1.	Record Nr.	UNINA9910830886903321
	Autore	Good Irving John
	Titolo	Breaking teleprinter ciphers at Bletchley Park : an edition of General report on Tunny with emphasis on statistical methods (1945) / / I.J. Good, D. Michie and G. Timms ; edited and with introductions and notes by James A. Reeds, Whitfield Diffie and J.V. Field
	Pubbl/distr/stampa	Hoboken, New Jersey : , : John Wiley & Sons, Inc., , [2015] [Piscataqay, New Jersey] : , : IEEE Xplore, , [2015]
	ISBN	1-119-06160-1 1-119-06161-X
	Descrizione fisica	1 online resource (1118 p.)
	Disciplina	652.8
	Soggetti	Cryptography - Great Britain - History - 20th century World War, 1939-1945 - Electronic intelligence - Great Britain Bletchley Park (Milton Keynes, England) History
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa
	Livello bibliografico	Monografia
	Note generali	Description based upon print version of record.
	Nota di bibliografia	Includes bibliographical references and index.
	Nota di contenuto	Preface xiii -- Editorial Notes xiv -- Notes on Vocabulary xiv -- List of Abbreviations xv -- Cryptanalytic Significance of the Analysis of Tunny, by Whitfield Diffie xvii -- Editors' Introduction, by Whitfield Diffie and J. V. Field xxv -- Statistics at Bletchley Park, by S. L. Zabell lxxv -- Biographies of Authors ciii -- Notes on the Editors of the Present Volume cvii -- List of Figures cix -- General Report on Tunny, with emphasis on statistical methods 1 -- Part 0: Preface -- Chapter 01: Preface 3 -- Part 1: Introduction -- Chapter 11: German Tunny 6 -- Chapter 12: Cryptographic Aspects 22 -- Chapter 13: Machines 32 -- Chapter 14: Organisation 35 -- Chapter 15: Some Historical Notes 39 -- Part 2: Methods of Solution -- Chapter 21: Some Probability Techniques 43 -- Chapter 22: Statistical Foundations 50 -- Chapter 23: Machine Setting 80 -- Chapter 24: Rectangling 110 -- Chapter 25: Chi-Breaking from Cipher 139 -- Chapter 26: Wheel-Breaking from Key 185 -- Chapter 27: Cribs 219 -- Chapter 28: Language Methods 237 -- Part 3: Organisation -- Chapter 31: Mr Newman's Section 262 -- Chapter 32: Organisation of the Testery 267 -- Chapter 33: Knockholt

Sommario/riassunto

This detailed technical account of breaking Tunny is an edition of a report written in 1945, with extensive modern commentary Breaking Teleprinter Ciphers at Bletchley Park gives the full text of the General Report on Tunny (GRT) of 1945, making clear how the ideas, notation and the specially designed machines that were used differ from what was generally accepted in 1945, and, where a modern reader might be misled, from what is understood now. The editors of this book clarify the sometimes slightly strange language of the GRT and explain the text within a variety of contexts in several separate historical story lines, some only implicit in the GRT itself. The first story, told by the authors of the GRT, describes how, using specially designed machines, including from 1944 the "Colossus", the British broke the enciphered teleprinter messages sent by the highest command levels of the Germany Army. The cipher machines the Germans used were the Lorenz SZ 40 series, called "Tunny" by the British. The second story shows how the use of then-unfashionable Bayesian methods in statistics proved to be essential to the British success. The third story describes a significant stage in the invention of the modern digital computer. This story is connected with Alan Turing's 1936 paper on the theory of computability, which is nowadays seen as a starting point for the development of the modern digital computer. This book includes: . Over 200 pages of commentary, biographies, glossaries, and essays related to the text of the General Report on Tunny. The complete text of the original GRT, covering the general theory of Tunny breaking and of numerous refinements appropriate to special-case situations. All the examples of original worksheets and printouts, showing the Tunny-breaking process in action, that appear in the GRT The main purpose of this book is to present the actual words of the GRT for use by readers with a serious interest in the history of cryptography, computing, or mathematics.