

Dezentralisierte asymmetrische Verschlüsselung über Tor: Die Lösung für sicheres Messaging?

Windthorst-Gymnasium Meppen

18. November 2023

Inhaltsverzeichnis

1	Motivation	1
1.1	Tor-Netzwerk	1
1.2	Asymmetrische Verschlüsselung	1
1.3	Programmatischer Aspekt	1
2	Relevanz	1
3	Methodisches Vorgehen	1
3.1	Problemerkfassung	1
3.2	Aneignung von Wissen	2
3.2.1	asymmetrische Verschlüsselung	2
3.2.2	Tor-Netzwerk	2
3.3	Aufbau	2
4	Hypothesen	2
4.1	Zu viel Sicherheit - Kriminalität wird verstärkt	2
4.2	Meinungsfreiheit wird gefördert	2
4.3	Nicht umsetzbar in herkömmlichen Messengern	3

1 Motivation

Mein Interesse zu diesem Themenkomplex erstreckt sich über mehrere Ebenen. Neben der asymmetrischen und der dahinterliegenden Mathematik, gehört die Programmierung selbst und die Umsetzung eines sicheren Messengers im Tor-Netzwerk zu meiner Hauptmotivation
5 mich diesem komplexen Thema anzunehmen.

1.1 Tor-Netzwerk

Das Tor-Netzwerk und die Struktur dessen verfolge ich schon seit ein paar Jahren mit hohem Interesse. Oftmals ist das Tor-Netzwerk mit dem Begriff des Darknets verbunden, wodurch es bei den meisten Menschen negative Assoziationen hervorruft. Vor alldem die schwierige
10 Rückverfolgung spielt eine große Rolle in dem Darknet. Sie ist der Grund für mein Interesse, die Struktur zu verstehen und darauf einen neuartigen Messenger zu programmieren.

1.2 Asymmetrische Verschlüsselung

Innerhalb der asymmetrischen Verschlüsselung steht für mich ein mathematischer Erklärungsansatz mit unter im Vordergrund meines Interesses: "Wie schafft es der Angreifer nur
15 mit dem öffentlichen Schlüssel eine verschlüsselte Nachricht nicht entschlüsseln zu können".

1.3 Programmatischer Aspekt

Die höchste Aufmerksamkeit gilt der Programmierung selbst. Die vielen Facetten des Tor-Netzwerkes mit der asymmetrischen Verschlüsselung zu verknüpfen, sodass am Ende ein funktionierender Messenger entsteht. Die Dezentralisierung des Messengers tragen nochmals
20 zu der Schwierigkeit bei, sodass tiefe Kenntnisse der Informatik gefragt sind. Auch um dieses Wissen zu erlangen bin ich Feuer und Flamme.

2 Relevanz

In der heutigen Zeit spielt die Sicherheit in der Informatik eine immer größere Rolle. Besonders bei Messengern wird dieser Aspekt nochmals wichtiger, hier geht es um personenbezo-
25 gene und sensible Daten. Auch in Ländern mit eingeschränkter oder gar keiner Meinungsfreiheit wird Sicherheit und Anonymität wichtiger denn je. Über einen Tor-Messenger können Meinungen und Sichtweisen das autoritäre Land verlassen und aufklären. Die asymmetrische Verschlüsselung steht dabei natürlich im Mittelpunkt. Ohne sie kann selbst der autoritäre Staat auf die Daten zugreifen und die Person ausfindig machen. Fast jeder benutzt heut-
30 zutage Messenger, egal ob nur zum Verabreden mit einer Person oder zum Schreiben von Nachrichten an ein Business und auch hier wird wieder die Frage wichtig: Wie sicher ist das eigentlich?

3 Methodisches Vorgehen

In dieser Sektion werde ich beschreiben, wie ich in der Facharbeit vorgehen werde, bzw.
35 welche Schritte in welcher Reihenfolge wichtig sind.

3.1 Problemerkfassung

Zuerst muss man sich erstmal im Klaren sein, was überhaupt ein Messenger ist bzw. wie er funktioniert und natürlich auch, ob und welche Verschlüsselungsmethoden benutzt werden, um unsere täglichen Nachrichten sicher zu halten. Dazu sei gesagt, dass hier ein umfangrei-
40 ches Wissen wichtig ist, da es sehr viele verschiedene Messenger gibt, welche ihren Schwerpunkt unter anderem anderes gesetzt haben. Zum Beispiel auf Twitter, wo die Direktnachrichten nur eine „Nebenfunktion“ der Plattform sind und auf der anderen Seite Whatsapp, wessen Hauptzweck das Nachrichten verschicken ist. Hierzu muss das Problem erfasst und formuliert werden.

45 3.2 Aneignung von Wissen

Für eine Facharbeit darf das Aneignen von Wissen aus zum Beispiel Studien und Literatur nicht fehlen, um einen umfassenden Blick auf das Thema zu erlangen.

3.2.1 asymmetrische Verschlüsselung

50 Um einen sicheren Messenger zu programmieren, welcher Nachrichten mithilfe von asymmetrischer Verschlüsselung verschlüsselt, ist es natürlich wichtig das Konzept und die Mathematik hinter diesem Verfahren erstmal zu verstehen. Dazu werde ich mir Studien und weitere Literatur anschauen und besonderen Fokus auf die Sicherheit dieses Verschlüsselungsverfahrens legen.

3.2.2 Tor-Netzwerk

55 Das Tor-Netzwerk ist ein weiterer Baustein dieser Facharbeit. Mit dem Tor-Netzwerk lassen sich sicher und anonym Datenpakete verschicken, jedoch muss man hierfür vorher die Infrastruktur dieses Netzwerkes verstehen und in Quellcode umsetzen können. Auch hierfür werde ich in zahlreiche Studien einen Blick werfen. Das Tor-Netzwerk muss in der Facharbeit aufgeführt werden, sodass der Leser die Teile des Netzwerkes versteht und Verknüpfungen
60 zwischen den verschiedenen Komponenten des Messengers klar werden.

3.3 Aufbau

Ich werde meine Facharbeit mit einer Einleitung starten, welche das Problem vorstellt und versucht das Interesse des Lesers zu erfassen. Danach erkläre ich, was überhaupt ein Messenger ist bzw. welche Messenger gerade statistisch gesehen die größten und meistbenutzten sind.
65 Hierbei werde ich auf mögliche Sicherheitsbedenken aufmerksam machen und zur asymmetrischen Verschlüsselung überleiten. Hier werde ich erklären, wie asymmetrische Verschlüsselung funktioniert und warum sie so wichtig in unserem Alltag ist. Da das Tor-Netzwerk auch asymmetrische Verschlüsselungen benutzt, lässt sich zu dem Netzwerk gut überleiten. Folglich werde ich hier die Struktur des Tor-Netzwerkes elaborieren und die
70 Nutzen des Tor-Netzwerkes für den Messenger ausformulieren, wobei die Dezentralisierung ein wichtiges Detail ist, da somit keine kompromittierten Server auftreten können (bis auf infizierte Clients). Wenn die Theorie und die Umsetzung des Messengers geklärt ist, gehe ich in die Programmierung über und lasse den Leser an meiner Umsetzung teilhaben. Das Programm wird in der Programmiersprache „Rust“ programmiert sein, welche mir ermöglicht,
75 den Messenger in eine einzige ausführbare Datei zu compilieren, sodass für den Benutzer eine einfache Anwendung ermöglichen soll.

4 Hypothesen

Meiner Meinung nach, gibt es zu diesem Thema drei mögliche Hypothesen:

4.1 Zu viel Sicherheit - Kriminalität wird verstärkt

80 Durch einen Messenger über das Tor-Netzwerk ist es für die Behörden eines Landes *fast* unmöglich den Absender bzw. den Empfänger ausfindig zu machen. Somit wird die Kriminalität über das Tor-Netzwerk nur noch verstärkt und Kriminelle weichen von herkömmlichen Messengern auf einen sicheren Messenger über das Tor-Netzwerk aus.

4.2 Meinungsfreiheit wird gefördert

85 Eine andere Hypothese ist es, dass die Meinungsfreiheit, vor allem in Ländern mit starker Zensur, gefördert wird, eben weil die Anwendung dieses Messengers möglich leicht sein soll. Somit bekommen andere Länder besseren Einblick in autoritäre Länder und werden zusätzlich informiert.

4.3 Nicht umsetzbar in herkömmlichen Messengern

- ⁹⁰ Dieser Messenger ist nicht umsetzbar in herkömmlichen Messengern, da er über das Tor-Netzwerk fungiert, welches zwar sicher ist, jedoch sehr viel langsamer als ein zentralisiertes unverschlüsseltes Netzwerk. Durch die zusätzlichen Verschlüsselungen des vorgeschlagenen Messengers, wird die benötigte Zeit, um eine Nachricht zu verschicken nochmals verlängert.