

Inhaltsverzeichnis

Teil I Rahmenbedingungen für die Entwicklung

1	T-310-Chronologie	3
1.1	Historische Einordnung	3
1.2	SKS V/1 – Die Vorgeschichte	6
1.3	T-310-Chronologie	7
1.4	Quellen unseres kryptologisch-mathematischen Wissens	10
1.4.1	Öffentliche Kryptographie	10
1.4.2	Quellen unseres Wissens – die Anfänge	11
1.4.3	Schulung durch sowjetische Kryptologen	12
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	Die Entwicklung und die Produktion der T-310 in der Industrie	20
2.5	Einheit von Entwicklung und Analyse	21
2.6	Anforderungen an die Sicherheitsanalyse	23

Teil II Entwicklung und Analyse des Chiffrieralgorithmus

3	Blockstruktur des Chiffrieralgorithmus T-310	29
3.1	Blockstruktur der Chiffrieralgorithmen der Klasse ALPHA	29
3.2	Komplizierungseinheit	31
3.3	Verschlüsselungseinheit	32
3.4	Langzeitschlüssel	32
3.5	Zeitschlüssel	34
3.6	Initialisierungsvektor	34
4	Chiffrieralgorithmus T-310	37
4.1	Definition des Chiffrieralgorithmus SKS	38
4.2	Definition des Chiffrieralgorithmus T-310	40

4.2.1	Bezeichnungen	40
4.2.2	Abbildung φ	41
4.2.3	U -Vektorfolge	42
4.2.4	Substitution ψ	43
4.3	Das T-310-Schlüsselsystem	44
4.4	T-310-Festlegungen zur technischen Implementierung	44
4.4.1	Langzeitschlüssel (P, D, α)	44
4.4.2	Zeitschlüsselvorrat	45
4.4.3	U -Startvektor	45
4.5	Automatenmodell des Chiffrieralgorithmus T-310	45
4.6	Chiffrieralgorithmenklasse ALPHA	48
5	Langzeitschlüssel	53
5.1	Langzeitschlüsselauswahl	53
5.2	Langzeitschlüsselklasse KT1	54
5.3	Langzeitschlüsselklasse KT2	57
5.4	Die Entscheidung für KT1	59
6	Eigenschaften der Substitution ψ	61
6.1	Substitutionsfolge und Geheimtext	61
6.2	Phasengleiche Texte und äquivalente Schlüssel	64
7	Elementare Eigenschaften der Abbildung φ	67
7.1	Z-Funktion, nichtlineare Komponente der Abbildung φ	68
7.1.1	Design der Z-Funktion	68
7.1.2	Analyse der Z-Funktion – Anfänge der Differentialkryptoanalyse	71
7.1.3	Statistische Struktur und Anfänge der Linearen Kryptoanalyse	74
7.2	Einfluss der Zeitschlüsselkomponenten $S1$ und $S2$	78
7.3	Berechnung der inversen Abbildung	81
7.4	Zyklenlängen	84
7.4.1	Rolle der Zyklusstruktur	84
7.4.2	Teilweise Berechnung der Zyklen mittels einer Kontrollwertmenge	85
7.4.3	Anwendung auf Permutationen	86
7.5	Stark zusammenhängende Graphen	88
7.5.1	Analytische Betrachtungen	88
7.5.2	Graph der Abbildung φ	92
7.5.3	Konstruktion einer reduzierten Menge	94
7.5.4	Die Verbindung der Zyklen durch Wege in den Graphen $\vec{G}(M, \varphi, \varphi^{-1})$ und $\vec{G}(M, \varphi)$	97
7.5.5	Forderungen an die LZS-Klassen	100

7.6	Ergänzende Ergebnisse zum Graphen $\vec{G}(M, \varphi)$	100
7.6.1	Abschätzung des Durchmessers des Graphen	101
7.6.2	Urnenmodell des Durchmessers.	106
7.6.3	Zusammenhang des Graphen und Invariante der Zustandsfunktion	108
8	Gruppe $G(P, D)$	111
8.1	Die Permutationsgruppe $G(P, D)$	112
8.1.1	Erzeugendensysteme	113
8.1.2	Transitivität	114
8.2	Homomorphismen der Permutationsgruppen	115
8.2.1	Effektivitätsgebiete.	116
8.2.2	Reduktionshomomorphismen	120
8.3	Untersuchung der Imprimitivitätssysteme	123
8.4	Prüfung auf Primitivität	131
8.4.1	Kriterium bei unvollständig bekannter Zyklusstruktur	132
8.4.2	Algorithmus zur Prüfung der Primitivität	135
8.4.3	Teilerfremde Zykluslängen und Primzahlen	137
8.4.4	Primitivitätsnachweis für $G(P, D)$	139
8.5	Die Gruppen $G(P, D)$ und die Alternierende Gruppe $\mathfrak{A}(M)$	142
8.6	Auswahl der LZS.	147
8.7	Ergänzende Ergebnisse zu den Gruppen	149
8.7.1	Vollständige Berechnung der Zykluslängen	149
8.7.2	Alternierende Gruppe.	149
8.7.3	Invariante der Abbildung φ über mehrere Schritte.	150
9	Stochastische Modelle	155
9.1	Die f -Folge als zufällige Binärfolge	156
9.2	Statistische Tests	157
9.3	Tests auf Linearität.	159
9.4	Markov-Ketten	161
9.5	Ergänzende Ergebnisse: Das Modell der Markov-Chiffren von Lai/Massey	162
9.6	Zufällige Abbildungen und Permutationen	165
10	Perioden	169
10.1	Automatenmodelle.	169
10.2	Elementare Periodizitätseigenschaften	171
10.3	Nachweis sehr langer Perioden	178
10.4	Ergänzende Ergebnisse zu Periodenlängen	184
10.5	Periodizität und Überdeckung	186
11	Äquivalente Schlüssel	189
11.1	Ergebnisse zu Schlüsseläquivalenzen aus den 80er Jahre	189
11.2	Automaten und Äquivalenzen	193

11.3	Ergänzende Ergebnisse zu Schlüsseläquivalenzen.	195
11.3.1	Automaten der Zwischenfolgen.	195
11.3.2	Schlüsseläquivalenzen verschiedener Ausgabefolgen	198
11.3.3	Abschätzung der Anzahl der Schlüsseläquivalenzklassen	202
12	Chiffrieralgorithmus T-310 aus heutiger Sicht	213
12.1	Vergleich mit einer Feistelchiffre.	214
12.2	Eine Langzeitschlüsseltechnologie heute	216
12.3	Einschätzung der Sicherheit des Chiffrieralgorithmus T-310 in Veröffentlichungen	217
12.4	Ergänzende eigene Ergebnisse.	218
12.5	Sicherheit des Chiffrieralgorithmus T-310	219
 Teil III Entwicklung und Analyse der Chiffrierverfahren		
13	Chiffrierverfahren	223
13.1	Chiffrierverfahren ARGON und ADRIA.	223
13.2	Chiffrierverfahren SAGA.	225
13.3	Analyse der Chiffrierverfahren	225
13.4	Bedrohungsmodell für das Chiffrierverfahren ARGON	227
14	Chiffriergeräte und Schlüsselmittel	231
14.1	Chiffriergeräte T-310/50 und T-310/51	232
14.2	Chiffurator und Langzeitschlüssel.	237
14.3	Schlüsselmittel.	238
14.4	Zufallsgeneratoren	240
14.4.1	Systemzufallsgenerator	241
14.4.2	Physikalischer Zufallsgenerator.	242
14.4.3	Stochastisches Modell der Zufallsgeneratoren	243
14.5	Schutz der Chiffrierung vor Fehlern und Manipulationen.	246
14.5.1	Physische Sicherheit der Chiffriergeräte	246
14.5.2	Selbsttest und prophylaktische Prüfung.	247
14.6	Kompromittierende Ausstrahlung	248
15	Sicherheit des Chiffrierverfahrens im Einsatz.	253
15.1	Installationsvorschrift.	254
15.2	Gebrauchsanleitung	255
15.3	Verkehrsanalyse	258
15.4	Authentisierung	259
15.5	Voraussetzungen für die Dekryptierung.	259
15.5.1	Angriffe auf den Zeitschlüssel	260
15.5.2	Kompromittierung einzelner Klartexte	261
15.5.3	Hypothetische Angriffe	262
15.6	Chiffriergeräte T-310 und die Chiffrierverfahren aus heutiger Sicht.	263

Teil IV Ende und Neuanfang

16 Das Ende des ZCO und der T-310	267
16.1 Drei Phasen im Vereinigungsprozess	268
16.2 Die Ereignisse in der ersten Phase und davor	270
16.3 Die Ereignisse in der zweiten Phase bis Juli 1990	270
16.3.1 Die gesicherte Fernschreibverbindung zwischen den beiden Innenministerien	273
16.3.2 Die Gegenstelle in der DDR	274
16.3.3 Warum das T-310-Gerät eingesetzt wurde	276
16.3.4 Kontakte zum ZSI/BSI – unsere Dienstreisen nach Bonn	277
16.3.5 Dienstreise von Dr. Leiberich zum ZCO in Dahlwitz-Hoppegarten	280
16.4 Die Ereignisse in der dritten Phase bis Oktober 1990 und danach	281
16.4.1 Die Auswirkungen der schnellen Vereinigung vom 3. Oktober	282
16.4.2 Die gesicherte Fernschreibverbindung zwischen den beiden Verteidigungsministerien	283
16.4.3 Nachtrag	284
16.5 Unsere letzte Aufgabe – Vernichtung der Geräte	285
17 Neuanfang bei der SIT	287
17.1 Umzug und Beginn der Arbeit	288
17.2 Nutzung der ALPHA-Dokumente	289
17.3 Unser Abschied von der SIT	289
A Liste der Vortragsthemen sowjetischer Kryptologen	291
B Liste der VS-Unterlagen ALPHA	293
C Operative LZS für SKS und T-310	297
D Dienstreisen nach Bonn im Sommer 1990	303
E LAMBDA1-Algorithmus	315
F Dienstreise von Dr. Leiberich am 24. Juli 1990	321
G Abkürzungen	325
Literatur	327
Stichwortverzeichnis	333