

Contents

Section 1: Introduction

- Trends in the Fight Against Computer-Related Delinquency* 3
Bart De Schutter
- Technical Approaches to Thwart Computer Fraud* 20
Joos Vandewalle, René Govaerts, and Bart Preneel

Section 2: Theory

- Public Key Cryptography* 33
Marijke De Soete
- Better Login Protocols for Computer Networks* 50
Dominique de Waleffe and Jean-Jacques Quisquater
- Secret-Key Exchange with Authentication* 71
Johan van Tilburg
- Information Authentication: Hash Functions and Digital Signatures* 87
Bart Preneel, René Govaerts, and Joos Vandewalle
- Key Management* 132
Walter Fumy

Section 3: Applications

- Evaluation Criteria for IT Security* 151
David W. Roberts

<i>Standardization of Cryptographic Techniques</i>	162
Bart Preneel	
<i>Numbers Can Be a Better Form of Cash than Paper</i>	174
David Chaum	
<i>ISO-OSI Security Architecture</i>	179
Jan Verschuren, René Govaerts, and Joos Vandewalle	
<i>Security Aspects of Mobile Communications</i>	193
Klaus Vedder	
<i>(Local Area) Network Security</i>	211
Walter Fumy	
<i>Cryptography Within Phase I of the EEC-RACE Programme</i>	227
Antoon Bosselaers, René Govaerts, and Joos Vandewalle	
<i>EDI security</i>	235
Gordon Lennox	
<i>AXYTRANS: Physical Funds Transport and DES</i>	244
Marc Geoffroy, Ronny Bjones, and Hedwig Cnudde	
<i>Unix Security & Kerberos</i>	257
Bart De Decker	
Author Index	275