

Inhalt

Vorwort: Zur weltweiten Krise der Privatsphäre - Der Aufbruch von Verschlüsselung und ihr Weg in die Dritte Epoche der Kryptographie • 11

1 Angstfrei, vertraulich und abhörsicher – Braucht Demokratie das Recht auf Verschlüsselung? • 25

- 1.1 Der erste Akt: Hauptrolle der europäischen Parlamentarierinnen und Parlamentarier * 28
- 1.2 Der zweite Akt: Big Five & Five Eyes - Hauptrollen von mehr als fünf (Geheim-)Agenten * 31
- 1.3 Der dritte Akt: Hauptrolle der Novellen * 60
- 1.4 Der vierte Akt: Niemand hat die Absicht, zu überwachen: Zur Krise der Privatheit im 21. Jahrhundert * 75
- 1.5 Der fünfte Akt: Apples Sündenfall - Realität schaffen mittels technologischer Macht als fünfte Staatsgewalt nach Legislative, Judikative, Executive und den Medien * 96

2 26 Shades of Grey - Die Fahndung nach verborgener Multi-Verschlüsselung in der Steganographie • 103

- 2.1 Wir spielen Halma: mit der Null-Cipher * 107
- 2.2 Dank Schablonen-Filter: Ich sehe was, was Du nicht siehst! * 109
- 2.3 Die Bacon's Cipher: Wandlung statt Illusion * 114
- 2.4 Verstecken und Vermischen durch Transformation: Die XOR-Funktion * 118
- 2.5 Abstreitbarer Cipher-Text: Eine neue Forschungsrichtung oder nur eine gesalzene Botschaft? * 121

3 Mit Lernkurven: Zurück in die Zukunft eines neuen WhatsApp? • 126

- 3.1 Der sechste Akt: Hauptrolle der Lehrenden * 126
- 3.2 Der siebte Akt: Hauptrolle Europol und die Polizistinnen und Polizisten * 129
- 3.3 Der achte Akt: Hauptrolle Otto Normal – Vertrauen ist gut, Verschlüsselung ist besser * 132
- 3.4 Der neunte Akt: Hauptrolle WhatsApp, ein verstorbener Kanarienvogel und Captain L. * 138

- 3.5 Der zehnte Akt: Die Entdeckung von innovativen Alternativen * 150
- 3.6 Demokratisierung von quell-offener Verschlüsselung: Ein großartiges Schauspiel nur der Mathematik? * 152
- 3.7 Mein Auftakt: Wie gehe ich als Lernender persönlich an das Thema Verschlüsselung heran? * 162

4 Historische Anfänge und Grundlagen der Kryptographie • 168

- 4.1 Von Caesar über Enigma zum AES: Die symmetrische Verschlüsselung * 173
 - 4.1.1 Ein Sonderfall: Das One-Time-Pad (OTP) * 184
 - 4.1.2 Dreidimensionales Mischen als Gedanken-Modell bei der Cube Encryption * 188
- 4.2 Asymmetrische Verschlüsselung * 197
 - 4.2.1 GPG (GNU Privacy Guard) * 202
 - 4.2.2 S/MIME * 208
- 4.3 Hash-Funktionen, Zertifikate und Signaturen: SHA, Argon2 & Co. * 209

5 Die Dritte Epoche der Kryptographie: Ein Zeitalter für Multi-Verschlüsselung, exponentielle Verschlüsselung & quantum-sichere Verschlüsselung? • 213

- 5.1 Aufbruch und Abschied: No Longer Secure * 214
- 5.2 Quanten-Computer und ihr überlegener Durchbruch in eine neue Epoche * 227
- 5.3 Multi-Verschlüsselung: Ein Cocktail an der Bar? * 237
- 5.4 Exponentielle Verschlüsselung mit dem Echo-Protokoll im Netz der Graphen * 244
- 5.5 McEliece & NTRU: Ein neuer Lebenszyklus mit sicheren Algorithmen?! * 254

6 Transformation der Kryptographie: Das Schlüssel-Transport-Problem wird gelöst • 259

- 6.1 Schlüsselaustausche über DHM, REPLEO, EPKS oder AutoCrypt? * 260
- 6.2 Cryptographisches Calling: von Forward Secrecy zu Instant Perfect Forward Secrecy (IPFS) * 269
- 6.3 Derivative Kryptographie: Secret Streams Schlüssel aus dem Socialist Millionaire Protokoll (SMP) ableiten * 274
- 6.4 Derivative Kryptographie: Juggernaut Schlüssel * 279

- 6.5 Kenntnissfreiheit in der Ali Baba Höhle * 282
- 6.6 Automatisierte Interaktionsfreiheit und andere Ausblicke auf Zero-Knowledge-Beweise für weitere Programmierungen in der Kryptographie * 286
- 7 Digitale und Kryptographische Souveränität: National, personal und unternehmerisch • 306**
- 8 Apps, Programme und Werkzeuge – mit denen Lernende lernen, Verschlüsselungs-Meisterin und -Meister Nr. 1 zu werden • 321**
 - 8.1 Festplatten-Verschlüsselung mit Veracrypt * 321
 - 8.2 Smoke Crypto Chat: Mobiler McEliece-Messenger * 325
 - 8.3 Spot-On – Bekannte Suite für Verschlüsselung * 334
 - 8.4 Rosetta-Crypto-Pad – Mit Konversionen zur Konversation * 338
 - 8.5 GoldBug Messenger – Zeig’ mir Deine GUI * 341
 - 8.6 Delta-Chat: POPTASTIC populär * 345
 - 8.7 Silence - Eine SMS-App mit Ende-zu-Ende-Verschlüsselung * 348
 - 8.8 Conversations: Der alte Dino in der Mauser? * 349
 - 8.9 Hacker’s Keyboard: Abgriffe im Klar-Text verhindern * 352
 - 8.10 Federation ohne Accounts: Echo Chat Server & XMPP Server & Matrix Server & Co * 353
 - 8.11 Netcat & Socat: Terminal-Befehle als Telekommunikationsanlage? * 364
 - 8.12 RetroShare: Was war noch mal Turtle Hopping? * 366
 - 8.13 Vier Postfächer ohne Menschennummer-Identifikation bei Freundinnen und Freunden erhalten: Institution, Care-Of, Ozone und BitMessage * 369
 - 8.14 Im unsichtbaren DHT-Netzwerk mit Briar * 385
 - 8.15 Verschlüsseltes File-Sharing: Freenet & Offsystem * 388
 - 8.16 OnionShare – Transfer ohne Chat * 397
 - 8.17 Websuche und P2P-URL-Sharing mit YaCy & Spot-On * 399
 - 8.18 Webbrowser mit Dooble, Iron und einem Cookie-Washer * 406
 - 8.19 Tor Browser: Die IP-Adresse verschleiern * 409
 - 8.20 Ein Netzwerk mit Perspektive zum Surfen: Hallo Echo... * 411
 - 8.21 I2P Network: Unsichtbar im Mix-Netz * 412
 - 8.22 Kannste UNIX, kannste GNUnet * 413
 - 8.23 OpenVPN – ein etablierter Tunnel zum Peer? * 414
 - 8.24 Checkpoint CryptPad * 416

- 8.25 OpenStego – Ich sehe nichts, was Du wohl siehst * 417
- 8.26 Tails – Amnesie am Kiosk * 418
- 8.27 Mumble Audio sowie Jitsi, Nextcloud und BigBlueButton Video Chat * 419
- 8.28 Telegram, Threema und Wire * 420
- 8.29 Mastodon's dezentrales Chat-Servernetz * 422
- 8.30 Staatsfeinde Nr. 1: Bargeld und Mikrofon-freie Räume verhindern gläserne Menschen * 423
- 8.31 Cryptographische Cafeteria * 426

9 Interoperabilität, Kongruenz und Interkonnektivität von Schottischen Eiern • 428

- 9.1 Interoperabilität: nicht nur technisch ein hoffnungsloses Unterfangen? * 428
- 9.2 Big-7-Studie: Quell-offene Messenger im Vergleich * 433
- 9.3 Messenger Scorecards: Zur Vollständigkeit kryptographischer Kriterien * 440
- 9.4 Mögliche Empfehlungen zur Standardisierung und Interoperabilität von Messengern * 447
- 9.5 Technischer Ausblick: Dem Schottischen Ei sein Mantel - Staatliche Server als Overlay-Netz? * 453

10 Gesellschaftlicher Ausblick: Mit einer No-Plaintext-Strategie in das Dilemma einer verschlüsselten Gesellschaft? • 460

Abbildungsverzeichnis • 480

Glossar • 482

Didaktische Fragestellungen • 494

Bibliographische Verweise • 497

Abkürzungsverzeichnis • 518

Register • 522

Referenzen • 527