

# **Dezentralisierte asymmetrische Verschlüsselung über Tor**

Die Lösung für sicheres Messaging?

---

Hendrik Lind

Facharbeit

Windthorst-Gymnasium Meppen

Seminarfach Informatik

8. Februar 2024

# Inhaltsverzeichnis

<b>1</b>	<b>Einleitung</b>	<b>1</b>
<b>2</b>	<b>Asymmetrische Verschlüsselung</b>	<b>2</b>
2.1	Grundlagen . . . . .	2
2.2	Mathematische Betrachtung . . . . .	3
2.2.1	Eulersche Phi-Funktion . . . . .	3
2.2.2	Generierung des Schlüsselpaars . . . . .	3
2.3	Sicherheit . . . . .	4
2.4	Vergleich zur symmetrischen Verschlüsselung . . . . .	5
<b>3</b>	<b>Anonymität des Tor-Netzwerkes</b>	<b>5</b>
3.1	Onion Services . . . . .	6
3.1.1	Verbindungsaufbau . . . . .	7
3.2	Vor- und Nachteile . . . . .	8
<b>4</b>	<b>Dezentralisierung</b>	<b>9</b>
4.1	Sicherheit . . . . .	9
<b>5</b>	<b>Vor- und Nachteile</b>	<b>9</b>
5.1	Kriminalität . . . . .	9
5.2	freie Meinungsäußerung . . . . .	9
<b>6</b>	<b>Umsetzung des Messengers</b>	<b>9</b>
<b>7</b>	<b>Fazit</b>	<b>9</b>

## 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 [vgl. ebd.].

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; Bh23].

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, sowie der Sicherheitsbetrachtung der asymmetrischen Verschlüsselung [vgl. LB21]. Die Arbeit geht dabei nicht auf weitere Padding-Verfahren ein. Eine mögliche Lösung, um eine Anonymität über das Internet zu gewährleisten wird in Kapitel drei vorgeschlagen, wobei das Tor-Netzwerk eine wichtige Rolle spielt. Diese Arbeit befasst sich im vierten Kapitel mit einer Dezentralisierung der Infrastruktur, um eine weitere Sicherheitsebene zu schaffen. Zuletzt werden im fünften Kapitel die Vor-

## über Tor – Die Lösung für sicheres Messaging?

und Nachteile eines solchen Messengers betrachtet, im sechsten Kapitel wird eine mögliche Umsetzung des Messengers beschrieben und im siebten Kapitel wird ein

35 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]. Dazwischenliegen-

40 de Akteure, wie zum Beispiel Server oder mögliche Angreifer, können demzufolge die Nachricht nicht lesen [vgl. ebd.]. **Nur** der Empfänger der Nachricht kann diese auch entschlüsseln. Als Ent- und Verschlüsselungsverfahren der Nachrichten wird die asymmetrische Verschlüsselung verwendet [vgl. ebd.]. Diese Arbeit beschränkt sich bei der asymmetrischen Verschlüsselung auf das RSA-Verfahren.

### 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 aber nicht entschlüsseln kann [vgl. ebd.]. **Nur** der zum Schlüsselpaar dazugehörige private Schlüssel ist in der Lage, die verschlüsselte Nachricht wieder zu entschlüsseln (siehe Abb. 1) [vgl. ebd.].

50

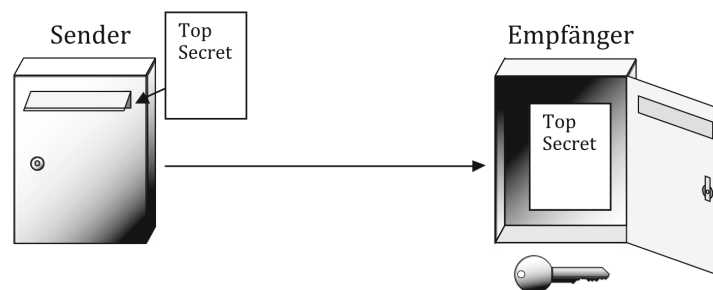


Abbildung 1: Jeder Sender kann mit dem öffentlichen Schlüssel die Nachricht „verschlüsseln“ (also eine Nachricht in den Briefkasten werfen), aber nur der Empfänger kann den Briefkasten mit seinem privaten Schlüssel öffnen und somit die Nachricht herausnehmen [vgl. BSW15a]

## 2.2 Mathematische Betrachtung

Alle Variablen der folgenden Berechnungen liegen im Bereich  $\mathbb{N}$  [vgl. Is16].

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

### 60 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 (bei wie vielen Zahlen der größte gemeinsame Teiler (gcd) 1 ist) [vgl. Ta13].

Somit ergibt  $\phi(6) = 2$  oder bei einer Primzahl  $\phi(7) = 7 - 1 = 6$  somit  $\phi(x) = x - 1$ ,

65 wenn  $x$  eine Primzahl ist, da jede Zahl kleiner als  $x$  teilerfremd sein muss [vgl. Tu08].

$$\phi(n) = \phi(P \cdot Q)$$

$$\phi(n) = \phi(P) \cdot \phi(Q)$$

$$\phi(P) = P - 1 \qquad \phi(Q) = Q - 1$$

$$\phi(n) = (P - 1) \cdot (Q - 1)$$

### 2.2.2 Generierung des Schlüsselpaares

Sowohl der private als auch der öffentliche Schlüssel besteht unter anderem aus folgender Komponente:  $n = P \cdot Q$  [vgl. Ta96]. Für den öffentlichen Schlüssel benötigen wir die Komponente  $e$ , die zur Verschlüsselung einer Nachricht verwendet

70 wird [vgl. ebd.].  $e$  ist hierbei eine zufällige Zahl, bei welcher folgende Bedingungen gelten [vgl. ebd.]:

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

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  $d$ , wel-

75 che zur Entschlüsselung verwendet wird [vgl. MS13].

$$\phi(n) = (P - 1)(Q - 1)$$

$$e \cdot d = 1 \mod \phi(n)$$

## 2.3 Sicherheit

Um die Sicherheit des RSA-Verfahrens betrachten zu können, müssen wir nun den Ver/-Entschlüsselungsvorgang betrachten.

$$c = m^e \mod n \quad \text{Verschlüsselung zu } c \text{ mit } m \text{ als Nachricht}$$

$$m = c^d \mod n \quad \text{Umkehroperation (Entschlüsselung) von } c \text{ zu } m$$

Um die verschlüsselte Nachricht  $c$  zu entschlüsseln, bräuchte ein Angreifer die Komponente des privaten Schlüssels  $d$ .  $d$  ist allerdings mit einem starken Rechenaufwand verbunden, da, wie schon vorher bereits gezeigt, dafür  $\phi(n)$  kalkuliert werden müsste. Somit wird eine Primfaktorzerlegung von  $n$  benötigt wird [vgl. Ta13]. Bei der Verschlüsselung von  $m$  zu  $c$  liegt eine Trapdoor-Einwegfunktion vor [vgl. Kr16a]. Das bedeutet, dass es zwar leicht ist  $f(x) = i$  zu berechnen (bei RSA: Verschlüsselung), es jedoch unmöglich ist von  $i$  auf den Ursprungswert  $x$  zu schließen, ohne dass weitere dafür notwendigen Komponente bekannt sind (bei RSA wäre die benötigte Komponente  $d$ ) [vgl. ebd.].

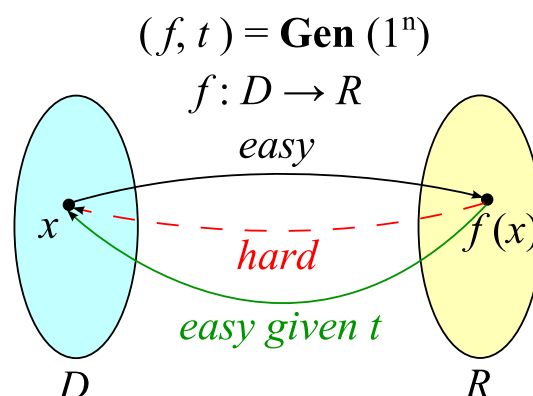


Abbildung 2: Die Trapdoor-Einwegfunktion bildlich dargestellt[vgl. Kr16b]

Wichtig bei dem RSA-Verfahren ist, dass die Länge von  $n$  (die Schlüssellänge) mindestens 3000 Bit betragen sollte, da sonst die Primfaktorzerlegung von  $n$  mit modernen Computern möglich sein könnte [vgl. Si23].

## 2.4 Vergleich zur symmetrischen Verschlüsselung

Bei der symmetrischen Verschlüsselung wird der gleiche Schlüssel sowohl für die Verschlüsselung als auch für die Entschlüsselung verwendet [vgl. IBM21]. Im Vergleich zu der asymmetrischen Verschlüsselung, ist die symmetrische Verschlüsselung schneller und keine Beschränkung des Chiffretextes [vgl. HK20; Op24]. Jedoch muss der Schlüssel der symmetrischen Verschlüsselung sicher an den jeweils anderen Kommunikationspartner übermittelt werden, um Nachrichten zu entschlüsseln [vgl. ebd.].

## 3 Anonymität des Tor-Netzwerkes

Der zweite zentrale Aspekt dieser Arbeit ist die Anonymität über das Internet. Bei normalen Routing, wie wir es tagtäglich nutzen, kommuniziert der Client direkt mit dem Zielservers. Der Zielservers kann hierbei die IP-Adresse des Clients sehen, somit ist eine Rückverfolgung möglich [vgl. Fä23; El16]. Und genau bei diesem Problem setzt das Tor-Netzwerk an. Das Tor-Netzwerk besteht hierbei aus vielen *Nodes*, welche eingehende Tor-Verbindungen akzeptieren und weiterverarbeiten. Damit ein Client überhaupt eine Anfrage über das Netzwerk verschicken kann, sucht er sich zunächst einen Pfad durch das Netzwerk, genannt *Circuit* [vgl. To24d]. Dieser *Circuit* besteht dabei meist aus drei *Nodes* und ist für 10 Minuten gültig, bis der Client das *Circuit* erneuert (also einen neuen Pfad „sucht“) [vgl. To24c]. Der *Entry Node*, einer *Relay Node* und einer *Exit Node*, worüber später Anfragen an die Zielservers geschickt werden können [vgl. ebd.]. Dabei verschlüsselt der Client verschlüsselt die eigentliche Anfrage mehrmals, hüllt sie also in ein mehrere „Schalen“ ein, welche eine *Onion* bilden, und leitet diese über den *Circuit* an den Zielservers weiter [vgl. DMS04]. Anfangs wird die *Onion* von dem Tor-Client an die *Entry Node* geschickt [vgl. ebd.]. Bei jeder *Node*, also auch der *Entry Node*, wird eine Schale der *Onion* „geschält“ (die Nachricht also einmal entschlüsselt), welche Informationen zu dem nächsten Knotenpunkt enthält, somit schickt jene Node, die Anfrage an den nächsten Knotenpunkt weiter [vgl. Au18]. Sobald die Anfrage bei der *Exit Node* angekommen ist, entfernt diese die letzte „Schale“ der Anfrage, welche nun vollständig entschlüsselt ist (wenn die eigentliche Anfrage nicht mit HTTPS verschlüsselt wurde), und schickt diese an den Zielservers [vgl. ebd.]. Nur die *Ent-*

## über Tor – Die Lösung für sicheres Messaging?

125 *ry Node* weiß somit die reale IP-Adresse des Clients und **nur** die letzte Node (*Exit Node*) weiß, an welchen Zielserver die Anfrage geschickt wurde [vgl. ebd.]. Wichtig hierbei ist allerdings, dass die *Entry Node* nicht weiß, was der Zielserver der Anfrage ist [vgl. ebd.]. Die *Exit Node* weiß im Gegenzug die reale IP-Adresse des Clients nicht. Allerdings könnte die *Exit Node* die IP-Adressen der Zielserver sehen oder möglicherweise Informationen der Nutzer auslesen (wenn die Anfrage nicht mit HTTPS verschlüsselt wurde) [vgl. Ch+11]. Hier herrscht also eine Schwachstelle des Tor-Netzwerkes.

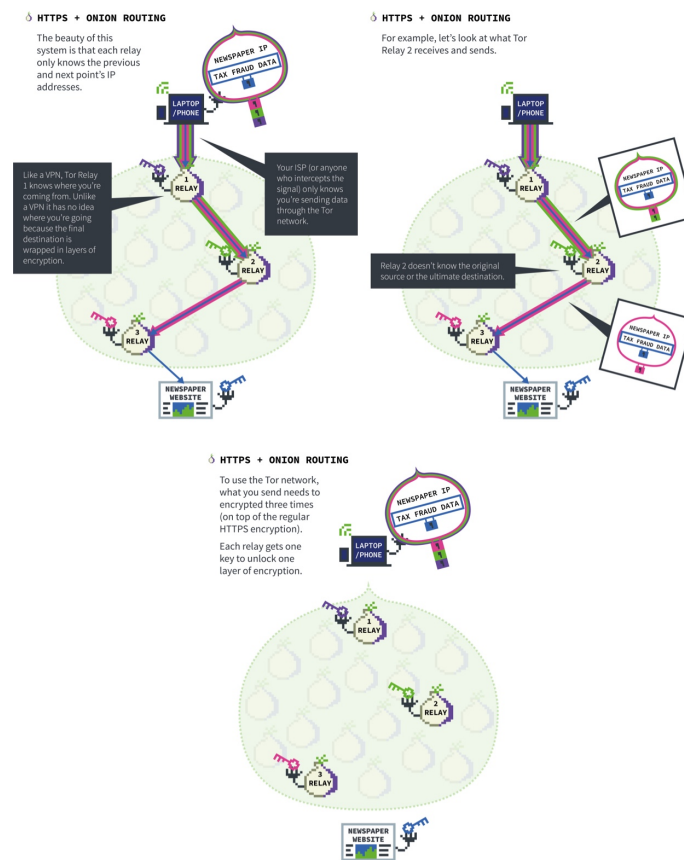


Abbildung 3: Tor Entschlüsselungslayer [vgl. To22]

130 

### 3.1 Onion Services

Onion Services lösen dieses Problem, da diese nicht auf die *Exit Node* angewiesen sind und nur innerhalb des Tor-Netzwerkes mit anderen Tor-Clients kommunizieren [vgl. To24g]. Sie nicht über das normale Internet erreichbar, wie die Zielserver im vorherigen Beispiel, sondern nur über das Tor-Netzwerk [vgl. To24f]. Bei dem Onion Service müssen im Kontrast zu normalen öffentlichen Servern keine Ports geöffnet

135



## über Tor – Die Lösung für sicheres Messaging?

werden, damit ein Client sich mit dem Server verbinden kann, da der Onion Service direkt mit dem Tor-Netzwerk über ausgehende Verbindungen kommuniziert (auch bekannt als *NAT punching*) und darüber sämtliche Daten geleitet werden [vgl. ebd.]. Für Außenstehende sieht der Onion Service also aus, wie als wäre er ein normaler Tor-Client [vgl. ebd.].

### 3.1.1 Verbindungsaufbau

Zunächst generiert der Onion Service ein Schlüsselpaar, bestehend aus einem öffentlichen und einem privaten Schlüssel [vgl. Ge23]. Unter anderem wird nun aus dem öffentlichen Schlüssel die Adresse des Onion Services generiert und endet mit „onion“ [vgl. ebd.]. Ein Beispiel für eine solche Adresse ist die der Suchmaschine DuckDuckGo:

*duckduckgogg42xjoc72x3sjasowoarfbgcmvfimaftt6twagswzczad.onion* [vgl. Du24].

Der Onion Service sich nun mit dem Tor-Netzwerk wie ein normaler Client über einen *Circuit*, welcher aus drei *Nodes* besteht [vgl. To24f]. Der Service sendet eine

Anfrage an das letzte Relay im *Circuit*, sodass es als *Introduction Point* dient und etabliert eine Langzeitverbindung jenem (der *Circuit* erneuert sich also nicht alle 10 Minuten wie bei dem Tor-Client) [vgl. ebd.]. Dieser Vorgang wiederholt sich zwei Mal, bis der Onion Service drei *Introduction Points* auf drei verschiedenen *Circuits* gefunden hat [vgl. ebd.]. Damit andere Clients den Onion Service erreichen können,

erstellt der Onion Service einen *Onion Service descriptor*, welcher die Adressen der *Introduction Points* und Authentifizierungsschlüssel enthält, signiert diesen mit seinem privaten Schlüssel und schickt den *descriptor* an die Directory Authority [vgl. To24a; To24e]. Die Directory Authority ist ein Server, welcher Informationen über das Tor-Netzwerk, wie zum Beispiel die des Onion Services, speichert und verteilt

[vgl. To24b]. Im Sinne dieser Arbeit, hat der Onion Service sich nun von Person A mit dem Tor-Netzwerk verbunden, jedoch braucht es noch Person B, welche sich über ihren Tor-Client mit dem Onion Service der Person B verbindet. Damit der Tor-Client von Person A sich allerdings verbinden kann, fragt der Client nun die Directory Authority an den signierten *descriptor* des Onion Services von Person B an den Client zu schicken [vgl. K 23]. Der Client besitzt nun die Adressen der *Introduction Points* und die Signatur des *descriptors*, sodass dieser mit dem öffentlichen Schlüssels der Onion Adresse die Signatur überprüfen kann [vgl. ebd.]. Der Client

## über Tor – Die Lösung für sicheres Messaging?

generiert nun 20 zufällige Bytes (Secret) und schickt diese an eine zufällig ausgewählte *Relay Node*, welche nun als *Rendezvous Point* dient [vgl. To23b]. Das Secret  
170 wird von dem Client auch an eine von den *Introduction Points* geschickt, sodass der Onion Service mit dem gleichen Secret eine Verbindung zu dem *Rendezvous Point* aufbauen kann [vgl. To23a]. Der *Rendezvous Point* leitet, wenn der Client und der Onion Service über deren *Circuits* miteinander verbunden sind, die Nachrichten zwischen den beiden weiter [vgl. To23b]. Der Client und der Onion Service kommunizieren nun also nur über das Tor-Netzwerk miteinander und sind nicht mehr auf  
175 die *Exit Node* angewiesen.

### 3.2 Vor- und Nachteile

Vorteile des Tor-Netzwerkes (bezogen auf Onion Services) sind zum Beispiel, wie bereits genannt, die Anonymität. Das Routing über das Tor-Netzwerk ist im Vergleich  
180 zum normalen Routing um das 120-fache langsamer [vgl. LSS10]. Ein möglicher Angriff gegen die Anonymität des Onion Services ist die des „SignalCookies“, welcher auf einen Fehler im Protokoll des Tor-Netzwerkes zurückzuführen ist [vgl. Ch+19]. Hierbei wird ein zufälliger Cookie, bestehend aus 20 Bytes generiert und zwischengespeichert [vgl. ebd.]. Der Client sendet nun eine Anfrage in das Tor-Netzwerk,  
185 dass der Client mit dem Onion Service eine Verbindung aufbauen will und hängt den Cookie an die Anfrage an. Der Onion Service baut nun, wie bereits beschrieben eine Verbindung über einen *Circuit* auf und einigt sich auf einen *Rendezvous Point* mit dem Client, jedoch schickt er während der Anfrage an den *Rendezvous Point* aufgrund eines Protokollfehlers des Tor-Netzwerkes den vorher gegebenen  
190 Cookie des Clients mit [vgl. ebd.]. Wenn der *Rendezvous Point* nun von einem Angreifer kontrolliert wird, kann dieser den Cookie des Clients mit dem Cookie des Onion Services vergleichen und somit den Onion Service identifizieren, wodurch sich von hieraus vorgearbeitet werden kann, sodass die *Entry Node* des Onion Services identifiziert wird und kompromittiert werden kann [vgl. ebd.].

195

## **4 Dezentralisierung**

### **4.1 Sicherheit**

## **5 Vor- und Nachteile**

### **5.1 Kriminalität**

### **5.2 Freie Meinungsäußerung**

200

## **6 Umsetzung des Messengers**

## **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.
- [DMS04] Roger Dingledine, Nick Mathewson und Paul Syverson. „Tor: The Second-Generation Onion Router“. In: *13th USENIX Security Symposium (USENIX Security 04)*. San Diego, CA: USENIX Association, Aug. 2004. URL: <https://www.usenix.org/conference/13th-usenix-security-symposium/tor-second-generation-onion-router>.
- [Tu08] Clay S Turner. „Euler’s totient function and public key cryptography“. In: *Nov 7 (2008)*, S. 138.
- [LSS10] Tomáš Liška, Tomáš Sochor und Hana Sochorová. „Comparison between normal and TOR-Anonymized Web Client Traffic“. In: *Procedia - Social and Behavioral Sciences 9 (2010)*. World Conference on Learning, Teaching and Administration Papers, S. 542–546. ISSN: 1877-0428. DOI: <https://doi.org/10.1016/j.sbspro.2010.12.194>. URL: <https://www.sciencedirect.com/science/article/pii/S1877042810022998>.
- [Ch+11] Sambuddho Chakravarty, Georgios Portokalidis, Michalis Polychronakis und Angelos D. Keromytis. „Detecting Traffic Snooping in Tor Using Decoys“. In: *Recent Advances in Intrusion Detection*. Hrsg. von Robin Sommer, Davide Balzarotti und Gregor Maier. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, S. 222–241. ISBN: 978-3-642-23644-0.
- [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>.

## über Tor – Die Lösung für sicheres Messaging?

- [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](https://doi.org/10.1007/978-3-8348-2322-9_1).
- [El16] Elektronik Kompendium. *TCP/IP*. Nov. 2016. URL: <https://www.elektronik-kompendium.de/sites/net/0606251.htm> (besucht am 23. 01. 2024).
- [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.
- [Kr16a] 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.
- [Au18] Autumn. „How does Tor \*really\* work?“. In: (Feb. 2018). URL: <https://hackernoon.com/how-does-tor-really-work-c3242844e11f> (besucht am 23. 01. 2024).
- [Ch+19] Muqian Chen, Xuebin Wang, Tingwen Liu, Jinqiao Shi, Zelin Yin und Binxing Fang. „SignalCookie: Discovering Guard Relays of Hidden Services in Parallel“. In: *2019 IEEE Symposium on Computers and Communications (ISCC)*. 2019, S. 1–7. DOI: 10.1109/ISCC47284.2019.8969639.

## über Tor – Die Lösung für sicheres Messaging?

- [HK20] Aljaafari Hamza und Basant Kumar. „A Review Paper on DES, AES, RSA Encryption Standards“. In: *2020 9th International Conference System Modeling and Advancement in Research Trends (SMART)*. 2020, S. 333–338. DOI: 10.1109/SMART50582.2020.9336800.
- [IBM21] *IBM Documentation*. März 2021. URL: <https://www.ibm.com/docs/en/ztpf/2020?topic=concepts-symmetric-cryptography> (besucht am 23. 01. 2024).
- [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](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).
- [Bh23] Jasdeep Bhatia. *Understanding System Design Whatsapp & Architecture*. Mai 2023. URL: [https://pwskills.com/blog/system-design-whatsapp/#Client-Server\\_Architecture](https://pwskills.com/blog/system-design-whatsapp/#Client-Server_Architecture) (besucht am 22. 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.

## über Tor – Die Lösung für sicheres Messaging?

- [Ge23] GeeksforGeeks. *What are onion services in Tor Browser*. Okt. 2023. URL: <https://www.geeksforgeeks.org/what-are-onion-services-in-tor-browser> (besucht am 04. 02. 2024).
- [K 23] Arun K. L. „Detailed Anatomy of the Tor Network | Structure of the Tor Network“. In: *Sec Master* (Okt. 2023). URL: <https://thesecmaster.com/detailed-anatomy-of-the-tor-network-structure-of-the-tor-network> (besucht am 23. 01. 2024).
- [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](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).
- [To23a] Tor Project. *The introduction protocol [INTRO-PROTOCOL] - Tor Specifications*. Dez. 2023. URL: <https://spec.torproject.org/rend-spec/introduction-protocol.html> (besucht am 04. 02. 2024).
- [To23b] Tor Project. *The rendezvous protocol - Tor Specifications*. Nov. 2023. URL: <https://spec.torproject.org/rend-spec/rendezvous-protocol.html> (besucht am 04. 02. 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).
- [Du24] DuckDuckGo. *duckduckgo onion at DuckDuckGo*. Feb. 2024. URL: <https://duckduckgo.com/?q=duckduckgo+onion&atb=v160-7&ia=web> (besucht am 02. 02. 2024).

## über Tor – Die Lösung für sicheres Messaging?

- [Op24]      Openssl Foundation, Inc. */docs/man3.1/man3/RSA\_public\_encrypt.html*. Jan. 2024. URL: [https://www.openssl.org/docs/man3.1/man3/RSA\\_public\\_encrypt.html](https://www.openssl.org/docs/man3.1/man3/RSA_public_encrypt.html) (besucht am 04. 02. 2024).
- [To24a]     Tor Project. *Deriving blinded keys and subcredentials [SUBCRED] - Tor Specifications*. Jan. 2024. URL: <https://spec.torproject.org/rend-spec/deriving-keys.html> (besucht am 04. 02. 2024).
- [To24b]     Tor Project. *directory authority | Tor Project | Support*. Feb. 2024. URL: <https://support.torproject.org/glossary/directory-authority> (besucht am 02. 02. 2024).
- [To24c]     Tor Project. *How can we help? | Tor Project | Support*. Feb. 2024. URL: <https://support.torproject.org/#ChangePaths> (besucht am 04. 02. 2024).
- [To24d]     Tor Project. *Kanal | Tor Project | Hilfe*. Jan. 2024. URL: <https://support.torproject.org/de/glossary/circuit> (besucht am 31. 01. 2024).
- [To24e]     Tor Project. *src/core/or · main · The Tor Project / Core / Tor · GitLab*. Feb. 2024. URL: [https://gitlab.torproject.org/tpo/core/tor/-/blob/main/src/feature/hs/hs\\_descriptor.c?ref\\_type=heads](https://gitlab.torproject.org/tpo/core/tor/-/blob/main/src/feature/hs/hs_descriptor.c?ref_type=heads) (besucht am 04. 02. 2024).
- [To24f]     Tor Project. *Tor Project | How do Onion Services work?* [Online; accessed 2. Feb. 2024]. Jan. 2024. URL: <https://community.torproject.org/onion-services/overview>.
- [To24g]     Tor Project. *Tor Project | Talk about onions*. Jan. 2024. URL: <https://community.torproject.org/onion-services/talk> (besucht am 31. 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](https://doi.org/10.1007/978-3-8348-2322-9_2).
- [Kr16b] 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.
- [To22] Tor Project. *Tor Project | All About Tor*. Aug. 2022. URL: <https://community.torproject.org/training/resources/all-about-tor/#/0/7> (besucht am 23.01.2024).

Quellcode: <https://github.com/sshcrack/enkrypton>