

## Contents

Reminiscences and Reflections of a Codebreaker . . . . .	1
<i>Peter Hilton</i>	
FISH and I. . . . .	9
<i>W. T. Tutte</i>	
Sturgeon, The FISH BP Never Really Caught . . . . .	18
<i>Frode Weierud</i>	
ENIGMA and PURPLE: How the Allies Broke German and Japanese Codes During the War . . . . .	53
<i>David A. Hatch</i>	
The Geheimschreiber Secret . . . . .	62
<i>Lars Ulfving, Frode Weierud</i>	
The RSA Public Key Cryptosystem . . . . .	101
<i>William P. Wardlaw</i>	
Number Theory and Cryptography (using Maple) . . . . .	124
<i>John Cosgrave</i>	
A Talk on Quantum Cryptography or How Alice Outwits Eve . . . . .	144
<i>Samuel J. Lomonaco, Jr.</i>	
The Rigidity Theorems of Hamada and Ohmori, Revisited . . . . .	175
<i>T. S. Michael</i>	
Counting Prime Divisors on Elliptic Curves and Multiplication in Finite Fields . . . . .	180
<i>M. Amin Shokrollahi</i>	
On Cyclic MDS-Codes . . . . .	202
<i>M. Amin Shokrollahi</i>	
Computing Roots of Polynomials over Function Fields of Curves . . . . .	214
<i>Shuhong Gao, M. Amin Shokrollahi</i>	
Remarks on codes from modular curves: MAPLE applications . . . . .	229
<i>David Joyner and Salahoddin Shokranian</i>	
Index . . . . .	251

Coding Theory and Cryptography  
From Enigma and Geheimschreiber to Quantum Theory  
Joyner, D. (Ed.)  
2000, VII, 256 p. 7 illus., Softcover  
ISBN: 978-3-540-66336-2