Name	Telefonnummer	ist bei WA?	Hashwert der Telefonnr.	ist bei Signal?
(ich)	(meine)			

Name	Telefonnummer	ist bei WA?	Hashwert der Telefonnr.	ist bei Signal?
(ich)	(meine)			

Name	Telefonnummer	ist bei WA?	Hashwert der Telefonnr.	ist bei Signal?
(ich)	(meine)			

Whatsapp-Server

Anmeldung eines Clients:

Ein Client (z.B. „Alice“) will sich bei dir anmelden und sagt dir dabei Namen und Nummer.

Falls du sie schon im Adressbuch hattest:

- ➔ **dann** machst du neben dem Namen einen Haken unter „ist bei WA“,
- ➔ **sonst** schreibst du seinen Namen ins Soziogramm, seinen Namen und Nummer ins Server-Adressbuch und machst dort neben dem Namen einen Haken für „ist bei WA“.

Du fragst *„Lies‘ mir dein gesamtes Adressbuch vor – Namen mit Telefonnummern!“*.

Bei jedem Namen („Bob“), den der Client dir vorliest, schaust du nach:

- ➔ **ist „Bob“** schon in meinem Server-Adressbuch? Ist die Antwort...
  - ➔ **Ja:** dann ziehst du im Soziogramm einen Pfeil von „Alice“ zu „Bob“ (*Alice → Bob* bedeutet also „Alice kennt Bob“)
  - ➔ **Nein:** dann schreibst du Bobs Namen ins Soziogramm; im Soziogramm einen Pfeil von „Alice“ zu „Bob“; Bobs Namen und Nummer ins Server-Adressbuch.

Jetzt kann sich der nächste Client anmelden.

Abgleich der Adressbücher

Nach der letzten Anmeldung **meldest du dich** der Reihe nach bei allen angemeldeten Clients: *„Du bist bei Whatsapp – lies‘ mir nochmal dein gesamtes Adressbuch vor!“*. Falls der vorgelesene Name im Server-Adressbuch ein Kreuz „ist bei WA“ hat, **sagst du** dem Client Bescheid: „Ist bei Whatsapp“.

Serveradressbuch:

Nr.	Name	Telefonnummer	ist bei WA
1:			
2:			
3:			
4:			
5:			

Soziogramm:

Nr 1: _____

Nr 2: _____ Nr 3: _____

Nr 4: _____ Nr 5: _____

Whatsapp-Nutzer

… melden sich folgendermaßen beim Server an:

„Ich möchte mich bei Whatsapp anmelden. Ich heiße <xyz> und meine Telefonnummer ist <123456>“.
Wenn der Whatsapp-Server dich nach deinem Adressbuch fragt,
➔ liest du ihm alle Namen und Telefonnummern daraus vor.
Falls er dir dabei mitteilt, jemand aus deinem Adressbuch „ist bei Whatsapp“, dann
➔ machst du bei dir einen Haken unter „ist bei WA“.

Whatsapp-Nutzer

… melden sich folgendermaßen beim Server an:

„Ich möchte mich bei Whatsapp anmelden. Ich heiße <xyz> und meine Telefonnummer ist <123456>“.
Wenn der Whatsapp-Server dich nach deinem Adressbuch fragt,
➔ liest du ihm alle Namen und Telefonnummern daraus vor.
Falls er dir dabei mitteilt, jemand aus deinem Adressbuch „ist bei Whatsapp“, dann
➔ machst du bei dir einen Haken unter „ist bei WA“.

Whatsapp-Nutzer

… melden sich folgendermaßen beim Whatsapp-Server an:

„Ich möchte mich bei Whatsapp anmelden. Ich heiße <xyz> und meine Telefonnummer ist <123456>“.
Wenn der Whatsapp-Server dich nach deinem Adressbuch fragt,
➔ liest du ihm alle Namen und Telefonnummern daraus vor.
Falls er dir dabei mitteilt, jemand aus deinem Adressbuch „ist bei Whatsapp“, dann
➔ machst du bei dir einen Haken unter „ist bei WA“.

Signal-Nutzer

… melden sich folgendermaßen beim Signal-Server an:

- Berechne für jede Telefonnummer in deinem Adressbuch die „Versteckzahl“ (die heißt eigentlich „Hashwert“). Du kannst dafür das Hashwerte-Arbeitsblatt benutzen.
- Trage alle Hashwerte ins Adressbuch ein.
- Du meldest dich beim Signal-Server: „Ich möchte mich bei Signal anmelden. Ich heiße <xyz>, meine Telefonnummer ist <123456> und deren Hashwert <99>.“

Wenn der Signal-Server dir Hashwerte vorliest,

➔ vergleichst du sie mit den Hashwerten in deinem Adressbuch;

➔ **falls** ein vorgelesener Hashwert auch in deinem Adressbuch vorkommt,

➔ machst du dort den Haken „ist bei Signal“ – aber du sagst nichts zum Server!

Signal-Nutzer

… melden sich folgendermaßen beim Signal-Server an:

- Berechne für jede Telefonnummer in deinem Adressbuch die „Versteckzahl“ (die heißt eigentlich „Hashwert“). Du kannst dafür das Hashwerte-Arbeitsblatt benutzen.
- Trage alle Hashwerte ins Adressbuch ein.
- Du meldest dich beim Signal-Server: „Ich möchte mich bei Signal anmelden. Ich heiße <xyz>, meine Telefonnummer ist <123456> und deren Hashwert <99>.“

Wenn der Signal-Server dir Hashwerte vorliest,

➔ vergleichst du sie mit den Hashwerten in deinem Adressbuch;

➔ **falls** ein vorgelesener Hashwert auch in deinem Adressbuch vorkommt,

➔ machst du dort den Haken „ist bei Signal“ – aber du sagst nichts zum Server!

Signal-Nutzer

… melden sich folgendermaßen beim Signal-Server an:

- Berechne für jede Telefonnummer in deinem Adressbuch die „Versteckzahl“ (die heißt eigentlich „Hashwert“). Du kannst dafür das Hashwerte-Arbeitsblatt benutzen.
- Trage alle Hashwerte ins Adressbuch ein.
- Du meldest dich beim Signal-Server: „Ich möchte mich bei Signal anmelden. Ich heiße <xyz>, meine Telefonnummer ist <123456> und deren Hashwert <99>.“

Wenn der Signal-Server dir Hashwerte vorliest,

➔ vergleichst du sie mit den Hashwerten in deinem Adressbuch;

➔ **falls** ein vorgelesener Hashwert auch in deinem Adressbuch vorkommt,

➔ machst du dort den Haken „ist bei Signal“ – aber du sagst nichts zum Server!

Signal-Server

Anmeldung:
Wenn sich ein Client bei dir anmelden will:
➔ **dann** schreibst du alle seine Angaben ins Server-Adressbuch.

Abgleich der Kontakte:
Nach der letzten Anmeldung meldest du dich der Reihe nach bei deinen Signal-Clients:
Du liest ihnen alle Hashwert aus deinem Server-Adressbuch vor; bekommst aber keine Antwort.

Serveradressbuch:

Name	Telefonnummer	Hash

Hashwerte für `Signal` berechnen

Telefonnummer (hier 6 Ziffern)	4	8	3	1	0	7	Beispiel
Faktoren für Ziffern	·11	·7	·5	·3	·2	·1	
Zwischenergebnisse	44+	56+	15+	3+	0+	7	Hash = 125

·11	·7	·5	·3	·2	·1	
.....+	.....+	.....+	.....+	.....+	.....=	....

·11	·7	·5	·3	·2	·1	
.....+	.....+	.....+	.....+	.....+	.....=	....

·11	·7	·5	·3	·2	·1	
.....+	.....+	.....+	.....+	.....+	.....=	....

·11	·7	·5	·3	·2	·1	
.....+	.....+	.....+	.....+	.....+	.....=	....

·11	·7	·5	·3	·2	·1	
.....+	.....+	.....+	.....+	.....+	.....=	....

Metadaten: Sequenzdiagramme analysieren

Viele Mailserver (z.B. Google Mail oder GMX) lesen automatisch jede Mail mit, unter anderem um zu erfahren, wer sich für welche Themen interessiert.

Manche Messenger-Server können das nicht, weil die Chatnachrichten Ende-zu-Ende-verschlüsselt sind: Das heißt, dass sie beim Absender verschlüsselt, in dieser Form an den Server geschickt, von ihm weitergeleitet – und erst ganz am Schluss beim Empfänger entschlüsselt werden. Der Server kennt also den eigentlichen Inhalt der Nachrichten nicht.

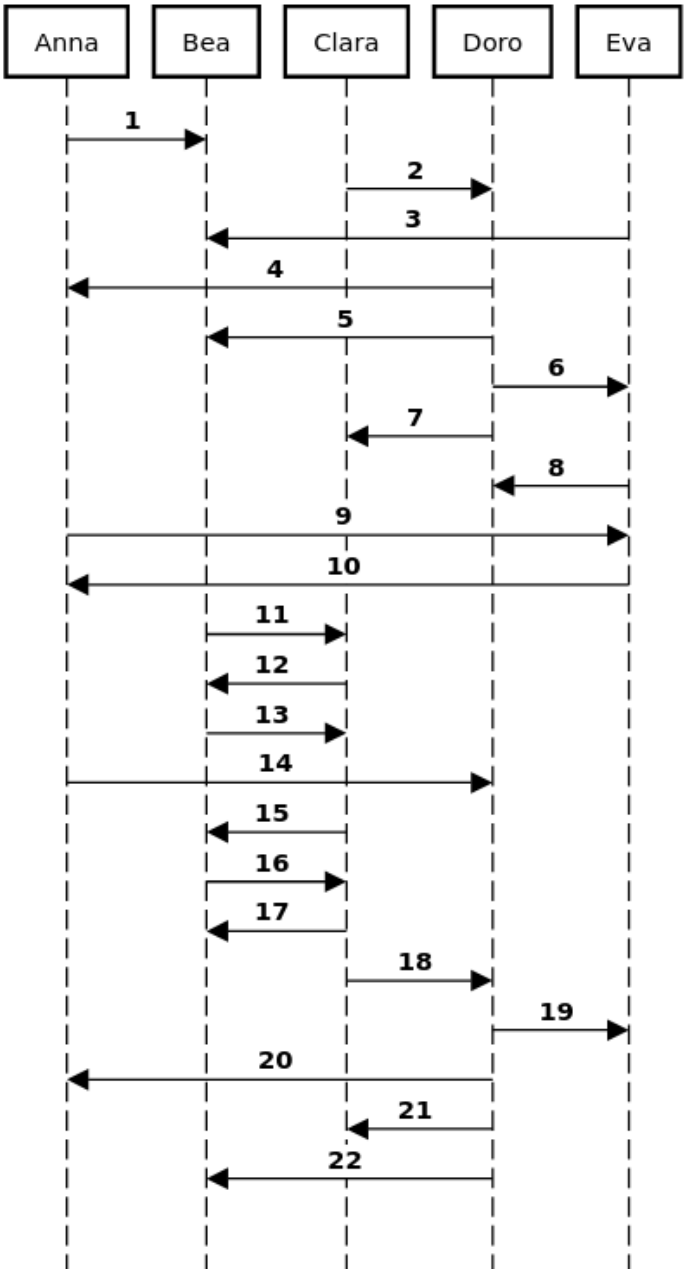
Trotzdem weiß er, wer wem wann schreibt und welche Nachrichten eine große oder kleine Datenmenge enthalten. Diese Angaben nennt man „Metadaten“. Auch sie sagen schon eine ganze Menge über die beteiligten Personen.

Sequenzdiagramm: Beachvolleyball

Aus den Metadaten kann man ein sogenanntes „Sequenzdiagramm“ machen:

Du kannst damit beispielsweise herausfinden, welche der fünf Frauen die Trainerin dieser Beachvolleyballmannschaft ist.

Welche ist es, und woran erkennt man das?



……..

……..

……..

……..

……..

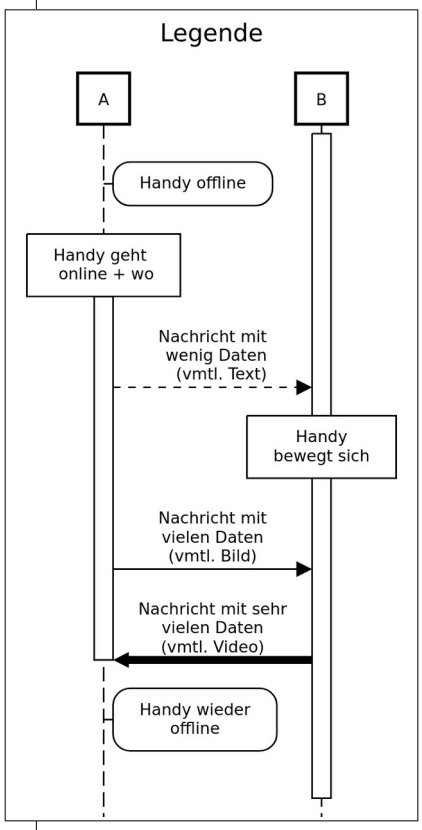
……..

……..

Sequenzdiagramm: Gestern in der 9a

Hier siehst du ein paar Leute aus der 9a.

Die Legende erklärt, wie das Diagramm zu lesen ist:



Der Whatsapp-Server weiß hier auch, wer wann wo ist (dazu liest der Whatsapp-Client die GPS- oder WLAN-Ortung aus und meldet sie dem Server) und welche Nachrichten viele oder wenige Daten enthalten.

Tipp: Der Unterricht endet für alle um 15:30.

Sei fantasievoll und notiere alles, was du aus dem Diagramm herauslesen kannst.