



Protocols for Authentication and Key Establishment /

Boyd, Colin

Springer Berlin Heidelberg,
2003

Electronic books

Monografía

Protocols for authentication and key establishment are the foundation for security of communications. The range and diversity of these protocols is immense, while the properties and vulnerabilities of different protocols can vary greatly. This is the first comprehensive and integrated treatment of these protocols. It allows researchers and practitioners to quickly access a protocol for their needs and become aware of existing protocols which have been broken in the literature. As well as a clear and uniform presentation of the protocols this book includes a description of all the main attack types and classifies most protocols in terms of their properties and resource requirements. It also includes tutorial material suitable for graduate students

<https://rebiunoda.pro.baratznet.cloud:38443/OpacDiscovery/public/catalog/detail/b2FpOmNlbGVicmF0aW9uOmVzLmJhcmF0ei5yZW4vMjE4ODM4ODU>

Título: Protocols for Authentication and Key Establishment by Colin Boyd, Anish Mathuria

Editorial: Berlin, Heidelberg Springer Berlin Heidelberg 2003

Descripción física: 1 online resource (xxiv, 323 pages)

Mención de serie: Information Security and Cryptography, Texts and Monographs 1619-7100

Contenido: A Tutorial Introduction to Authentication and Key Establishment -- Goals for Authentication and Key Establishment -- Protocols Using Shared Key Cryptography.-Authentication and Key Transport Using Public Key Cryptography -- Key Agreement Protocols -- Conference Key Protocols -- Password-Based Protocols -- Appendix A -- Standards for Authentication and Key Establishment -- Appendix B -- Summary of Notation -- References -- Index of Protocols -- General Index

Copyright/Depósito Legal: 934998421 936319355

ISBN: 9783662095270 electronic bk.) 3662095270 electronic bk.) 9783642077166 3642077161 3662095270

Materia: Computer science Computer Communication Networks Data protection Data encryption (Computer science) Computer software Computer science Computer software Data encryption (Computer science) Data protection

Autores: Mathuria, Anish

Enlace a formato físico adicional: Print version 9783642077166

Baratz Innovación Documental

- Gran Vía, 59 28013 Madrid
- (+34) 91 456 03 60
- informa@baratz.es