

# Inhaltsverzeichnis

<b>Inhaltsverzeichnis</b>	<b>3</b>
<b>I. Über dieses Skriptum</b>	<b>7</b>
I.1. Wer	7
I.2. Wo	7
<b>II. Einleitung</b>	<b>9</b>
II.1. Was ist Sicherheit?	9
II.2. Wichtigste Sicherheitsziele	10
II.3. Praxisprobleme	10
<b>III. Symmetrische Verschlüsselung</b>	<b>11</b>
III.1. Stromchiffren	11
III.1.1. Anforderungen	11
III.2. Blockchiffren	11
III.2.1. Definition	11
III.2.2. Anforderungen	11
III.2.3. Beispiel: DES (Data Encryption Standard)	12
III.2.4. Beispiel: Rijndael/AES (Advanced Encryption Standard)	12
III.2.5. Betriebsmodi	13
<b>IV. Hashfunktionen</b>	<b>15</b>
IV.1. Anwendungen	15
IV.2. Eigenschaften	15
IV.3. Merkle-Damgård-Konstruktion	15
IV.4. Das Random Oracle Model	15
IV.5. Der Angriff von Wang	16
IV.6. Symmetrische Authentifikation (MAC - Message Authentication Code)	16
<b>V. Schlüsselaustausch</b>	<b>17</b>
V.1. 3-Pass	17
V.2. Wide-Mouth-Frog	17
V.3. Kerberos	17
V.4. Merkle Puzzle	18
V.5. Diffie-Hellman-Schlüsselaustausch (DH)	18
V.5.1. Decisional-Diffie-Hellman-Annahme	18
V.5.2. Man-in-the-Middle-Angriff	18
<b>VI. Public-Key-Kryptographie</b>	<b>19</b>
VI.1. Definition	19
VI.2. Sicherheitsbegriff: IND-CCA2-Sicherheit	19
VI.3. Beispiel: Elgamal	19

VI.4. Beispiel: RSA . . . . .	19
VI.4.1. Die RSA-Funktion . . . . .	19
VI.4.2. Textbook-RSA . . . . .	20
VI.4.3. RSA-ES-OAEP . . . . .	20
<b>VII Digitale Signaturen</b>	<b>21</b>
VII.1 Begriffe . . . . .	21
VII.2 Beispiel: Signieren mit RSA (anschaulich) . . . . .	21
VII.3 Definition Signatur . . . . .	21
VII.4 Sicherheitsbegriff: EUF-CMA . . . . .	21
VII.5 Beispiel: Elgamal-Signaturen . . . . .	21
VII.5.1 Probleme . . . . .	22
VII.6 Beispiel: DSA (Digital Signature Algorithm) . . . . .	22
VII.7 Beispiel: One-Time-Signaturen (aus Hashfunktionen) . . . . .	22
VII.8 Ist EUF-CMA genug? . . . . .	23
VII.8.1 Key Substitution Attacks . . . . .	23
VII.8.2 Subliminal Channel . . . . .	23
<b>VIII Key Management</b>	<b>25</b>
VIII.1 PKI (Public-Key-Infrastruktur) . . . . .	25
VIII.1.1 „Definition“ . . . . .	25
VIII.2 Beispiel: X.509-Zertifikat . . . . .	25
VIII.3 Certificate Revocation . . . . .	25
VIII.4 Web of Trust . . . . .	26
VIII.5 TLS (Transport Layer Security) . . . . .	26
VIII.5.1 Ablauf . . . . .	26
VIII.5.2 Besonderheiten . . . . .	26
VIII.6 Key Renegotiation Attack . . . . .	26
VIII.6.1 Ziel . . . . .	26
VIII.6.2 Ablauf . . . . .	26
<b>IX. Netzwerksicherheit</b>	<b>27</b>
IX.1. CIA-Paradigma . . . . .	27
IX.2. Sicherheitsbegriff . . . . .	27
IX.3. Das ISO/OSI-Referenzmodell . . . . .	27
IX.4. IPsec . . . . .	27
IX.5. Bedrohungen für Rechner in Netzwerken . . . . .	28
IX.6. Schutzmaßnahmen . . . . .	28
IX.6.1. Firewalls . . . . .	28
IX.6.2. Monitoring . . . . .	28
IX.6.3. Honeypots . . . . .	28
IX.6.4. Datendiode . . . . .	28
<b>X. Zugriffskontrolle</b>	<b>29</b>
X.1. Bell-LaPadula-Modell . . . . .	29
X.1.1. Definition . . . . .	29
X.1.2. Basic Security Theorem . . . . .	30
X.1.3. Nachteile . . . . .	30
X.1.4. Vorteile . . . . .	30

X.2. Chinese-Wall-Modell . . . . .	30
X.2.1. Definition . . . . .	30
X.2.2. Eigenschaften . . . . .	31
<b>XI. Zero Knowledge</b>	<b>33</b>
XI.1. Eigenschaften: . . . . .	33
XI.2. Beispiel: Graph-Isomorphismus . . . . .	33
XI.2.1. Ablauf . . . . .	33
XI.2.2. Eigenschaften . . . . .	33
XI.3. Beispiel: Graph-3-Färbbarkeit . . . . .	33
XI.3.1. Ablauf . . . . .	34
XI.3.2. Eigenschaften . . . . .	34
<b>XII Authentifikation</b>	<b>35</b>
XII.1 Definition . . . . .	35
XII.2 Ansätze . . . . .	35
XII.3 Komponenten . . . . .	35
XII.4 Typische Anwendung: Kennworte . . . . .	35
XII.5 Maßnahmen gegen Offline-Attacken . . . . .	36
XII.5.1 Wahl guter Kennworte . . . . .	36
XII.6 Maßnahmen gegen Online-Attacken . . . . .	36
XII.7 Beispiel: CAPTCHAs . . . . .	36
XII.8 Raffiniertere Verfahren (Challenge-Response) . . . . .	36
XII.8.1 Schema . . . . .	36
XII.8.2 Beispiele . . . . .	36
<b>XIII Seitenkanalangriffe</b>	<b>39</b>
<b>XIV Implementierungsfehler</b>	<b>41</b>
XIV.1 in Programmen . . . . .	41
XIV.2 in Webanwendungen . . . . .	41
XIV.3 Lektion fürs Leben . . . . .	41
<b>XV Sicherheitsbewertung/Zertifizierung</b>	<b>43</b>
XV.1 Gründe für eine Zertifizierung . . . . .	43
XV.2 Common Criteria (ISO 15408) . . . . .	43
XV.2.1 Evaluation Insurance Levels . . . . .	43
<b>XVI Data Base Privacy</b>	<b>45</b>
XVI.1 k-Anonymität . . . . .	45
XVI.1.1 Kritik . . . . .	45
XVI.2 Differential Privacy . . . . .	45
<b>XVII Secure Function Evaluation</b>	<b>47</b>
XVII.1 Beispiel: Datingproblem . . . . .	47
XVII.1.1 Lösung: Secure AND . . . . .	47
XVII.2 allgemeine Secure Function Evaluation . . . . .	47
XVII.2.1 Baustein: „oblivious transfer“ (OT) . . . . .	47
XVII.2.2 Realisierung . . . . .	48
XVII.2.3 Realisierung mit Funktion $f$ . . . . .	48
XVII.2.4 Yao's Garbled Circuits . . . . .	48

