Dezentralisierte asymmetrische Verschlüsselung über Tor

Die Lösung für sicheres Messaging?

Hendrik Lind

Facharbeit

Windthorst-Gymnasium Meppen

Seminarfach Informatik

21. Januar 2024

Inhaltsverzeichnis

1 Einleitung

Russland, China, Iran. In all diesen totalitären Staaten herrscht eine starke Zensur [vgl. Am23]. Rund 1,7 Milliarden Menschen sind allein nur in diesen drei Staaten von der Einschränkung der Meinungsfreiheit betroffen [vgl. Un22]. Wie können Bürger dieser Staaten ihre Meinung also verbreiten und andere Staaten auf staatskritische Probleme aufmerksam machen ohne sich selber in Gefahr zu bringen?

Bei herkömmlichen Messengern, wie Whatsapp, Signal und co., braucht die Außenwelt die Telefonnummern der im totalitären Staat wohnenden Bürgern und Reportern, um diese zu kontaktieren. Allerdings könnte ein totalitärer Staat, sich als Empfänger ausgeben, sodass Bürger/Reporter ihre private Nummer an den Staat überreichen und dieser somit jene Nummer rückverfolgen kann [vgl. Fä23]. Und genau hier liegt das Problem: Bürger und Reporter können nicht durch alltägliche Messenger mit der Außenwelt kommunizieren, da der Staat deren Nummer zurückverfolgen kann und somit weiter die Meinungsfreiheit einschränkt und unterbindet.

Durch die zentrale Infrastruktur, welche die meisten Messenger, wie zum Beispiel WhatsApp und Signal verwenden, ist es für totalitäre Staaten, wie China, möglich, die IP-Adressen jener Server zu blockieren und somit für Bürger und Reporter unzugänglich zu machen [vgl. Wu+23].

Ein dezentralisierter Messenger, welcher Ende-zu-Ende verschlüsselt ist und über das Tor-Netzwerk kommuniziert, könnte bei diesen Problemen eine Lösung sein. Die Frage, ob ein solcher Messenger die Lösung für Bürger eines totalitären Staates ist, soll in dieser Arbeit geklärt werden.

Um diese Frage beantworten zu können, beschäftigt sich diese Arbeit in dem zweiten Kapitel mit der asymmetrischen Verschlüsselung, welche benötigt wird um die Ende-zu-Ende-Verschlüsselung (E2EE) umzusetzen und die Definition der E2EE und asymmetrischen Verschlüsselung [vgl. LB21]. Das dritte Kapitel beinhaltet eine mögliche Lösung, um eine Anonymität über das Internet zu gewährleisten, wobei das Tor-Netzwerk eine wichtige Rolle spielt. Im vierte Kapitel befasst sich diese Arbeit mit einer Dezentralisierung der Infrastruktur, um eine weitere Sicherheitsebene zu schaffen. Zuletzt werden im fünften Kapitel die Vor- und Nachteile eines solchen Messengers betrachtet, im sechsten Kapitel wird eine mögliche Umsetzung des

Messengers beschrieben und im siebten Kapitel wird ein Fazit gezogen.

2 Asymmetrische Verschlüsselung

Um einen sicheren Nachrichtenaustausch zu gewährleisten, wird in dieser Arbeit die E2EE implementiert. Bei der E2EE wird von dem Sender die Nachricht, bevor sie an den Empfänger geschickt wird, verschlüsselt [vgl. Gr14]. Dazwischenliegende Akteure, wie zum Beispiel Server oder mögliche Angreifer, können demzufolge die Nachricht nicht lesen. **Nur** der Empfänger der Nachricht kann diese auch entschlüsseln. Als Ent- und Verschlüsselungsverfahren der Nachrichten wird die asymmetrische Verschlüsselung verwendet. Für diese Arbeit werde ich die gängigste asymmetrische Verschlüsselung, das RSA-Verfahren, verwenden.

2.1 Grundlagen

Grundsätzlich gibt es bei der asymmetrischen Verschlüsselung ein Schlüsselpaar (Keypair), welches aus einem privaten Schlüssel (private key) und einem öffentlichen Schlüssel (public key) besteht [vgl. BSW15b]. Diese beiden Schlüssel hängen mathematisch zusammen, sodass der öffentliche Schlüssel Nachrichten **nur** verschlüsseln und nicht entschlüsseln kann. **Nur** der zum Schlüsselpaar dazugehörige private Schlüssel ist in der Lage, die verschlüsselte Nachricht wieder zu entschlüsseln (siehe Abb. 1).

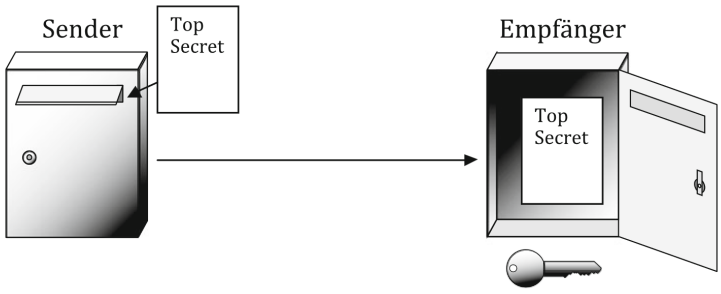

Abbildung 1: Jeder Sender kann mit dem öffentlichen Schlüssel die Nachricht „verschlüsseln“ (also in den Briefkasten eine Nachricht werfen), aber nur der Empfänger kann den Briefkasten mit seinem privaten Schlüssel öffnen [vgl. BSW15a]

2.2 Mathematische Betrachtung

Alle Variablen der folgenden Berechnungen liegen im Bereich $\mathbb{N}$.

Für die Generierung des Schlüsselpaares benötigen wir zuerst zwei große zufällige Primzahlen, P und Q. Daraus ergibt sich $n = P * Q$, wobei $P \neq Q$, sodass P bzw. Q nicht durch $\sqrt{n}$ ermittelt werden kann [vgl. Is16]. Der private Schlüssel besteht aus den Komponenten $\{n, d\}$ währenddessen der öffentliche Schlüssel aus $\{n, e\}$ besteht [vgl. Wa+13].

2.2.1 Eulersche Phi-Funktion

Die Eulersche Phi-Funktion spielt eine wichtige Rolle in dem RSA-Verfahren [vgl. Tu08]. Grundsätzlich gibt $\phi(x)$ an, wie viele positive teilerfremde Zahlen bis x existieren (wo also der größte gemeinsamer Teiler (gcd) 1 ist) [vgl. Ta13]. Somit ergibt $\phi(6) = 2$ oder bei einer Primzahl $\phi(7) = 7 - 1 = 6$ somit $\phi(x) = x - 1$, wenn x eine Primzahl ist, da jede Zahl kleiner als x teilerfremd sein muss.

$$\begin{aligned} \phi(n) &= \phi(P \cdot Q) \\ \phi(n) &= \phi(P) \cdot \phi(Q) \\ \phi(P) &= P - 1 \qquad\qquad \phi(Q) = Q - 1 \\ \phi(n) &= (P - 1) \cdot (Q - 1) \end{aligned}$$

[vgl. Tu08]

2.2.2 Generierung des Schlüsselpaares

Sowohl der private als auch der öffentliche Schlüssel besteht unter anderem aus folgender Komponente: $n = P \cdot Q$. Für den öffentlichen Schlüssel benötigen wir die Komponente e, welche zur Verschlüsselung einer Nachricht benötigt wird. e ist hierbei eine zufällige Zahl, bei welcher folgende Bedingungen gelten [vgl. Ta96]:

$$e = \begin{cases} 1 < e < \phi(n) \\ \text{gcd}(e, \phi(n)) = 1 \\ e \text{ kein Teiler von } \phi(n) \end{cases}$$

Mit der errechneten Komponente e, welche Nachrichten verschlüsselt, kann der öffentliche Schlüssel nun an den Sender übermittelt werden.

Um den privaten Schlüssel zu berechnen benötigen wir die Komponente d, welche zur Entschlüsselung verwendet wird [vgl. MS13].

$$\phi(n) = (P-1)(Q-1)$$
$$e * d = 1 \mod \phi(n)$$

2.3 Sicherheit

Das RSA-Verfahren macht sich die Trapdoor-Einwegfunktion zu Nutze. Das bedeutet, dass eine Funktion mit modernen Computern unmöglich ist, zu invertieren, wenn eine Komponente fehlt (in diesem Fall d). Wenn diese jedoch gegeben ist, ist die Umkehroperation leicht. Zu sehen ist dies bei der Ver-/Entschlüsselung von Nachrichten mit dem öffentlichen und privaten Schlüssel [vgl. Kr16].

$c = m^e \mod n$ Verschlüsselung zu c mit m als Nachricht

$m = c^d \mod n$ Umkehroperation (Entschlüsslung) von c zu m

Um die verschlüsselte Nachricht c zu entschlüsseln, bräuchte ein möglicher Angreifer die Komponente des privaten Schlüssels d. Diese ist allerdings schwer zu berechnen, da, wie schon vorher bereits gezeigt, dafür $\phi(n)$ benötigt wird. Auch $\phi(n)$ ist rechenaufwendig, da dafür eine Primfaktorzerlegung von n benötigt wird. Wichtig hierbei ist aber, dass die Länge von n (Schlüssellänge) mindestens 3000 Bit betragen sollte, da sonst die Primfaktorzerlegung von n mit modernen Computern möglich sein könnte [vgl. Si23].

3 Anonymität mit dem Tor-Netzwerk

3.1 Sicherheit

4 Dezentralisierung

4.1 Sicherheit

5 Vor- und Nachteile

5.1 Kriminalität

5.2 freie Meinungsäußerung

6 programmatische Umsetzung

7 Fazit

Literatur

[Ta96] D. Taipale. „Implementing the Rivest, Shamir, Adleman cryptographic algorithm on the Motorola 56300 family of digital signal processors“. In: *Southcon/96 Conference Record*. Juni 1996, S. 10–17. DOI: 10.1109/SOUTHC.1996.535035.

[Tu08] Clay S Turner. „Euler's totient function and public key cryptography“. In: *Nov* 7 (2008), S. 138.

[MS13] Prerna Mahajan und Abhishek Sachdeva. „A study of encryption algorithms AES, DES and RSA for security“. In: *Global Journal of Computer Science and Technology* 13.15 (2013), S. 15–22.

[Ta13] Marius Tarnauceanu. *A generalization of the Euler's totient function*. 2013. DOI: 10.48550/arXiv.1312.1428. arXiv: 1312.1428 [math.GR]. URL: https://doi.org/10.48550/arXiv.1312.1428.

[Wa+13] Hongjun Wang, Zhiwen Song, Xiaoyu Niu und Qun Ding. „Key generation research of RSA public cryptosystem and Matlab implement“. In: *PROCEEDINGS OF 2013 International Conference on Sensor Network Security Technology and Privacy Communication System*. 2013, S. 125–129. DOI: 10.1109/SNS-PCS.2013.6553849.

[Gr14] Andy Greenberg. „Hacker Lexicon: What Is End-to-End Encryption?“ In: *WIRED* (Nov. 2014). URL: https://www.wired.com/2014/11/hacker-lexicon-end-to-end-encryption (besucht am 16. 01. 2024).

[BSW15b] Albrecht Beutelspacher, Jörg Schwenk und Klaus-Dieter Wolfenstetter. „Ziele der Kryptographie“. In: *Moderne Verfahren der Kryptographie: Von RSA zu Zero-Knowledge*. Wiesbaden: Springer Fachmedien Wiesbaden, 2015, S. 1–7. ISBN: 978-3-8348-2322-9. DOI: 10.1007/978-3-8348-2322-9_1. URL: https://doi.org/10.1007/978-3-8348-2322-9_1.

[Is16] Ni Made Satvika Iswari. „Key generation algorithm design combination of RSA and ElGamal algorithm“. In: *2016 8th International Conference on Information Technology and Electrical Engineering (ICITEE)*. 2016, S. 1–5. DOI: 10.1109/ICITEED.2016.7863255.

[Kr16] N. Krzyworzeka. „Asymmetric cryptography and trapdoor one-way functions“. In: *Automatyka / Automatics* 20.2 (2016), S. 39–51. ISSN: 1429-3447. DOI: 10.7494/automat.2016.20.2.39.

[LB21] Ben Lutkevich und Madelyn Bacon. „end-to-end encryption (E2EE)“. In: *Security* (Juni 2021). URL: https://www.techtarget.com/searchsecurity/definition/end-to-end-encryption-E2EE (besucht am 16. 01. 2024).

[Un22] United Nations. *World Population Prospects - Population Division*. Jan. 2022. URL: https://population.un.org/wpp/Download/Files/1_Indicators%20(Standard)/EXCEL_FILES/1_General/WPP2022_GEN_F01_DEMOGRAPHIC_INDICATORS_COMPACT_REV1.xlsx (besucht am 13. 01. 2024).

[Am23] Amnesty International. *Amnesty International Report 2022/23*. London WC1X 0DW, United Kingdom: International Amnesty Ltd, 2023, S. 307–312, 122–128, 196–201. ISBN: 978-0-86210-502-0. URL: https://www.amnesty.org/en/wp-content/uploads/2023/04/WEBPOL1056702023ENGLISH-2.pdf (besucht am 13. 01. 2024).

[Fä23] Jan Fährmann. „Rechtliche Rahmenbedingungen der Nutzung von Positionsdaten durch die Polizei und deren mögliche Umsetzung in die Praxis–zwischen Strafverfolgung und Hilfe zur Wiedererlangung des Diebesguts“. In: *Private Positionsdaten und polizeiliche Aufklärung von Diebstählen*. Nomos Verlagsgesellschaft mbH & Co. KG. 2023, S. 141–176. ISBN: 978-3-8487-5905-7.

[Si23] Bundesamt für Sicherheit in der Informationstechnik. *BSI TR-02102-1 Kryptographische Verfahren: Empfehlungen und Schlüssellängen*. Bundesamt für Sicherheit in der Informationstechnik, Jan. 2023, S. 39–41. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.pdf?__blob=publicationFile&v=9 (besucht am 21. 01. 2024).

[Wu+23] Mingshi Wu, Jackson Sippe, Danesh Sivakumar, Jack Burg, Peter Anderson, Xiaokang Wang, Kevin Bock, Amir Houmansadr, Dave Levin und

Eric Wustrow. „How the Great Firewall of China Detects and Blocks Fully Encrypted Traffic“. In: *32nd USENIX Security Symposium (USENIX Security 23)*. Anaheim, CA: USENIX Association, Aug. 2023, S. 2653–2670. ISBN: 978-1-939133-37-3. URL: https://www.usenix.org/conference/usenixsecurity23/presentation/wu-mingshi (besucht am 14. 01. 2024).

Anhang

[BSW15a] Albrecht Beutelspacher, Jörg Schwenk und Klaus-Dieter Wolfenstetter. „Kryptologische Grundlagen“. In: *Moderne Verfahren der Kryptographie: Von RSA zu Zero-Knowledge*. Wiesbaden: Springer Fachmedien Wiesbaden, 2015, S. 9–30. ISBN: 978-3-8348-2322-9. DOI: 10.1007/978-3-8348-2322-9_2. URL: https://doi.org/10.1007/978-3-8348-2322-9_2.