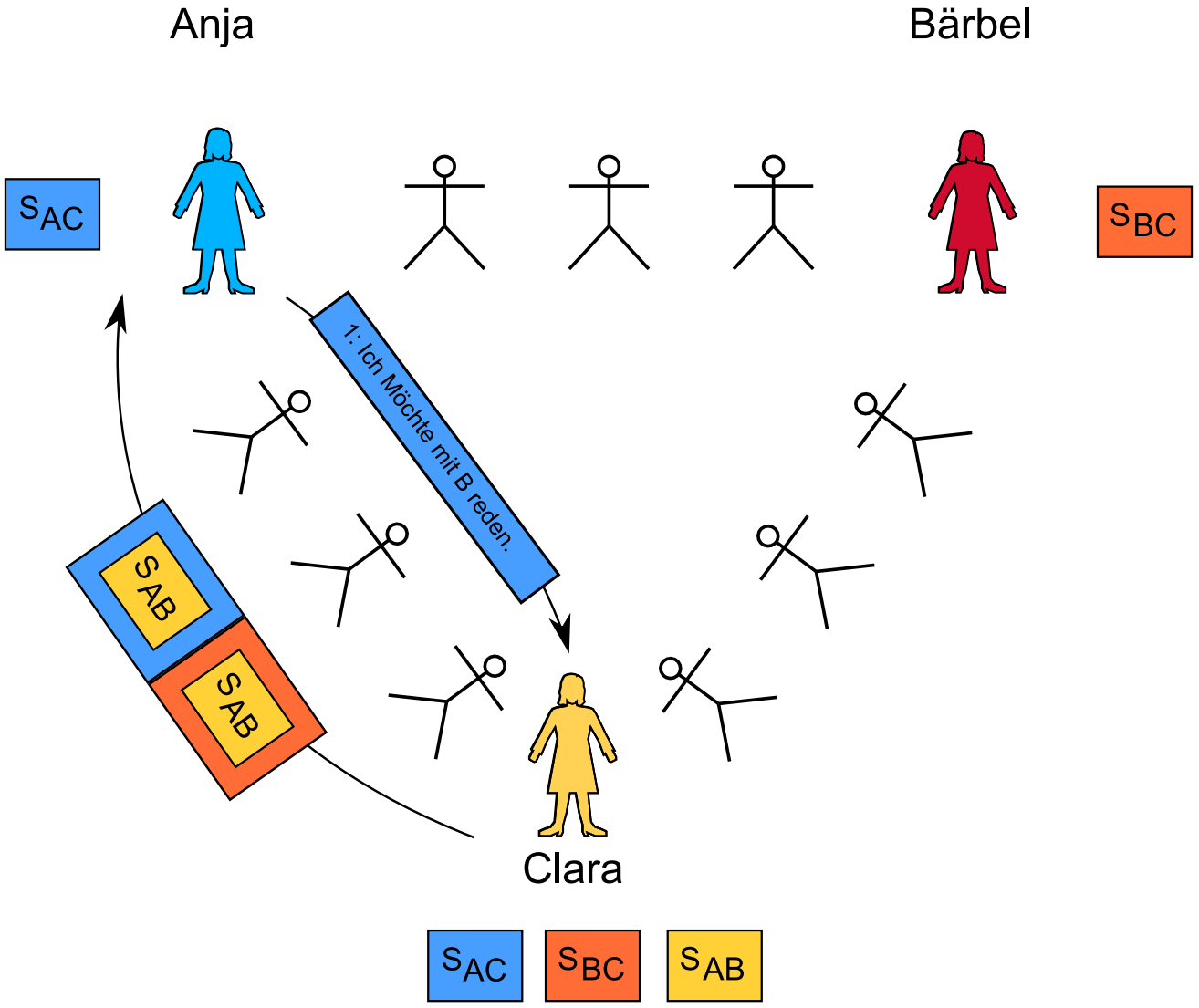
Needham-Schroeder



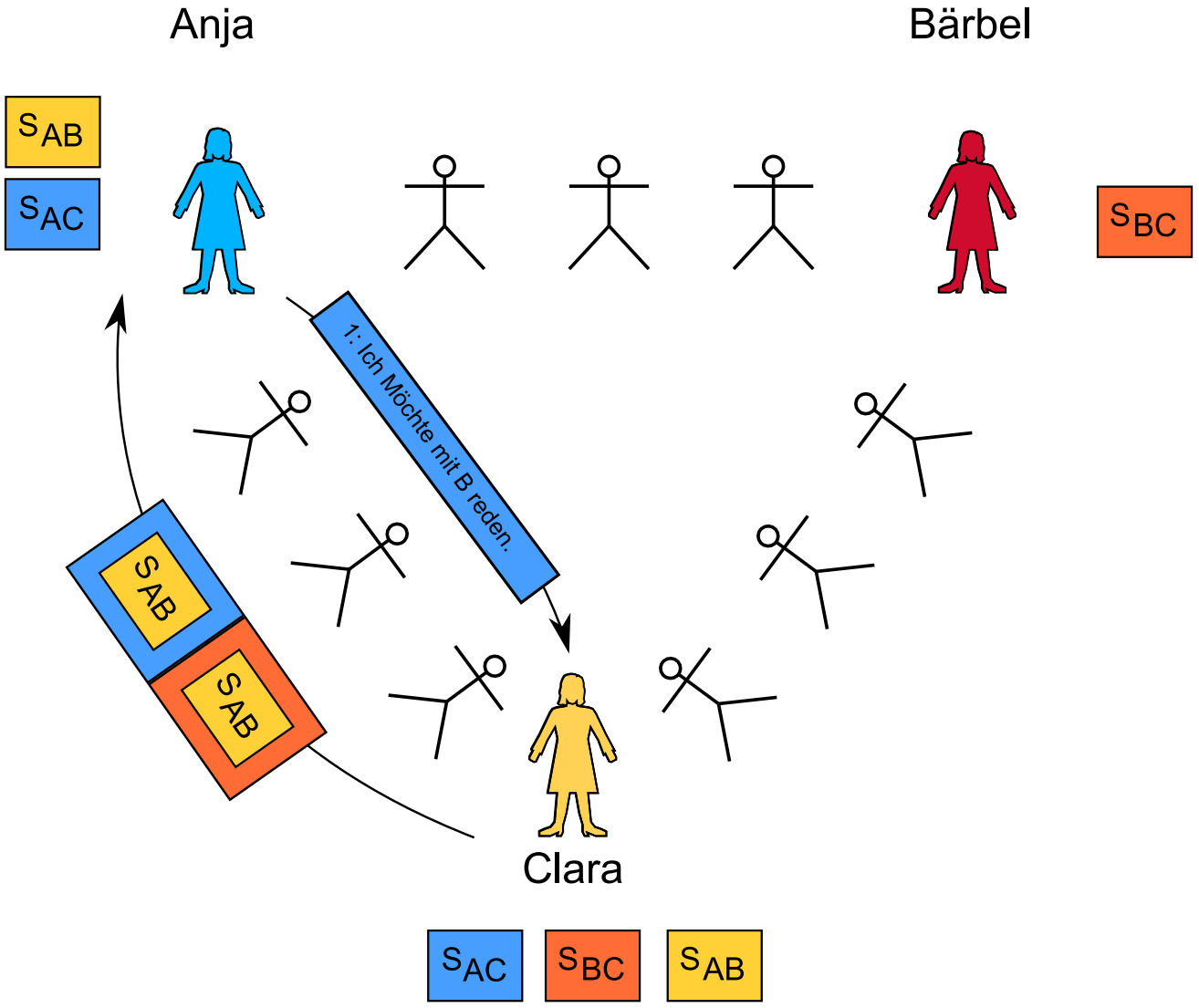
Needham-Schroeder

- Schritt 3:
  - A entschlüsselt 1. Teilnachricht und erhält S_{AB}
  - A sendet den zweiten Teil der Nachricht an B
- Schritt 4:
  - B entschlüsselt die Nachricht und erhält S_{AB}

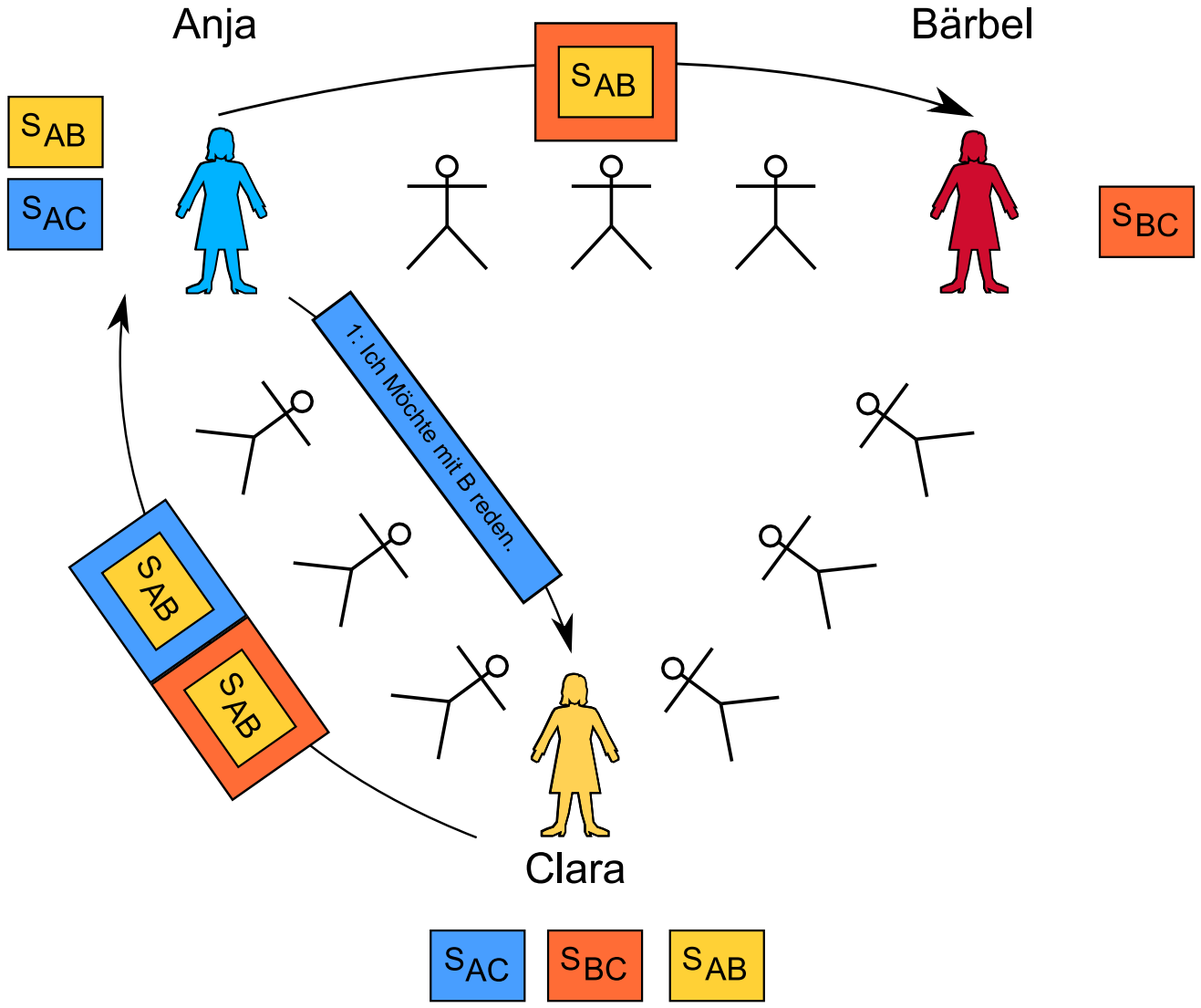
Needham-Schroeder



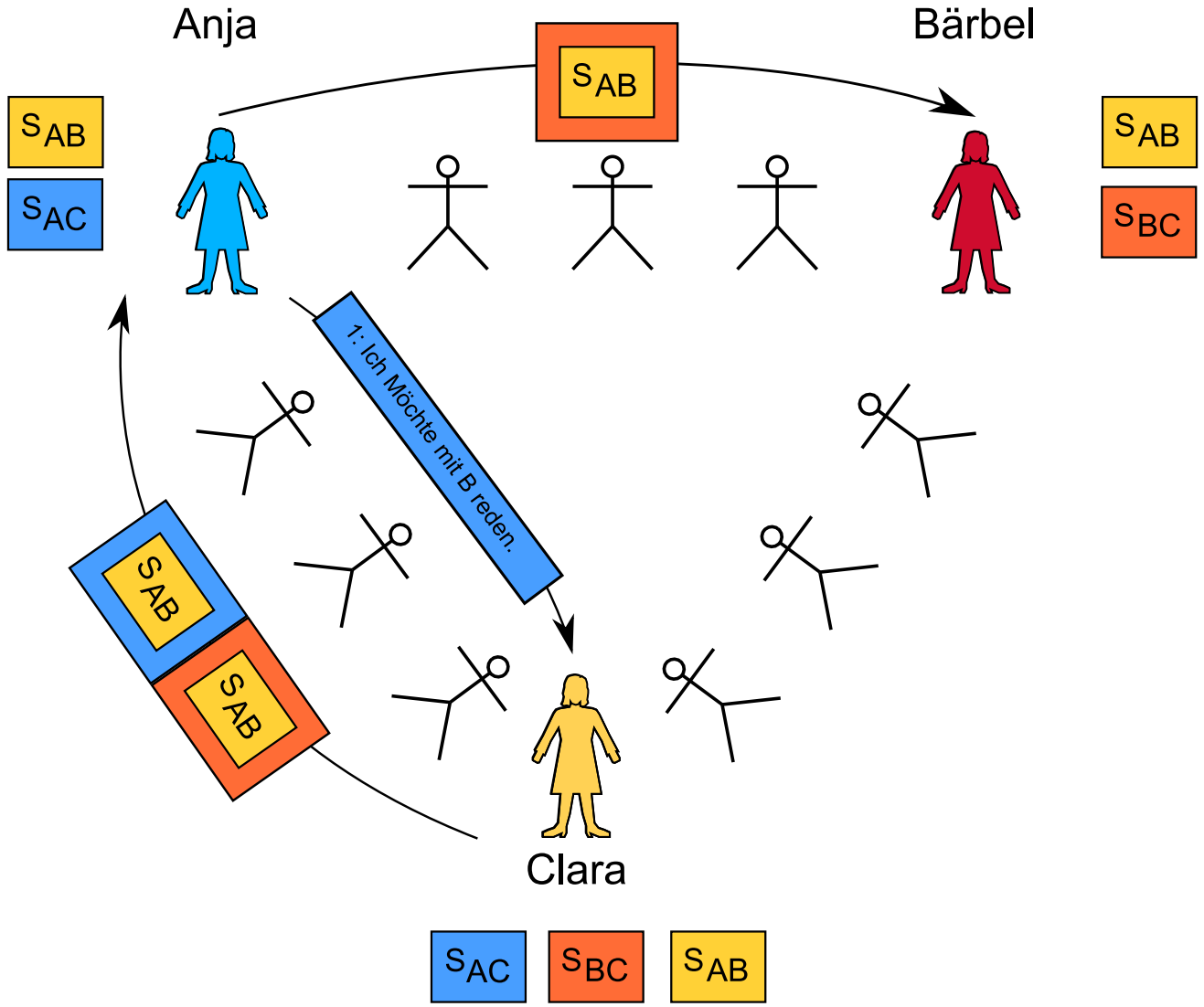
Needham-Schroeder



Needham-Schroeder



Needham-Schroeder



Needham-Schroeder

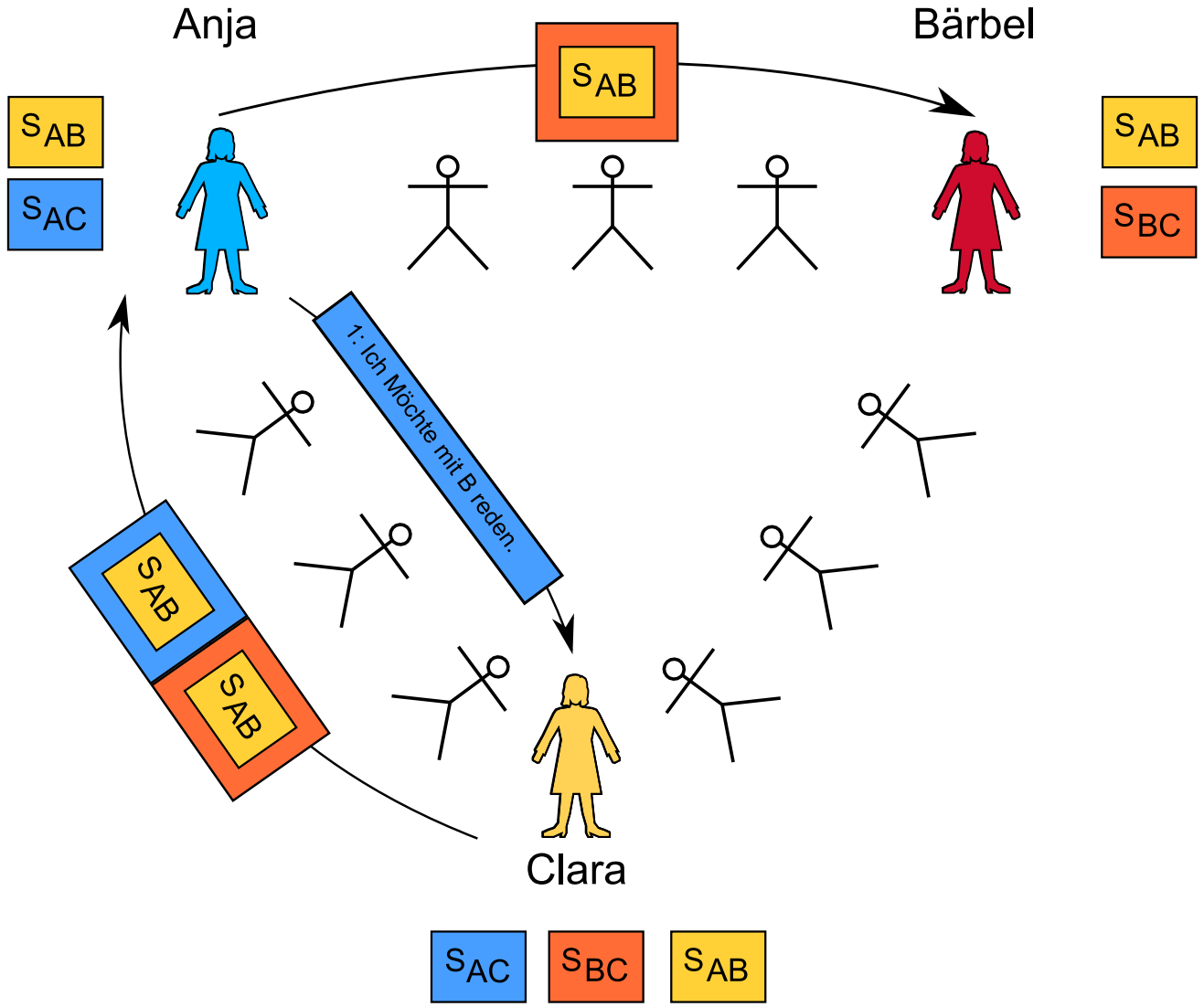
- Alle Nachrichten waren verschlüsselt

☞ Niemand kann etwas verändert haben

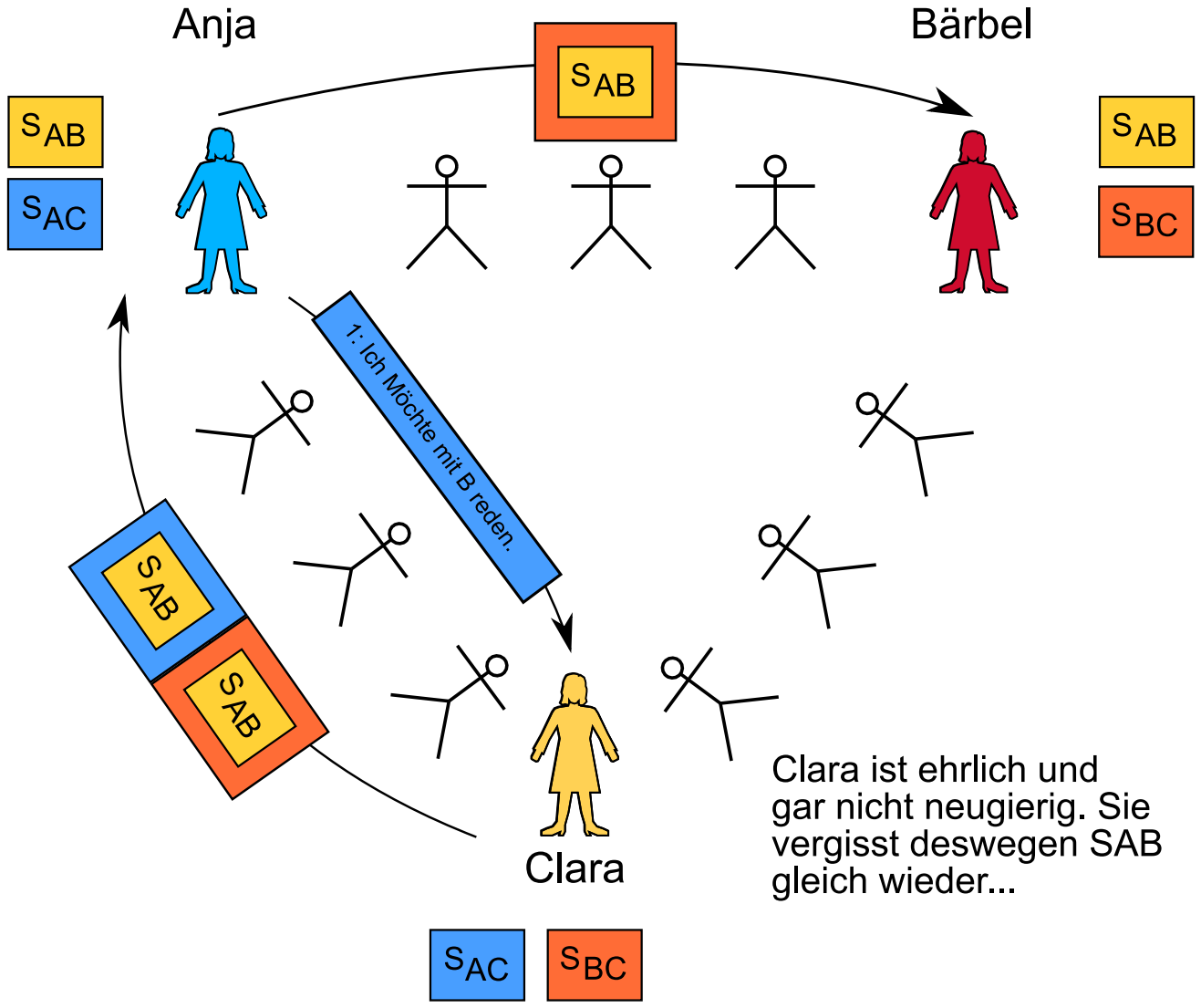
☞ Bärbel weiß, dass A wirklich Anja ist

☞ A und B haben einen gemeinsamen Schlüssel um geheime Nachrichten auszutauschen

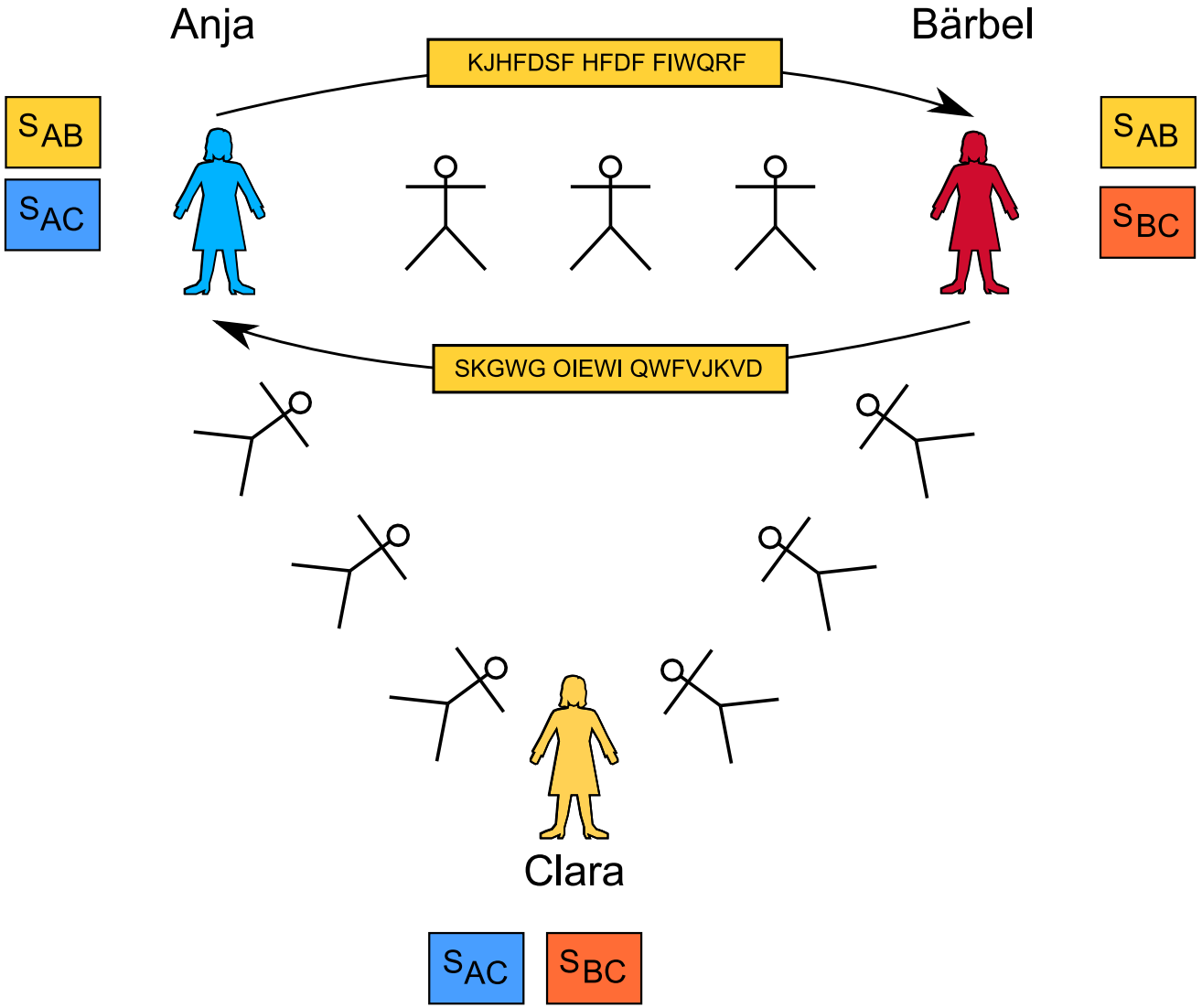
Needham-Schroeder



Needham-Schroeder



Needham-Schroeder



Geht das auch einfacher?

Geht das auch einfacher?

☞ Njein: Asymmetrische Verschlüsselung...

Ausblick: Asymmetrische Verschlüsselung

- Jeder hat ein Schlüsselpaar: einen öffentlichen und einen geheimen Schlüssel
- Nachrichten, die mit dem öffentlichen Schlüssel verschlüsselt werden, können mit dem zugehörigen geheimen Schlüssel entschlüsselt werden

☞ Verschlüsseln und Signieren

Ausblick: Asymmetrische Verschlüsselung

- Asymmetrische Verschlüsselung für E-Mails:

  GNU Privacy Guard

- Anleitung:

  http://de.wikibooks.org/wiki/GnuPG

- Technischer Hintergrund: http://de.wikipedia.org/wiki/GNU_Privacy_Guard

Danke! Noch Fragen?

Bildnachweis

Die in diesem Vortrag verwendeten fotografischen Abbildungen entstammen dem zentralen Medienarchiv der Wikimedia Commons* und sind entweder gemeinfrei, unter einer GNU-Lizenz für freie Dokumentation, oder unter den Bedingungen einer Creative Commons-Lizenz veröffentlicht.

*http://de.wikipedia.org/wiki/Hilfe:Wikimedia_Commons