Inhaltsverzeichnis

Teil I Rahmenbedingungen für die Entwicklung

1 T-310-Chronologie 3
1.1 Historische Einordnung 3
1.2 T-310-Chronologie 5
1.3 SKS V/1 – Die Vorgeschichte 7
1.4 Quellen unseres kryptologisch-mathematischen Wissens 9
1.4.1 Öffentliche Kryptographie 9
1.4.2 Quellen unseres Wissens 10
1.4.3 Schulung durch sowjetische Kryptologen 11

2 Grundbegriffe und Entwicklungsanforderungen 15
2.1 Chiffrierverfahren 15
2.2 Absolute und quasiabsolute Sicherheit – das Kerckhoffs' Prinzip 17
2.3 Operative und technische Forderungen an die Chiffrierverfahren 18
2.4 Einheit von Entwicklung und Analyse 20
2.5 Anforderungen an die Entwicklung und die Analyse des Chiffrieralgorithmus T-310 22

Teil II Entwicklung und Analyse des Chiffrieralgorithmus

3 Grundstruktur des Chiffrieralgorithmus T-310 27
3.1 Blockschema des Chiffrieralgorithmus T-310 27
3.2 Komplizierungseinheit 29
3.3 Verschlüsselungseinheit 30
3.4 Langzeitschlüssel 30
3.5 Zeitschlüssel 32
3.6 Initialisierungsvektor 32

4 Chiffrieralgorithmus T-310 35
4.1 Definition des Chiffrieralgorithmus T-310 35
4.2 Definition 36

Bibliografische Informationen
http://d-nb.info/1210357917

digitalisiert durch DEUTSCHE NATIONAL BIBLIOTHEK

4.2.1 Bezeichnungen ... 36
4.2.2 Abbildung φ ... 37
4.2.3 U-Vektorfolge ... 39
4.2.4 Substitution ψ – Formeldarstellung ... 39
4.3 Schlüsselsystem ... 39
4.4 Festlegungen zur technischen Implementierung ... 40
4.4.1 Langzeitschlüssel (P, D, α) ... 40
4.4.2 Zeitschlüsselvorrat ... 41
4.4.3 U-Startvektor ... 41
4.4.4 Substitution ψ – Matrixdarstellung ... 41
4.5 Automatenmodell des Chiffrieralgorithmus T-310 ... 42
4.5.1 Automaten ... 42
4.5.2 Chiffrierautomat und Dechiffrierautomat ... 42
4.5.3 Automat zur Erzeugung der Steuerfolge ... 44

5 Langzeitschlüssel ... 45
5.1 Langzeitschlüsselauswahl ... 45
5.2 Langzeitschlüsselklasse KT1 ... 47
5.3 Langzeitschlüsselklasse KT2 ... 49

6 Integration der Substitution ψ ... 53
6.1 Substitutionsreihe und Geheimtext ... 53
6.2 Phasengleiche Texte und äquivalente Schlüssel ... 56
6.3 Verschärfte Voraussetzung für die Analyse ... 57

7 Abbildung φ ... 59
7.1 Z-Funktion, nichtlineare Komponente der Abbildung φ ... 60
7.1.1 Design der Z-Funktion ... 60
7.1.2 Analyse der Z-Funktion – Anfänge der Differentialkryptoanalyse ... 61
7.1.3 Statistische Struktur und die Anfänge der Linearen Kryptoanalyse ... 63
7.2 Einfluss der Schlüssel $S1$ und $S2$ ... 65
7.3 Bijektive Abbildungen ... 66
7.4 Stark zusammenhängende Graphen ... 69
7.4.1 Konstruktion einer reduzierten Menge ... 71
7.4.2 Die Verbindung der Zyklen durch Wege in den Graphen $\overrightarrow{G}(M, \varphi, \varphi^{-1})$ und $\overrightarrow{G}(M, \varphi)$ ... 74
7.4.3 Forderungen an die LZS-Klassen ... 76
7.5 Effektivitätsgebiete ... 76

8 Gruppe $G(P, D)$ ... 81
8.1 Erzeugendensysteme ... 82
8.2 Vergleich mit zufällig erzeugten Gruppen ... 83
8.3 Transitivität ... 85

8.4 Homomorphismen der Permutationsgruppen 85
8.4.1 Reduktionshomomorphismen 86
8.4.2 Homomorphismen der Imprimitivitätsgebiete 88
8.5 Berechnung der Zyklenstruktur mit Kontrollwertmengen 98
8.5.1 Teilweise Berechnung der Zyklen mittels einer Kontrollwertmenge 99
8.5.2 Anwendung auf Permutationen aus $G(P, D)$ 100
8.6 Prüfung auf Primitivität 102
8.6.1 Algorithmus zur Prüfung der Primitivität 105
8.6.2 Primitivitätsnachweis für $G(P, R)$ 107
8.7 Identifikation von $G(P, D)$ mit $\mathfrak{A}(M)$ oder $\mathfrak{S}(M)$ 109
8.8 Die Auswahl der LZS 110

9 Stochastische Modelle 113
9.1 Die f-Folge als zufällige Binärfolge 114
9.2 Statistische Tests 115
9.3 Tests auf Linearität 117
9.4 Markov-Ketten 119
9.5 Modell der Markov-Chiffren von Lai/Massey 120
9.6 Zufällige Abbildungen und Permutationen 122

10 Perioden und Schlüsseläquivalenzen 125
10.1 Automatenmodelle 126
10.2 Periodizitätseigenschaften 127
10.3 Periodizität und Überdeckung 134
10.4 Äquivalente Schlüssel 135
10.4.1 Automaten und Äquivalenzen 136
10.4.2 Schlüsseläquivalenzen 141
10.4.3 Abschätzung der Anzahl der Schlüsseläquivalenzklassen 146

11 Chiffrieralgorithmus T-310 aus heutiger Sicht 157
11.1 Einordnung als Feistelchiffre 157
11.2 Einschätzung der Sicherheit des CA T-310 160

Teil III Entwicklung und Analyse der Chiffrierverfahren

12 Chiffrierverfahren 165
12.1 Chiffrierverfahren ARGON und ADRIA 165
12.2 Chiffrierverfahren SAGA 167
12.3 Analyse der Chiffrierverfahren 167

13 Chiffriergeräte und Schlüsselmittel 169
13.1 Chiffriergeräte T-310/50 und T-310/51 169
13.2 Langzeitschlüssel 173

13.3 Zufallsgeneratoren ... 175
13.3.1 Systemzufallsgenerator ... 176
13.3.2 Physikalischer Zufallsgenerator ... 178
13.3.3 Stochastisches Modell der Zufallsgeneratoren ... 179
13.4 Schutz der Chiffrierung ... 181
13.4.1 Physische Sicherheit ... 182
13.4.2 Selbsttest und prophylaktische Prüfung ... 183
13.4.3 Kompromittierende Ausstrahlung ... 185
13.5 Schlüsselmittel ... 186

14 Sicherheit des Chiffrierverfahrens im Einsatz ... 189
14.1 Bedienanalyse ... 190
14.2 Verkehrsanalyse ... 192
14.3 Authentisierung ... 193
14.4 Voraussetzungen für die Dekryptierung ... 194
14.4.1 Angriffe auf den Zeitschlüssel ... 194
14.4.2 Kompromittierung einzelner Klartexte ... 195
14.4.3 Hypothetische Angriffe ... 196
14.5 Chiffriergeräte T-310 und die genutzten Chiffrierverfahren aus heutiger Sicht ... 197

Teil IV Ende und Neuanfang

15 Das Ende des ZCO und der T-310 ... 201
15.1 Endzeit im ZCO ... 202
15.2 Fahrten nach Bonn und Dahlwitz-Hoppegarten ... 205
15.3 Unser letzter Einsatz – Vernichtung der Geräte ... 209

16 Neuanfang bei der SIT ... 211
16.1 Umzug ... 212
16.2 Nutzung der ALPHA-Dokumente ... 212
16.3 Unser Abschied von der SIT ... 213

Anhang A Liste der Vortragsthemen sowjetischer Kryptologen ... 215

Anhang B Liste der VS-Unterlagen zu ALPHA ... 217

Anhang C Dienstreisen nach Bonn im Sommer 1990 ... 221

Anhang D LAMBDA1-Algorithmus ... 233

Anhang E Abkürzungen ... 239

Literatur ... 241

Stichwortverzeichnis ... 245