Killmann / Stephan

Das DDR-Chiffriergerät T-310

Kryptographie und Geschichte

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. Der Leser kann die damaligen Methoden und Ergebnisse mit den aktuellen Möglichkeiten einer kryptologischen Analyse vergleichen – 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 unter den Lesern 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. Schließlich wird auch das Ende der T-310 beschrieben, das mit dem Untergang der DDR einhergeht: Das Gerät wurde letztmalig im Vereinigungsprozess auf einer gesicherten Fernschreibverbindung zwischen Bonn und Berlin eingesetzt. Beide Autoren sind studierte Mathematiker und wirkten maßgeblich an der Entwicklung und Analyse der T-310 mit. Hier berichten erstmals Insider über diese Arbeit.

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. Der Leser kann die damaligen Methoden und Ergebnisse mit den aktuellen Möglichkeiten einer kryptologischen Analyse vergleichen – 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 unter den Lesern 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. Schließlich wird auch das Ende der T-310 beschrieben, das mit dem Untergang der DDR einhergeht: Das Gerät wurde letztmalig im Vereinigungsprozess auf einer gesicherten Fernschreibverbindung zwischen Bonn und Berlin eingesetzt. Die Autoren Beide Autoren sind studierte Mathematiker und wirkten maßgeblich an der Entwicklung und Analyse der T-310 mit. Hier berichten erstmals Insider über diese Arbeit. Wolfgang Killmann arbeitete im Zentralen Chiffrierorgan der DDR (ZCO) als Gruppenleiter, Referatsleiter, Abteilungsleiter. Nach dem Ende der DDR war er bei der SIT GmbH tätig, wechselte zum debis Systemhaus (später T-Systems) und war dort Leiter der Prüfstelle für Common Criteria. Winfried Stephan wechselte nach einer kurzen Assistenzzeit ebenfalls zum ZCO. Nach einem Zusatzstudium an der staatlichen Lomonossow-Universität Moskau arbeitete er hier als Gruppenleiter, Referatsleiter, stellvertretender Abteilungsleiter. Auch er wechselte zur SIT GmbH und dann zum debis Systemhaus: Im Bereich Automotive Security arbeitete er als Teamleiter und Senior Consultant.

49,99 €
46,72 € (zzgl. MwSt.)

Nicht mehr lieferbar

Artikelnummer: 9783662618967
Medium: Buch
ISBN: 978-3-662-61896-7
Verlag: Springer
Erscheinungstermin: 05.01.2021
Sprache(n): Deutsch
Auflage: 1. Auflage 2021
Produktform: Kartoniert
Gewicht: 454 g
Seiten: 248
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)