Unterrichtseinheit „Klemmchat“

Luisa Gebhardt, Marc Leinweber
Institut für Informationssicherheit und Verlässlichkeit (KASTEL)
Karlsruher Institut für Technologie (KIT)
luisa.gebhardt9@kit.edu, marc.leinweber@kit.edu

In diesem Dokument wird der Unterrichtsentwurf vorgestellt, wie er im Rahmen der Studie zum Papier „Grasping the Concept of Decentralized Systems for Instant Messaging“[1] durchgeführt wurde.

Ziel der Unterrichtseinheit ist, Schüler:innen die Vor- und Nachteile von verschiedenen zentralen oder dezentralen Algorithmen am Beispiel von Instant-Messengern zu vermitteln. Dabei liegt der Fokus auf der Zuverlässigkeit und Machtverteilung in den Messengern und der Einfluss der Zuverlässigkeit und Machtverteilung auf die Nutzung des Messengers.

Klemmchat vereinfacht die komplizierten Algorithmen solcher Messenger, um sie an Schüler:innen ohne technisches Vorwissen und Computer zu vermitteln. Dabei vernachlässigt Klemmchat die Vertraulichkeit der Nachrichten und verwendet keine Verschlüsselungsmechanismen.

Klemmchat simuliert mit Hilfe von Duplo-Steinen, die zwischen Gruppen von Schüler:innen nach Regeln in Abhängigkeit des jeweilig simulierten Algorithmus ausgetauscht werden, einen Gruppenchat, wie er in modernen Messengern existiert. Die Aufgabe der Schüler:innen ist es, nach einer kurzen Erklärung den jeweiligen Algorithmus zu manipulieren, um dem Messenger zu schaden; die Schüler:innen spielen also Angreifer und ehrlicher Anbieter und Nutzer zugleich.

Klemmchat kann dabei flexibel im Unterricht eingesetzt und begleitet werden. In diesem Dokument wird ein exemplarischer Unterrichtsentwurf vorgestellt zum Einsatz von Klemmchat. Folgende Lernziele sollen dabei von den Schüler:innen erreicht werden:

Die Schüler:innen können…

1. …die Grundfunktionalität der verschiedenen (zentralen, verteilten und dezentralen) Algorithmen für Messenger beschreiben.
2. …die Vor- und Nachteile der verschiedenen Algorithmen diskutieren.
3. …den Einsatz der verschiedenen Algorithmen in gegeben Szenarien abwägen.
4. …Messenger basierend auf dem zugrundeliegenden Algorithmus in verschiedenen Szenarien evaluieren.

Aufbau von Klemmchat

Die Kommunikation in einem Messenger erfolgt in den meisten Fällen von einem Client eines Users zu einem Client eines anderen Users. Der Anbieter des Messengers koordiniert den Nachrichtenaustausch und hält bestimmte Teile des Dienstes verfügbar.

Die Clients der User sind die Anwendungen auf den Geräten. Die Nachricht m eines Senders c_1 an Empfänger c_2 wird also von der App auf dem Smartphone an den Server eines Anbieters geschickt. Dieser Anbieter speichert die Nachricht im Nachrichtenverlauf zwischen den Teilnehmenden c_1 und c_2. Dieser Nachrichtenverlauf wird dann von beiden Teilnehmenden regelmäßig zum Lesen beim Anbieter abgerufen. Das Schreiben und Abrufen von Nachrichten kann auf verschieden Arten architekturell und

[1] https://publikationen.bibliothek.kit.edu/1000150316

politisch organisiert werden. In Klemmchat wird eine zentrale, eine verteilte und eine dezentrale Variante simuliert.

Klemmchat benötigt folgende Bestandteile, um die verschiedenen Algorithmen zu simulieren:

Teilnehmende: Eine Gruppe von drei bis vier Schüler:innen simuliert einen Teilnehmenden. Wir unterscheiden nicht zwischen dem User selbst und der Anwendung auf dem Gerät. Die Schüler:innen verkörpern also sowohl User als auch Anwendung.

Nachricht: Eine Nachricht besteht aus einen oder mehreren Duplo-Steinen mit demselben Absender und Nachrichtentext. Der Nachrichtentext wird auf den Stein mithilfe eines Whiteboard-Markers geschrieben.

Absender einer Nachricht: Der Absender einer Nachricht ist durch die Farbe des Nachrichten-Steins angegeben. Um diese Zuordnung eindeutig zu machen, erhält jede Gruppe Steine in einer von den anderen Gruppen unterschiedlichen Farbe.

Empfänger einer Nachricht: Klemmchat simuliert einen Gruppenchat. Eine Nachricht ist immer an alle Teilnehmenden adressiert. Eine explizite Kenntlichmachung eines Empfängers ist nicht notwendig.

Anbieter: Abhängig vom jeweiligen Algorithmus wird der Anbieter von anderen Gruppen/Personen simuliert. Genaueres wird im Absatz über den jeweiligen Algorithmus spezifiziert.

Nachrichtenverlauf: Der Nachrichtenverlauf entsteht, indem ein erhaltener Nachrichten-Stein unten an die bisher erhaltenen Nachrichten-Steine angehangen wird. So entsteht ein Turm an Nachrichten-Steinen. Möchte man den Inhalt eines Nachrichtenverlaufs lesen, so liest man ihn von oben nach unten vor, in dem man für jeden Stein „*Farbe des Senders* schreibt *Nachricht“* sagt.

Schreib- und Lese-Funktionen: Diese Funktionen sind abhängig vom jeweiligen Algorithmus. Um den Ablauf der Algorithmen zu ordnen, gibt es Lese- und Schreibphasen. In einer Schreibphase darf nur geschrieben werden, in der Lese-phase wird einmal der Nachrichtenverlauf gelesen.

Zentraler Algorithmus

Im zentralen Algorithmus wird der Nachrichtenverlauf auf dem Server eines Anbieters gespeichert. Dieser Server wird durch die Lehrkraft gespielt. Es gibt also nur eine Version des Nachrichtenverlaufs. Geht dieser Nachrichtenverlauf verloren oder der Server bzw. die Lehrkraft ist nicht erreichbar oder beschäftigt, so kann nicht gelesen bzw. geschrieben werden.

Möchte eine Gruppe schreiben, so beschriftet die Gruppe einen Stein mit der Nachricht und meldet sich, um zu signalisieren, dass eine Nachricht abgeholt werden kann. Die Lehrkraft läuft dann zu dieser Gruppe und prüft, ob die Farbe des Steins zur Farbe der Gruppe passt. Ist die Prüfung erfolgreich, nimmt die Lehrkraft den Stein und bringt ihn zum Pult, wo der Nachrichtenverlauf liegt, und hängt den Stein an den Nachrichtenverlauf an. Wenn nicht, ignoriert die Lehrkraft den Stein. Zum Lesen liest die Lehrkraft den Nachrichtenverlauf vor.

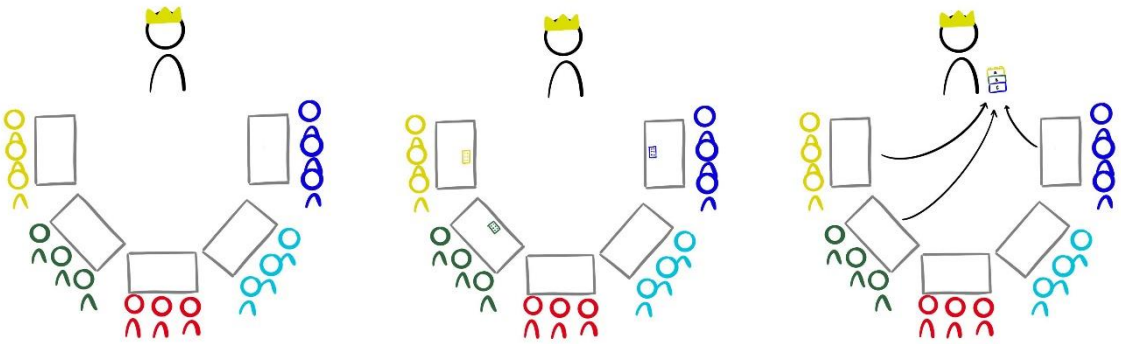

Abbildung 1: Illustration des zentralen Schreibvorgangs: Die gelbe, blaue und grüne Gruppe schreiben jeweils eine Nachricht. Diese werden von der Lehrkraft gesammelt

Folgende Aspekte können durch die Schüler:innen beobachtet werden:

Verlässlichkeit:

- Die Lehrkraft ist mit der Anzahl gleichzeitig zu verarbeitender Meldungen überfordert (Anfälligkeit für DoS-Angriffe).
- Es kann passieren, dass aus Versehen der Nachrichtenverlauf nicht mehr korrekt ist.

⇨ *Die Lehrkraft stellt mit ihrem Nachrichtenverlauf einen Single-Point-of-Failure da. Der Messenger ist nicht sehr zuverlässig, da er oft nicht funktioniert.*

Machtverteilung:

- Die Lehrkraft kann absichtlich die Nachrichten einer Gruppe ignorieren, auch wenn der Absender zur Farbe des Steins passt. Sie kann daher absichtlich strukturell diskriminieren.
- Die Lehrkraft kann fehlerhafte Nachrichten annehmen.
- Die Lehrkraft kann Schimpfwörter zensieren oder nicht annehmen, aber auch Nachrichten, die keinen schadhaften Inhalt haben. Sie kann willkürlich Inhalte zensieren und moderieren.
- Die Lehrkraft kann auch die Inhalte einer Nachricht durch andere ersetzen. Dabei kann Sie sich auch als eine teilnehmende Gruppe ausgeben.

⇨ *Die Teilnehmenden des Dienstes müssen darauf vertrauen, dass der Anbieter/die Lehrkraft im Sinne der Teilnehmenden handelt und ihre Macht über den Messenger nicht eigennützig ausnutzt. Diese Form der Machtverteilung kann mit einer Monarchie verglichen werden.*

Verteilter Algorithmus

Im verteilten Algorithmus wird der Nachrichtenverlauf verteilt auf mehrere Server eines Anbieters gespeichert. Diese Server-Gruppe wird durch eine ausgewählte Gruppe an Schüler:innen *r* gespielt. Dabei besitzt jede:r Schüler:in in Gruppe *r* eine eigene Kopie des Nachrichtenverlaufs auf dem Pult. Es gibt also mehrere Versionen des Nachrichtenverlaufs. Im Idealfall sind diese immer gleich. Die Fähigkeit zur Koordination durch einen einzelnen Anbieter wird durch Absprachen innerhalb der überschaubaren Gruppe an Schüler:innen ermöglicht.

Möchte eine teilnehmende Gruppe schreiben, so beschriftet die Gruppe einen Stein pro Schüler:in in der Gruppe *r* mit der gleichen Nachricht und meldet sich, sodass eine Nachricht bei abgeholt werden kann. Eine Person der Gruppe *r* läuft dann zu dieser Gruppe und prüft, ob die Farbe der Steine zur Farbe der Gruppe und die Steine zueinander passen. Ist die Prüfung erfolgreich, nimmt die abholende Person die Steine und verteilt sie an alle anderen Schüler:innen in Gruppe *r*. Diese bringen ihren Stein dann zum Pult, wo die Nachrichtenverläufe liegen, und hängen den Stein an ihren Nachrichtenverlauf

an. Die Gruppe *r* ignoriert die Nachricht, wenn die Prüfung nicht erfolgreich war. Es können mehrere Nachrichten gleichzeitig von Gruppe *r* angenommen werden. Dies kann zu Vertauschungen im Nachrichtenverlauf führen. Einfache Vertauschungen dürfen manuell aufgelöst werden. Trotzdem ist wichtig, dass die Schüler:innen dieses Problem erkennen.

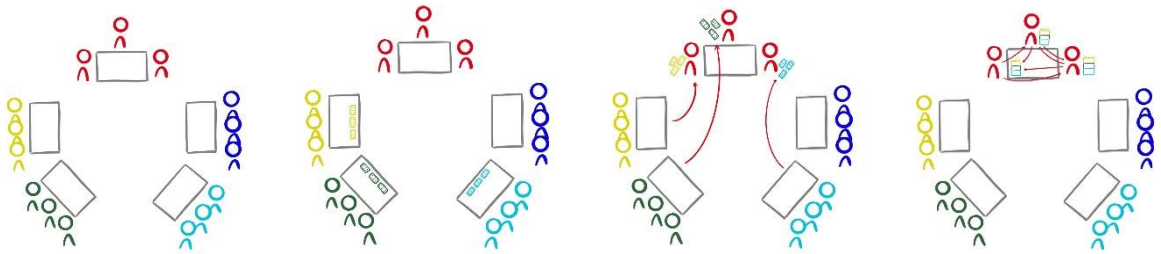

Abbildung 2: Illustration des verteilten Schreibvorgangs: Die hellblaue, gelbe und grüne Gruppe schreiben jeweils eine Nachricht. Diese werden von einer Person der roten Servergruppe *r* gesammelt. Diese Person verteilt dann die Steine an alle anderen in der Servergruppe *r*.

Zum Lesen liest jede Person in Gruppe *r* den Nachrichtenverlauf vor. Dann einigen sich die Schüler:innen in Gruppe *r* auf einen der Nachrichtenverläufe als „richtigen" Verlauf. Sollte es Unstimmigkeiten geben, zählt die Meinung der absoluten Mehrheit. Mit diesem Nachrichtenverlauf wird dann geantwortet.

Folgende Aspekte können durch die Schüler:innen beobachtet werden:

Verlässlichkeit:

- Die Gruppe *r* kann mehrere Meldungen gleichzeitig bearbeiten.
- Geht ein Nachrichtenverlauf kaputt, kann dies durch die Gruppe *r* korrigiert werden, da noch andere Kopien des Verlaufs existieren
- Es ist möglich, dass es keinen vollständig korrekten Nachrichtenverlauf gibt.

⇨ *Der Messenger ist verlässlicher, da es keinen Single-Point-of-Failure mehr gibt.*

Machtverteilung:

- Die Gruppe *r* kann sich absprechen und absichtlich die Nachrichten einer Gruppe ignorieren, auch wenn die Farbe des Steins zum Sender und die Nachrichten untereinander zueinander passen.
- Die Gruppe *r* kann sich absprechen und fehlerhafte Nachrichten annehmen.
- Die Gruppe *r* kann sich absprechen und Schimpfwörter zensieren oder nicht annehmen. Es ist aber auch möglich, gutwillige Nachrichten zu zensieren.
- Die Gruppe *r* kann sich absprechen und fehlerhafte Nachrichten annehmen.
- Die Gruppe *r* kann sich absprechen und die Inhalte einer Nachricht durch andere ersetzen und sich so für eine andere teilnehmende Gruppe ausgeben.

⇨ *Die Teilnehmenden des Dienstes müssen darauf vertrauen, dass der Anbieter/die Gruppe r im Sinne der Teilnehmenden zum Wohle des Messengers handelt und ihre Macht über den Messenger nicht zum eigenen Vorteil ausnutzt. Diese Form der Machtverteilung kann mit einer Oligarchie verglichen werden.*

Sonstiges:

- Der Algorithmus ist aufwändiger und komplizierter.

Dezentraler Algorithmus

Im dezentralen Algorithmus spielt jede Gruppe einen eigenen Server. Server und Client fallen in diesem Experiment zusammen. Die Nachricht wird an eigene, durch die Teilnehmenden gehostete Server, gesendet, welche die Nachrichten mit allen anderen Servern austauschen.

Der Nachrichtenverlauf wird verteilt auf die Server aller Teilnehmenden gespeichert. Jede Gruppe besitzt eine eigene Kopie des Nachrichtenverlaufs auf ihrem Tisch. Es gibt also wieder mehrere Versionen des Nachrichtenverlaufs. Im Idealfall sind diese immer gleich. Die Koordination aller Server ist erschwert, da es keinen einzelnen Anbieter mehr gibt. Eine Absprache zwischen den einzelnen Gruppen zur Koordination von Lese- und Schreibprozess ist dringend notwendig, wenn die Ziele des Messengers erfüllt werden sollen. Aufgrund der Replikation und der Absprachen kann eine Gruppe nicht im Alleingang den Nachrichtenverlauf beliebig manipulieren, ohne dass eine Korrektur möglich wäre.

Da nun die Steine einer Gruppe in die Hände jeder anderen Gruppe kommen kann, reicht die Farbe der Steine allein nicht aus, um Teilnehmende vor Identitätsdiebstahl zu schützen: eine Nachricht kann vom Stein gewischt und der Stein wiederverwendet werden. Deshalb werden zusätzlich digitale Signaturen in Form von buntem Klebeband verwendet. Jeder Gruppe bzw. Steinfarbe kann die Farbe eines bestimmten Klebebands zugeordnet werden. Statt direkt auf den Stein zu schreiben, schreibt eine Gruppe ihre Nachricht auf das eigene Klebeband, welches sie zuvor auf den Stein geklebt hat. Eine Nachricht ist nun nur gültig, wenn die Farbe des Steins und die Farbe des Klebebandes zu der Identität des Senders passt. Die Nachricht kann nun nicht mehr rückstandsfrei entfernt werden, ohne die Nachricht ungültig zu machen, da das Klebeband nicht abwischbar ist. Das Klebeband einer Gruppe darf niemals an eine andere Gruppe weitergegeben werden.

Möchte eine teilnehmende Gruppe schreiben, so beschriftet die Gruppe einen Stein pro anderer Gruppe mit der gleichen Nachricht auf Klebeband und meldet sich, sodass eine Nachricht bei abgeholt werden kann. Eine Person jeder anderen Gruppe läuft dann zur schreibenden Gruppe und prüft, ob die Nachricht gültig ist und die Steine zueinander passen. Ist die Prüfung erfolgreich, bringt jede dieser Personen den Stein zum eigenen Tisch, wo der Nachrichtenverlauf der Gruppe liegt, und hängt den Stein an ihren Nachrichtenverlauf an. Anderenfalls ignoriert die Gruppe die Nachricht. Es können wieder mehrere Nachrichten gleichzeitig von den Servern angenommen werden. Dies kann zu Vertauschungen im Nachrichtenverlauf führen. Einfache Vertauschungen dürfen manuell aufgelöst werden. Weiterhin ist wichtig, dass die Schüler:innen dieses Problem erkennen und merken, dass es in diesem Algorithmus weitaus schwieriger ist, die Nachrichtenverläufe konsistent zu halten.

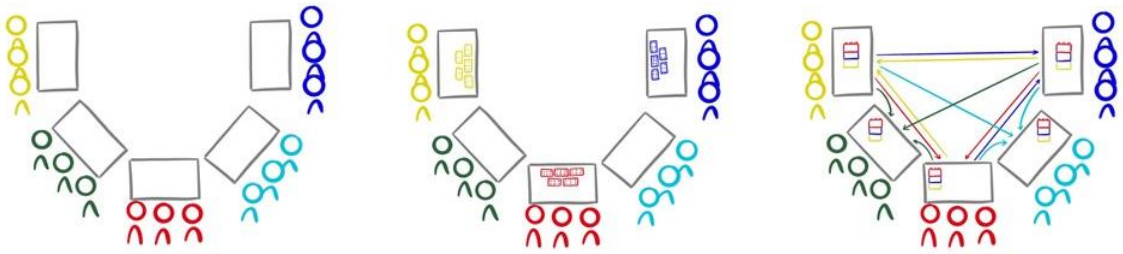

Abbildung 3: Illustration des dezentralen Schreibvorgangs: Die gelbe, rote und blaue Gruppe schreiben jeweils eine Nachricht. Eine Person jeder anderen Gruppe holt dann eine oder mehrere Nachrichten der anderen Gruppen ab.

Zum Lesen liest ein Repräsentant jeder Gruppe den eigenen Nachrichtenverlauf vor. Dann einigen sich die Repräsentanten jeder Gruppe auf einen der Nachrichtenverläufe als „richtigen“ Verlauf. Sollte es

Unstimmigkeiten geben, zählt die Meinung der absoluten Mehrheit. Mit diesem Nachrichtenverlauf wird dann geantwortet.

Folgende Aspekte können durch die Schüler:innen beobachtet werden:

Verlässlichkeit:

- Die Server können mehrere Meldungen gleichzeitig bearbeiten.
- Geht ein Nachrichtenverlauf kaputt, kann dies korrigiert werden, da noch andere Kopien des Verlaufs existieren.
- Es ist möglich, dass es keinen vollständig korrekten Nachrichtenverlauf gibt.
- ⇨ *Der Messenger ist verlässlicher, da es keinen Single-Point-of-Failure mehr gibt. Eine Einigung kann jedoch schwerer sein und es ist unwahrscheinlicher, dass es einen fehlerfreien Verlauf gibt.*

Machtverteilung:

- Die Mehrheit der Gruppen muss sich absprechen, um fehlerhafte Nachrichten anzunehmen, richtige Nachrichten abzulehnen, aber auch um Schimpfwörter zu zensieren.
- Zensur oder Moderation von Inhalten ist nur noch erschwert möglich, da immer Mehrheitsentscheidungen nötig sind. Aufgrund der mangelnden Moderation können einzelne Teilnehmende von anderen, wenigen Teilnehmenden in Chatnachrichten diskriminiert werden.
- Aufgrund der Signaturen kann der Nachrichteninhalt nicht nachträglich verändert werden.
- ⇨ *Die Teilnehmenden des Dienstes müssen nicht mehr darauf vertrauen, dass ein Anbieter im Sinne der Teilnehmenden handelt und eine Machtausnutzung durch einzelne Anbieter ist ausgeschlossen. Das nötige Vertrauen wird statt auf einzelne auf die Mehrheit einer Föderation gelegt. Diese Machtform ist vergleichbar mit einer Demokratie.*

Sonstiges:

- Aufgrund der Koordination zwischen den Gruppen und der durch die Gruppen redundant zu erledigenden Arbeit, ist der Algorithmus ist aufwändiger und komplizierter als die zentrale und die verteilte Variante.

Anmerkung:

Anstelle des Vorlesens der Nachrichtenverläufe, können diese auch unter einen Visualizer oder eine Dokumentenkamera gehalten werden. Wichtig ist nur, dass die Schüler:innen die Nachrichtenverläufe wahrnehmen können. In diesem Fall ist es dann auch möglich, dass beim Vorlesen etwas anderes gelesen wird, als tatsächlich im Verlauf steht. Angriffe, die von Schüler:innen nicht beobachtet werden, haben in Klemmchat keinen Zweck.

Unterrichtsentwurf zur beispielhaften Einbettung von Klemmchat

In der folgenden Tabelle ist ein exemplarischer Unterrichtsablauf gegeben, der die zuvor beschrieben Algorithmen und die dazugehörigen Lernziele vermittelt. Er richtet sich an Schüler:innen ab der 10. Klasse. Insbesondere ist es hilfreich, wenn die Schüler:innen bereits Wissen über die Machtverteilung in politischen Systemen besitzen.

Die Zeitangaben sind sehr knapp bemessen; es lohnt sich, die einzelnen Experimente und Diskussionen zu verlängern und ihnen mehr Raum zu geben.

Zeit	Phase	Inhalt	Aktivität
00:00 5 min	Einstieg	Begrüßung, Ziele der Stunde, Einstiegsfrage zu genutzten Messengern der Schüler:innen	Lehrer-Schüler-Gespräch
00:05 10 min		Erklärung des grundlegenden Aufbaus eines Messengers und Klemmchat, Hinweis zur fehlenden Verschlüsselung	Frontalvortrag
00:15 5 min	**Experiment 1:** Einstieg	Erklärung des zentralen Algorithmus	Frontalvortrag
00:20 10 min	Erarbeitung	Simulieren des zentralen Algorithmus in mehreren Runden. Jede Runde besteht aus einer Schreib- und einer Lesephase. Nach jeder Runde werden alle Auffälligkeiten gesammelt. Außerdem kann der Messenger zurückgesetzt werden (Steine zurückgeben). In der ersten Runde sollten noch keine Manipulationsversuche durchgeführt werden. In den folgenden Runden sollen oben beschriebene Eigenschaften explorativ entdeckt werden. Die Lehrkraft kann hierbei unterstützen.	Gruppenarbeit
00:30 5 min	Ergebnissicherung	Zusammenfassung der Auffälligkeiten. Dabei soll die zentrale Stellung und das Vertrauen in den Anbieter sowie die Verbindung zu Machtverteilung betont werden.	Lehrer-Schüler-Gespräch
00:35 5 min	**Experiment 2:** Einstieg	Erklärung des verteilten Algorithmus	Frontalvortrag
00:40 10 min	Erarbeitung	Simulieren des verteilten Algorithmus in mehreren Runden (siehe zentraler Algorithmus).	Gruppenarbeit
00:50 10 min	Ergebnissicherung	Zusammenfassung der Auffälligkeiten. Es ist wichtig, dass durch einen Vergleich zum vorherigem Algorithmus Unterschiede und Gemeinsamkeiten herausgearbeitet werden.	Lehrer-Schüler-Gespräch
01:00 5 min	**Experiment 3:** Einstieg	Erklärung des dezentralen Algorithmus	Frontalvortrag
01:05 10 min	Erarbeitung	Simulieren des dezentralen Algorithmus in mehreren Runden (siehe zentraler Algorithmus).	Gruppenarbeit
01:15 5 min	Ergebnissicherung	Zusammenfassung der Auffälligkeiten. Es ist wichtig, dass durch einen Vergleich zu den beiden vorherigen Algorithmen Unterschiede und Gemeinsamkeiten herausgearbeitet werden.	Lehrer-Schüler-Gespräch
01:20 10 min	Abschlussreflexion	Reflexionsfragen: • Welchen Algorithmus würden die Schüler:innen für einen eigenen Messenger wählen? Wieso? • Welchen Algorithmus nutzen die Messenger, die anfänglich durch die Schüler:innen genannt wurden? • Beeinflusst das Gelernte die Nutzungsentscheidung der Schüler:innen?	Lehrer-Schüler-Gespräch