Killmann / Stephan

Das DDR-Chiffriergerät T-310

Kryptographie und Geschichte

54,99 €
51,39 € (zzgl. MwSt.)

Lieferfrist: bis zu 10 Tage

Dieses Buch beschreibt, unter welchen Bedingungen das in der DDR am weitesten verbreitete Fernschreibchiffriergerät sowie der dazugehörige Algorithmus vor etwa 50 Jahren zum Schutz von Staatsgeheimnissen entwickelt wurden. So können die damaligen Methoden und Ergebnisse mit den aktuellen Möglichkeiten der kryptologischen Analyse verglichen werden – insbesondere unter dem Aspekt der heute zur Verfügung stehenden Computertechnik.

Es wird herausgearbeitet, dass die konsequente Anwendung von Methoden der Gruppen- und Automatentheorie in der Analyse eine zentrale Rolle spielte. Dieser algebraische Analyseansatz aus der sowjetischen Schule wird bis heute unterschätzt – die Betrachtungsweisen können auch für Nichtkryptologen von Nutzen sein. Darüber hinaus werden die Unterschiede dargestellt zwischen der Analyse des Chiffrieralgorithmus, der Sicherheitsanalyse des Geräts und der Chiffrierverfahren, in denen es zum Einsatz kommt.

Die Ergänzungen in der zweiten Auflage beruhen auf Informationen früherer Mitarbeiter und auf Dokumenten aus den 80er Jahren, die erst nach Erscheinen der Erstauflage zugänglich wurden: Auf der Basis von Originaldokumenten wird nun die Historie der T-310-Entwicklung ausgehend vom Vorläuferalgorithmus SKS genauer dargestellt. Außerdem gelang es den Autoren, einige zuvor nicht lösbare Probleme mit der heute zur Verfügung stehenden Computertechnik zu bearbeiten – daran wird deutlich, wie begrenzt die Rechenkapazität in den 70er und 80er Jahren war. Schließlich wird der letzte Einsatz der T-310 zur Realisierung von gesicherten Fernschreibverbindungen zwischen Ministerien der BRD und der DDR rekonstruiert.

Dieses Buch beschreibt, unter welchen Bedingungen das in der DDR am weitesten verbreitete Fernschreibchiffriergerät sowie der dazugehörige Algorithmus vor etwa 50 Jahren zum Schutz von Staatsgeheimnissen entwickelt wurden. So können die damaligen Methoden und Ergebnisse mit den aktuellen Möglichkeiten der kryptologischen Analyse verglichen werden - insbesondere unter dem Aspekt der heute zur Verfügung stehenden Computertechnik.Es wird herausgearbeitet, dass die konsequente Anwendung von Methoden der Gruppen- und Automatentheorie in der Analyse eine zentrale Rolle spielte. Dieser algebraische Analyseansatz aus der sowjetischen Schule wird bis heute unterschätzt - die Betrachtungsweisen können auch für Nichtkryptologen von Nutzen sein. Darüber hinaus werden die Unterschiede dargestellt zwischen der Analyse des Chiffrieralgorithmus, der Sicherheitsanalyse des Geräts und der Chiffrierverfahren, in denen es zum Einsatz kommt.Die Ergänzungen in der zweiten Auflage beruhen auf Informationen früherer Mitarbeiter und auf Dokumenten aus den 80er Jahren, die erst nach Erscheinen der Erstauflage zugänglich wurden: Auf der Basis von Originaldokumenten wird nun die Historie der T-310-Entwicklung ausgehend vom Vorläuferalgorithmus SKS genauer dargestellt. Außerdem gelang es den Autoren, einige zuvor nicht lösbare Probleme mit der heute zur Verfügung stehenden Computertechnik zu bearbeiten - daran wird deutlich, wie begrenzt die Rechenkapazität in den 70er und 80er Jahren war. Schließlich wird der letzte Einsatz der T-310 zur Realisierung von gesicherten Fernschreibverbindungen zwischen Ministerien der BRD und der DDR rekonstruiert.

Artikelnummer: 9783662675830
Medium: Buch
ISBN: 978-3-662-67583-0
Verlag: Springer
Erscheinungstermin: 04.01.2024
Sprache(n): Deutsch
Auflage: 2., überarbeitete und erweiterte Auflage 2023
Produktform: Kartoniert
Gewicht: 546 g
Seiten: 335
Format (B x H): 155 x 235 mm

Kundenservice Verlag Dr. Otto Schmidt KG
Neumannstraße 10, 40235 Düsseldorf | kundenservice@otto-schmidt.de | 0221-93738-997 (Inland)