

# WHATSAPP-SIGNAL-SPIEL

Autor(en): Leonore Dietrich  
Urs Lautebach

Stand: März 2022

Lizenz 

Dieses Werk ist unter einem Creative Commons 4.0 Deutschland Lizenzvertrag lizenziert:

- Namensnennung
- Keine kommerzielle Nutzung
- Weitergabe unter gleichen Bedingungen

Um die Lizenz anzusehen, gehen Sie bitte zu [www.creativecommons.org](http://www.creativecommons.org) oder schicken Sie einen Brief an Creative Commons, 171 Second Street, Suite 300, San Francisco, California 94105, USA.



## Inhaltsverzeichnis

Das Whatsapp-Signal-Spiel (Lehrerblatt).....	3
Idee.....	3
Übersicht.....	3
Vorbereitung.....	3
Spielbeginn Whatsapp (Lehrerblatt).....	4
Einrichtung der Handys.....	4
Whatsapp-Runde: Anmeldung.....	4
Whatsapp-Runde: Whatsapp-Kontakte mitteilen.....	4
Whatsapp-Runde: Rückblick (Lehrerblatt).....	5
Spielbeginn Signal (Lehrerblatt).....	6
Signal-Runde: Handys berechnen Hashwerte.....	6
Signal-Runde: Anmeldung.....	6
Signal-Runde: Nachrichten schicken.....	6
Signal-Runde: Rückblick (Lehrerblatt).....	7
Beispielhafter Spielverlauf Whatsapp-/Signalrunde.....	8
Beide Messenger: Nachrichtenaustausch (Lehrerblatt).....	10
Bonus: Metadaten-Analyse (Lehrerblatt).....	11
Beachvolleyball.....	11
Nachmittag in der 9a.....	11
Whatsapp-Server.....	14
Anmeldung eines Clients:.....	14
Abgleich der Adressbücher.....	14
Soziogramm:.....	14
Whatsapp-Nutzer.....	15
Whatsapp-Nutzer.....	15
Whatsapp-Nutzer.....	15
Signal-Nutzer.....	16
Signal-Nutzer.....	16
Signal-Nutzer.....	16
Signal-Server.....	17
Hashwerte für Signal berechnen.....	18
Metadaten: Sequenzdiagramme analysieren.....	19
Sequenzdiagramm: Beachvolleyball.....	19
Sequenzdiagramm: Gestern in der 9a.....	20



# Das Whatsapp-Signal-Spiel (Lehrerblatt)

## Idee

Auf einem Elternabend der siebten Klasse inspirierte ein Vater dieses Spiel, als er recht meinungsstark äußerte: *„Whatsapp ist stärker verbreitet als Signal und hat damit gewonnen, da ist doch klar, was man benutzt! Uns kann’s egal sein, beide machen schließlich GENAU dasselbe.“*

Das stimmt natürlich nicht; tatsächlich gibt es erhebliche Unterschiede nicht nur zwischen den Geschäftsmodellen und damit beim erwartbaren Datenschutzniveau, sondern auch zwischen den technischen Umsetzungen.

Die Rollenspiele „Whatsapp-Server“ und „Signal-Server“ verdeutlichen das Zusammenspiel zwischen Server und Clients bei den Messengern Whatsapp und Signal. Sie sollen sichtbar machen, wie unterschiedlich die beiden Messenger mit den Daten ihrer Nutzer umgehen: Nicht nur verspricht Signal, die Privatsphäre seiner Nutzer zu respektieren – der Dienst garantiert sogar, dass er von vornherein viel weniger über sie erfährt.

## Übersicht

Das Spiel wurde in den Stufen 5-12 erprobt und eignet sich am besten ab Klasse 7. In jeder Schülergruppe spielt ein Server mit 3-5 Clients. Größere Gruppen sind besser. Notfalls kann in Dreier- oder Vierergruppen einer Server *und* einen Client spielen; bis zur Mittelstufen sollte man das aber vermeiden, weil die wichtige Rollenverteilung Client-/Server dadurch verwischt.

Es gibt eine Runde zur Einrichtung der Handys und dann je eine Whatsapp- bzw. Signal-Runde (insgesamt in Klasse 7 ca. 90 Minuten). Man kann zwei weitere Runden mit Metadaten-Analysen (ca. 10 und 20 Minuten) anhängen, in denen Schüler die eigentliche Kommunikation auswerten. Während der „Einrichtung“ füllen die Teilnehmer ihre Handy-Adressbücher; in der Whatsapp- und der Signal-Runde melden sich einige „Clients“ jeder Gruppe beim Messenger an.

Die Lehrkraft sollte das Spiel vorab einmal mit Kollegen oder älteren Schülern durchspielen.

Die Beobachtungen aus jeder Runde sollten unbedingt gemeinsam besprochen werden.

## Vorbereitung

0. Kopieren:
  - für jeden Schüler ein Papier-“Handy“ mit Adressbuch (S. 12, zerschneiden)
  - für jeden Schüler ein Blatt „Hashwerte berechnen“ (S. 18)
  - je Gruppe ein Whatsapp-Server (S. 14), ein Signal-Server (S. 17), eine Anleitung „WA-Nutzer“ (S. 15, schneiden) und eine Anleitung „Signal-Nutzer“ (S. 16, schneiden)
1. Klasse in Fünfer- und Sechsergruppen einteilen; kleinere Gruppen sind ungünstig.
2. Die Lehrkraft entscheidet, ob Klarnamen oder Pseudonyme verwendet werden sollen.
3. Material für Whatsapp-Runde austeilen.
4. Die Schüler sollen den Anleitungen sehr genau folgen und „wie ein Scratch-Programm“ genau das tun, was das Protokoll jeweils verlangt. Manche schreiben sonst Dinge auf, die sie in ihrer Rolle gar nicht wissen können. In vielen Fällen wird die Lehrkraft den typischen Schritt jeder Runde daher zunächst einmal demonstrieren.



## Spielbeginn Whatsapp (Lehrerblatt)

### Einrichtung der Handys

5. Jeder wählt für sich eine genau sechsstellige Handynummer. Weder Name noch Telefonnummer sollten im Team doppelt vorkommen. Name und Nummer werden nebeneinander ins eigene(!) Adressbuch eingetragen. In den meisten Klassen empfehlen sich Pseudonyme statt Realnamen.
6. Jeder trägt in sein Adressbuch auch Namen und Nummern einiger „Bekannte“ (anderer Gruppenmitglieder) – aber nicht die ganze Gruppe, denn auch im richtigen Leben kennt nicht jeder jeden. Auch sollte die Eintragung nicht immer gegenseitig sein.

**Die anderen Spalten im Telefonbuch bleiben noch frei.**

### Whatsapp-Runde: Anmeldung

Einige (aber nicht alle!) Clients eines Teams melden sich nun bei ihrem Whatsapp-Server an. Der zugehörige Ablauf ist auf den Schülerblättern „Whatsapp-Serverblatt“ und „Anleitung Whatsapp-Client“ detailliert beschrieben, jedoch immer nur aus *einer* Perspektive (Client oder Server). Aus Sicht des äußeren Beobachters läuft das so:

Client	Server
Client und Server folgen genau ihrer jeweiligen Anleitung:	
7. <b>Ein Client</b> spricht den Whatsapp-Server an: „Ich möchte mich anmelden!“ und nennt Namen und Nummer.	
8.	<b>Der Server</b> trägt beides (falls er sie noch nicht hatte) in sein Adressbuch ein und macht dort einen Haken „bei WA?“, um sich zu merken, dass dieser Client Whatsapp nutzt.
9. Außerdem fragt <b>der Server</b> den Client nach dessen Adressbuch („lies mir alle Namen und Telefonnummern aus deinem Telefonbuch vor!“).	
10.	<b>Der Client</b> liest dem Server alles vor. Der Server trägt alle Namen und Nummern in sein Adressbuch ein, die er vorher noch nicht kannte, und zeichnet „A kennt B“-Pfeile im Soziogramm.
11. Dann fängt <b>der nächste Client</b> (von denen, die sich anmelden möchten), wieder bei Schritt 6. an.	

### Whatsapp-Runde: Whatsapp-Kontakte mitteilen

12.	Dann lässt der Server sich <i>erneut</i> von seinen angemeldeten Client (aber nur denen!) das gesamte Adressbuch vorlesen:
13. Ein Client liest vor...	
14.	Der Server hört zu; bei jedem Namen, der im Server-Adressbuch als Whatsapp-Nutzer markiert ist, sagt der Server „ist bei Whatsapp“...
15. ... und der Client setzt den Haken dann in seinem eigenen Adressbuch.	
16.	Der Server fordert den nächsten Client zu Schritt 13 auf.



## Whatsapp-Runde: Rückblick (Lehrerblatt)

An dieser Stelle sollte man zurückblicken und ein paar Beobachtungen formulieren lassen. Ein Whatsapp-Serverblatt auf dem Beamer dient als Diskussionsgrundlage. Oft ist es jetzt besser, wenn Pseudonyme statt realer Schülernamen verwendet wurden:

A1: Was fällt euch auf?

Der Whatsapp-Server kennt viele Namen und Nummern, und zwar auch von Leuten, die sich gar nicht angemeldet haben.

Das ist nicht ganz fair und datenschutzrechtlich auch absolut unzulässig, weil sie weder gefragt wurden, noch zugestimmt haben. In Wirklichkeit ist es noch schlimmer, denn das Adressbuch enthält ja auch Geburtstage, Berufe, Hobbies und andere Angaben über die Bekannten.

A2: Haben die Whatsapp-Nutzer etwas davon?

Ja, durchaus: Sie bekommen von Whatsapp gesagt, welche ihrer Freunde ebenfalls bei Whatsapp sind. Das ist sehr praktisch. Und können ihnen Nachrichten schicken – scheinbar „kostenlos“, jedenfalls ohne Geld zu bezahlen. Auch das ist angenehm.

A3: Hat Whatsapp auch etwas davon? Anders gefragt: Whatsapp hat viele Mitarbeiter, Rechenzentren, alles sehr teuer, verlangt von seinen Nutzern aber kein Geld. Womit verdient Whatsapp eigentlich Geld? Oder, etwas provokanter: „Sarah, was zahlen deine Eltern monatlich für’s Whatsapp-Abo? Wie hoch war eure letzte Google-Rechnung?“

Die Frage ist schwierig, die Antworten bleiben vage. Schüler wissen dazu nur, dass Whatsapp nun „die Daten verkauft“; Erwachsener ebenfalls. Es gibt keine Vorstellung davon, wer hier eigentlich Geld bezahlt und wofür.

Schon aus dem Soziogramm weiß der Whatsapp-Server, wer wen kennt, wer viele oder wenige Kontakte hat. *Dieses Wissen ist keineswegs harmlos, sondern eine sehr persönliche Angelegenheit. Aus der täglichen Beobachtung seiner Nutzer erfährt Whatsapp noch sehr viel mehr, wie die letzte Spielphase „Metadaten“ zeigt. Das Wissen lässt sich gut verkaufen, etwa in folgendem Beispielszenario:*

Der Schuhhersteller EDELTRET möchte teure Schuhe verkaufen. Am besten wäre es, wenn EDELTRET-Schuhe als „in“ gelten. Das kann EDELTRET vielleicht schaffen, wenn die Firma sehr populären Schüler Rabattcoupons gibt: Wenn diese „Vorbilder“ dann EDELTRET tragen, wollen die anderen vielleicht auch welche haben. Aber wer ist populär? EDELTRET weiß das nicht. Aber Whatsapp weiß es: Es sind im Soziogramm die, auf die viele Pfeile zeigen. Dieses Wissen ist so wertvoll, dass man mit dem Verkauf sehr viel Geld verdienen kann.

A4: Könnte Whatsapp auch arbeiten, ohne sein Wissen zu verkaufen?

*Nein. Whatsapp hat keine andere Einnahmequelle.*

A5: Geht das überhaupt: dass der Messenger einer Nutzerin sagt, welche ihrer Freunde ebenfalls angemeldet sind – aber ohne dem Server das Telefonbuch zu übermitteln?

*Ja, das geht. Es ist aber ziemlich raffiniert. Die Frage leitet über zur Signal-Runde.*



## Spielbeginn Signal (Lehrerblatt)

### Signal-Runde: Handys berechnen Hashwerte

Die Schüler behalten ihre Handys mit den ausgefüllten Adressbüchern.

16. Vor der Signal-Phase berechnet jeder Client die Hashwerte aller Telefonnummern in seinem Telefonbuch. Dazu dient das Schülerblatt „Hashwerte berechnen“. Auch hier empfiehlt es sich, einen ersten Hashwert mit der Klasse gemeinsam zu berechnen.
17. Rechenfehler würden später Verwirrung stiften. Die „echten“ Clients können das zwar nicht, aber man kann Schüler zur Aufdeckung von Kopfrechenfehlern ihre Hashwerte vergleichen lassen: gleiche Telefonnummern müssen auch gleiche Hashwerte ergeben.

### Signal-Runde: Anmeldung

Die Clients des Teams (diesmal können es auch alle sein) melden sich nun bei Signal an:

Client	Server
Wieder der Hinweis, den Anleitungen genau zu folgen.	
18.	Ein Client spricht den Signal-Server an: „Ich möchte mich anmelden!“ und nennt dabei seinen eigenen (nur den eigenen!) Namen, Telefonnummer und Hashwert.
19.	Der Server trägt alles ins Serveradressbuch ein.
20.	Der Server benachrichtigt der Reihe nach alle Clients, die schon angemeldet waren, und teilt ihnen den Hashwert des neuen Clients mit.
21.	Die Clients hören dem Server zu, sagen aber nichts. Jeder Client prüft, ob er einen Namen mit diesem Hashwert im Adressbuch hat; falls ja, macht er dort ein Kreuz bei „nutzt Signal“. Dem Server sagt er nichts.
22.	Der nächste Client, der sich anmelden möchte, startet wieder bei Schritt 18, bis alle Clients angemeldet sind, die sich anmelden wollen.
23.	Wenn alle angemeldet sind, muss der Signal-Server normalerweise noch eine „Benachrichtigungsrunde“ durchführen, bis alle seine Clients die entsprechenden Kreuze gemacht haben.

### Signal-Runde: Nachrichten schicken

Aus technischen Gründen (s.o.) läuft der Nachrichtenaustausch bei Signal exakt so ab wie bei Whatsapp; hier gibt es keine Unterschiede. Diese Phase kann also ohne Weiteres entfallen.



## Signal-Runde: Rückblick (Lehrerblatt)

Man sollte als Diskussionsgegenstand wieder das Signal-Serverblatt einer Gruppe zeigen.

Der Unterschied zu Whatsapp ist eklatant:

- Der Signal-Server kann von den Leuten, die sich anmelden, kein Soziogramm erstellen.
- Von Leuten, die sich nicht selber anmelden, erfährt er *überhaupt nichts*.

Auch die meisten Siebtklässler erkennen und formulieren das von sich aus. Dieser Unterschied ist auch kein bloßes Versprechen, sondern wird mit technischen Mitteln *garantiert*.

Natürlich wirft das weitere Fragen auf:

A6: Womit verdient Signal dann Geld?

*Gar nicht.*

*Signal finanziert sich aus Spenden von Leuten, die einen datenschutzfreundlichen Messenger fördern wollen. Benutzen darf ihn jeder, ob er spendet oder nicht. Deswegen ist es das Versprechen, das Wissen über die Nutzer nicht zu verkaufen, bei Signal ziemlich glaubwürdig.*

A7: Macht Signal das wirklich so wie im Spiel?

*Nein.*

*Das Spiel ist sehr stark vereinfacht, damit man es in der siebten Klasse und auf Papier durchführen kann. Richtige Hashfunktionen sind viel komplizierter, der Austausch der Nummern funktioniert anders, und Signal kann auch nicht jedem alten Client jedesmal die Hashwerte aller neuen Signal-Clients mitteilen.*

*Durch das Spiel bekommt man aber in etwa die richtige Grundvorstellung.*

A8: Ist Signal so komfortabel wie Whatsapp?

*Signal sagt dem Nutzer, welche seiner Freunde Signal haben – wie Whatsapp. Signal hat Einzel- und Gruppenchats, verschickt Bilder und Videos – wie Whatsapp. Den Rest muss man einfach mal ausprobieren.*

A9: Ist Signal so sicher wie Whatsapp?

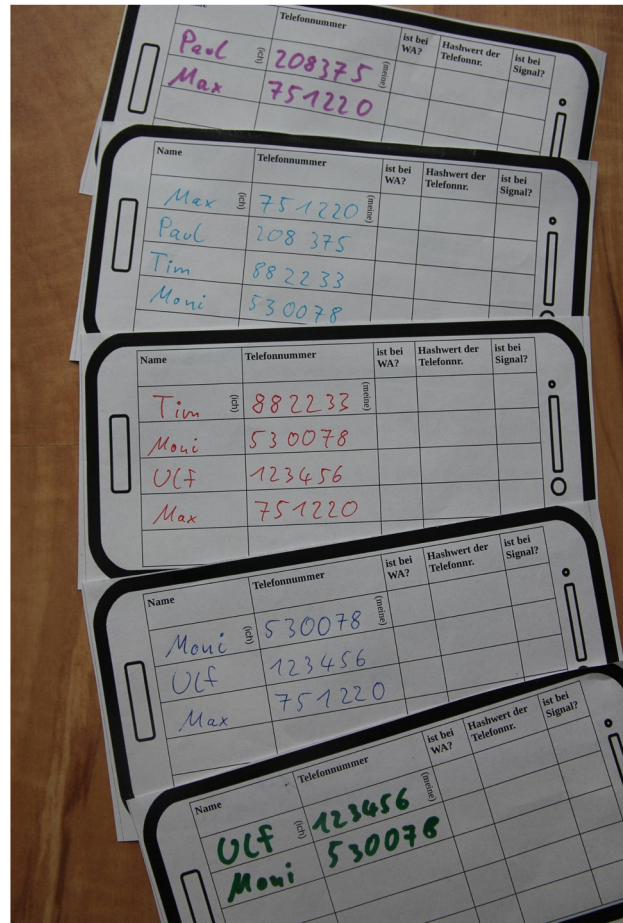
*Signal ist sogar etwas sicherer, denn*

- *Signal ist open source, das heißt jeder darf das Programm anschauen (wenn er weiß, wie man Programme liest). Signal hat also weniger Geheimnisse vor den Nutzern.*
- *Whatsapp verspricht zwar, dass der Whatsapp-Server die Nachrichten beim Weiterleiten nicht mitlesen kann – aber überprüfen kann man das nicht.*
- *Anders als Whatsapp muss Signal kein Geld verdienen, und anders als Whatsapp gehört Signal auch nicht zu Facebook.*
- *Übrigens hat Signal einen Trick erfunden, der es beim Abhören unmöglich macht, auch ältere Nachrichten zu entschlüsseln. Der Trick heißt „Axolotl-Ratsche“ und ist so gut, dass Whatsapp ihn etwas später abgesehen hat und jetzt auch benutzt :-)*

## Beispielhafter Spielverlauf Whatsapp-/Signalrunde



Schritt 5: Schüler tragen sich selbst ins Adressbuch ein



Schritt 6: Schüler tragen Freunde ins Adressbuch ein

gleich der Adressbücher

Serveradressbuch:

Nr.	Name	Telefonnummer	ist bei WA
1:	Paul	208375	✓
2:	Max	751220	✓
3:	Tim	882233	✓
4:	Moni	530078	
5:	Ulf	123456	

Soziogramm:

Nr 1: Paul

Nr 2: Max

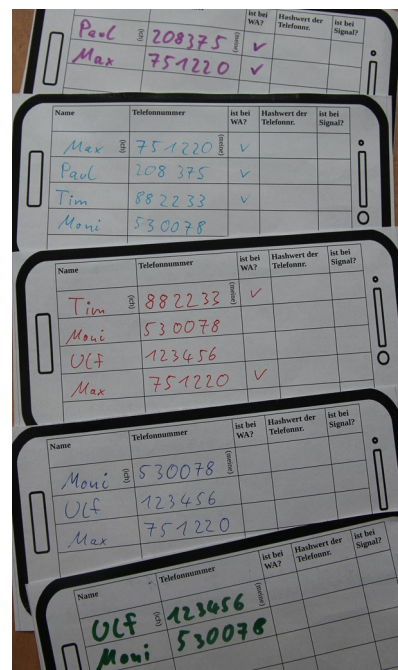
Nr 3: Tim

Nr 4: Moni

Nr 5: Ulf

Dietrich/Lautebach (03/2022) 12 / 18 ZPG Informatik

Whatsapp-Runde (Schritt 7-10):  
Clients melden sich beim Whatsapp-Server an.  
Der erfasst alle Adressbücher  
und erstellt ein Soziogramm



Whatsapp-Runde (Schritt 12-16):  
Whatsapp-Server teilt Clients mit,  
welche ihrer Kontakte auch bei Whatsapp sind





Name	Telefonnummer	ist bei WA?	Hashwert der Telefonnr.	ist bei Signal?
Tim	882233	✓	169	
Moui	530078		98	
ULF	123456		68	
Max	751220	✓	127	

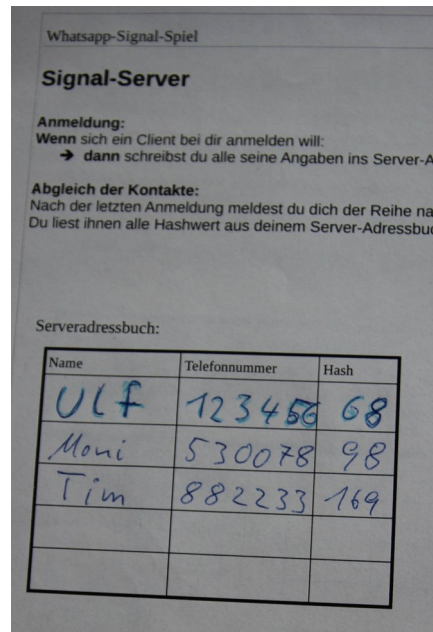
  

Name	Telefonnummer	ist bei WA?	Hashwert der Telefonnr.	ist bei Signal?
Moui	530078		98	
ULF	123456		68	
Max	751220		127	

Name	Telefonnummer	ist bei WA?	Hashwert der Telefonnr.	ist bei Signal?
ULF	123456		68	
Moui	530078		98	

Signal-Runde (Schritt 16):  
Client-Handys berechnen die Hashwerte der Telefonnummer in ihren Adressbüchern



Signal-Runde (Schritt 18-22):  
Clients melden sich beim Signal-Server an.  
Der erfährt nichts über Handys, die sich nicht selber anmelden.

Name	Telefonnummer	ist bei WA?	Hashwert der Telefonnr.	ist bei Signal?
Tim	882233	✓	169	✓
Moui	530078		98	✓
ULF	123456		68	✓
Max	751220	✓	127	✓

Name	Telefonnummer	ist bei WA?	Hashwert der Telefonnr.	ist bei Signal?
Moui	530078		98	✓
ULF	123456		68	✓
Max	751220		127	

Name	Telefonnummer	ist bei WA?	Hashwert der Telefonnr.	ist bei Signal?
ULF	123456		68	✓
Moui	530078		98	✓

Signal-Runde (Schritt 23):  
Der Signal-Server teilt den Client-Handys die Hashwerte der angemeldeten Telefonnummern mit; die Clients markieren sie in ihren Adressbüchern.



## Beide Messenger: Nachrichtenaustausch (Lehrerblatt)

Jetzt können die Clients sich gegenseitig schreiben. Jede Nachricht geht dabei immer vom Absender zunächst an den Whatsapp-Server und von dort zum Empfänger. Die Clients tauschen niemals etwas direkt aus! Warum ist das so?

*Das hat technische Gründe, die z.B. mit Firewall-Regeln zusammenhängen: Clients können Netzwerkverbindungen aufbauen, zum Beispiel zum Server. Sie können aber keine Verbindungen von anderen entgegennehmen, auch nicht von anderen Clients.*

*Es hat bei Whatsapp außerdem mit Geld zu tun: Whatsapp muss mitbekommen, wer wem wann wie viele Nachrichten schickt – genau das ist die Grundlage ihres Geschäfts.*

Diese Spielrunde ist nicht unbedingt nötig. Sie dauert aber auch nur ein paar Minuten und festigt wirksam das Bild vom Client-Server-Modell.

Vor allem bereitet sie den Boden für die anschließende Metadaten-Analyse.



## Bonus: Metadaten-Analyse (Lehrerblatt)

Der Server (egal ob Whatsapp oder Signal) vermittelt Nachrichten zwischen den Clients. Den Inhalt kann er zwar (bei Signal sicher, bei Whatsapp wahrscheinlich) nicht lesen, aber er bekommt mit, wer wann an wen schreibt. Whatsapp protokolliert auch, welches Handy gerade wo ist.

In dieser Runde erfährt man, dass auch diese sogenannten Metadaten überraschend viel über die Beteiligten aussagen.

### Beachvolleyball

Die leichtere Aufgabe „Beachvolleyball“ lösen manche Siebklässler in wenigen Minuten.

1. Wer ist die Trainerin dieser Mannschaft?<sup>1</sup>

### Nachmittag in der 9a

Die zweite Aufgabe ist umfangreicher, schwieriger und die Antworten nicht immer eindeutig. Man kann die Aufgabe so offen stellen wie auf dem Blatt formuliert, oder genauer fragen:

2. Wer ist mit wem befreundet?<sup>2</sup>
3. Wer hat offenbar keine Freunde? Oder, etwas deutlicher: Wer wird gemobbt?<sup>3</sup>
4. Wer ist sportlich?<sup>4</sup>
5. Wer hat die Hausaufgaben vermutlich gemacht, wer vermutlich nicht?<sup>5</sup>
6. Wenn eine Firma das Diagramm kennt, und alle sechs sich für ein Praktikum bewerben: Wer wird wohl zum Vorstellungsgespräch eingeladen, wer nicht, und warum?<sup>6</sup>
7. Wer hat sich möglicherweise verguckt und in wen?<sup>7</sup>
8. Kann man sein Handy so geschickt benutzen, dass man Whatsapp etwas vorspielt?<sup>8</sup>
9. Über wen weiß Whatsapp am wenigsten?<sup>9</sup>

1 Doro muss die Trainerin sein: Sie schreibt nicht oft, aber wenn sie schreibt, dann immer gleich an alle.

2 Alex und Bob: Sie chatten während des Unterrichts und hängen bis abends zusammen ab.

Debbi geht nach der Schule zu Fiona

Sobald Fiona Zeit hat, bespricht Eva mit ihr, wie sie auf die Nachrichten von Bob reagieren soll.

3 Carl schreibt nie und antwortet auch nicht auf Nachrichten von Alex und Bob. Vielleicht mobben sie ihn? Vielleicht ist er immer daheim, vielleicht aber auch unterwegs und hat sein Handy nicht mitgenommen – das kann Whatsapp nicht wissen.

4 Offensichtlich Eva und Fiona, vermutlich auch Alex und Bob.

Whatsapp bekommt aber auch mit, wer wie schnell und ausdauernd Fahrrad fährt. Auch das erlaubt Rückschlüsse.

5 Alex und Bob sehr wahrscheinlich nicht.

Debbi hat ihr Handy eine Weile ausgeschaltet (vielleicht um sich konzentrieren zu können) und postet anschließend Bilder in den Klassenchat (vielleicht die Lösungen).

6 Alex und Bob chatten im Unterricht. Zusammen mit dem Nachmittag im Skaterpark entsteht der Eindruck, dass sie Schule nicht so ernst nehmen. Das kann nun stimmen oder auch nicht, aber wenn die Firma zu viele Bewerbungen hat und sowieso nicht alle zum Vorstellungsgespräch einladen kann...?

Man kann vermuten, dass Debbi ihre Hausaufgaben gewissenhaft macht. Vielleicht würde eine Firma sie bevorzugen.

Auch die beiden Sportlerinnen haben eventuell mehr Ehrgeiz und Durchhaltevermögen als andere und sind dann bessere

Kandidatinnen, zumindest wenn sie erfolgreich Leistungssport machen. Und das weiß Whatsapp: Das Handy bekommt ja mit, ob jemand auf die Landesmeisterschaft geht, oder nur hie und da zum Breitensporttraining.

7 Bob schickt mehrfach Bilder und Videos an Eva, und zwar oft kurz nachdem er sie von Alex bekommen hat.

Vielleicht hat Alex ihn bei gelungenen Tricks gefilmt, und Bob möchte Eva damit beeindrucken.

Auch interessant: Eva antwortet erst, nachdem sie Fiona erreicht und sich mit ihr besprochen hat. Was sagt das über Fiona?

8 Sehr unwahrscheinlich.

Whatsapp kennt immer den Aufenthaltsort, sobald das Handy angeschaltet ist; Whatsapp bekommt viel mehr mit als nur einen Nachmittag; Whatsapp meldet alles an Facebook weiter, wo man zusätzlich noch das Surfverhalten jedes Menschen kennt; und dort arbeiten sehr schlaue Leute ständig an besseren Analysemethoden, die auf Papier gar nicht gehen.

9 Über Carl weiß Whatsapp deutlich weniger als über die anderen, denn er benutzt sein Handy nicht so viel.



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)			



Diese Seite muss nicht kopiert werden.

Das Bild wird als Hintergrund der Zellen der obigen Tabelle verwendet (falls es nochmal benötigt wird:)





# 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.

## Ableich 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.

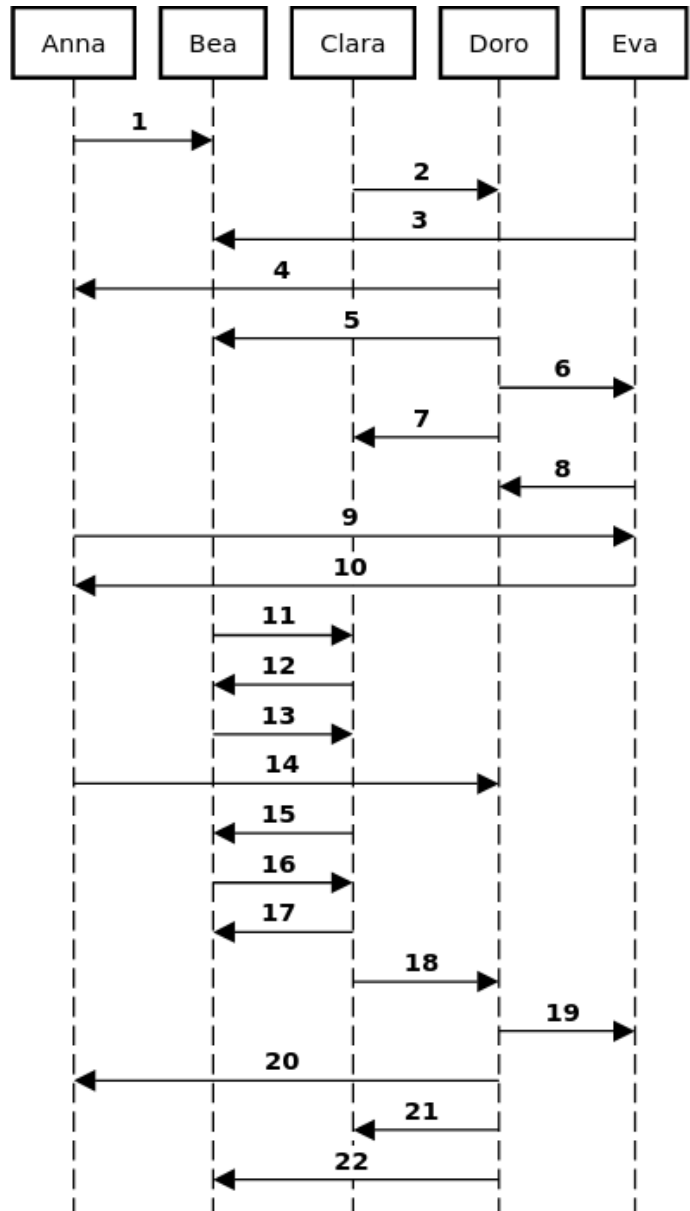
## Sequenzdiagramm: Beachvolleyball

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?

.....  
.....  
.....  
.....  
.....  
.....  
.....  
.....  
.....

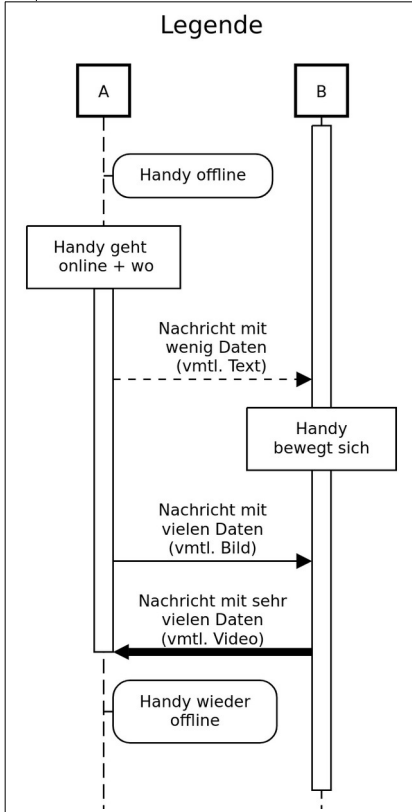




## Sequenzdiagramm: Gestern in der 9a

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.

