

Sicherheits- mechanismen

Bausteine zur Entwicklung sicherer Systeme

herausgegeben von

Dr. Otfried Fries, Siemens AG, München

Andreas Fritsch, IABG, Ottobrunn

Dr. Volker Kessler, Siemens AG, München

Birgit Klein, E.I. S. S., Universität Karlsruhe

Mit Beiträgen von

F. Damm (E.I.S.S.), H.-J. Knobloch (E.I.S.S.),

O. Kowalski (GMD), S. Mund (Siemens AG),

Dr. A. Steinacker (IABG), H. Strack (E.I.S.S.)

und P. Wichmann (E. I. S. S.)

R. Oldenbourg Verlag München Wien 1993

Inhaltsverzeichnis

Vorwort.....	<i>i</i>
I Handhabung.....	9
1.1 Aufbau des Katalogs.....	11
1.2 Anwendung des Katalogs.....	25
1.3 Literatur.....	30
II Mechanismen.....	31
Asymmetrische Verschlüsselung.....	31
Auditing.....	37
Beth Zero-Knowledge Identifikationsschema.....	43
Biometrische Verfahren.....	49
Blockchiffre im CBC-Modus.....	57
Blockchiffre im CFB-Modus.....	64
Blockchiffre im ECB-Modus.....	71
Blockchiffre im OFB-Modus.....	77
Blum-Micali-Zufallszahlengenerator.....	83
Capability.....	88
CCITT X.509: Authentifikationsprotokolle.....	94
CCITT X.509: Einfaches Authentifikationsprotokoll.....	103
CCITT X.509: Schlüsselverteilung von öffentlichen Schlüsseln.....	109
Chipkarte.....	116
Data Encryption Standard (DES).....	123
Diffie-Hellman Schlüsselaustausch.....	132
Digital Signature Algorithm (DSA).....	137
Digitale Signatur.....	144
Directory.....	152
Discretionary Access Control.....	157
Dummy Nachrichten.....	165
ElGamal-Signatur.....	171
ElGamal-Verschlüsselung.....	177
Fast Encipherment Algorithm (FEAL).....	182
Fiat-Shamir-Protokoll.....	193
GUARDS.....	200
IBM Schlüsselmanagement.....	206
Information Labeling.....	211
International Data Encryption Standard (IDEA).....	216
Intrusion-Detection Expert System (IDES).....	224
IP Paketfilterung.....	232

Inhaltsverzeichnis

ISO 9798 Ein-Weg-Authentifikation.....	241
ISO 9798 Zwei-Weg-Authentifikation.....	247
KATHY.....	252
Least Privilege.....	260
Mandatory Access Control.....	267
Message Authentication Code.....	274
Message Digest.....	281
Message Digest Algorithm MD4/MD5.....	289
Meyer-Schilling-Hashfunktion.....	299
Modulauthentifikation.....	306
Multicasting/Broadcasting.....	313
Needham-Schroeder-Protokoll (konventionell).....	319
Needham-Schroeder-Public-Key-Protokoll.....	325
Otway-Rees-Protokoll.....	330
Paßwortverfahren.....	335
RSA.....	342
Schieberegisterfolgen.....	350
Schnorr-Verfahren.....	360
Secure Hash Standard SHS.....	367
Senden über MIXe.....	375
Shared Secret Schemes.....	381
Square-mod-n.....	389
Stromchiffre.....	{...394
Subjektrestriktionsliste.....'.....>.....	400
Symmetrische Verschlüsselung.....	405
Überlagerndes Senden.....	410
Verbindungsorientierter Integritätsmechanismus.....	416
Zugriffskontrollliste.....	422
Zugriffskontrollmatrix.....	435
 Anhang.....	 439
 Indexregister.....'	 445