ISO/IEC 18033-2:2006, Information Technology - Security Techniques - Encryption Algorithms - Part 2: Asymmetric Ciphers


INTERNATIONAL STANDARD

ISO/IEC 18033-2

Information technology — Security techniques — Encryption algorithms —

Part 2:
Asymmetric ciphers

Synopsis

ISO/IEC 18033-2:2006 specifies encryption systems (ciphers) for the purpose of data confidentiality. The primary purpose of encryption (or encipherment) techniques is to protect the confidentiality of stored or transmitted data. An encryption algorithm is applied to data (often called plaintext or cleartext) to yield encrypted data (or ciphertext); this process is known as encryption. The encryption algorithm should be designed so that the ciphertext yields no information about the plaintext except, perhaps, its length. Associated with every encryption algorithm is a corresponding decryption algorithm, which transforms ciphertext back into its original plaintext.An asymmetric, i.e. public-key, encryption scheme allows a sender to use a recipient's public key to transmit an encryption of a message to the receiver, who can use his secret key to decrypt the given ciphertext, thereby obtaining the original message. Such a scheme should be secure in the sense that no information about the message should be leaked to a (resource-bounded) attacker, even if that attacker mounts a so-called 'chosen ciphertext' attack, in which he may obtain decryptions of other ciphertexts. This is the strongest type of attack that has been proposed for a public-key encryption scheme. ISO/IEC 18033-2:2006 specifies the functional interface of such a scheme, and in addition specifies a number of particular schemes that appear to be secure against chosen ciphertext attack. The different schemes offer different trade-offs between security properties and efficiency.

Book Information

Paperback: 132 pages

Publisher: Multiple. Distributed through American National Standards Institute (ANSI) (August 23, 2007)

Language: English

ASIN: B000XYT4A0

Product Dimensions: 8.2 x 0.3 x 10.5 inches

Shipping Weight: 13.4 ounces (View shipping rates and policies)

Average Customer Review: 5.0 out of 5 stars 1 customer review

Best Sellers Rank: #2,536,899 in Books (See Top 100 in Books) #24 inÃ Â Books > Engineering & Transportation > Engineering > Reference > American National Standards Institute (ANSI) Publications #442361 inÃ Â Books > Textbooks

Customer Reviews

I contribute to free and open source software. Publications like ISO/IEC 18033-2:2006 and IEE P1363A are essential for creating interoperable software. I am thankful the standard is available for

purchase on .I was not happy to spend a non-trivial amount of money on this since its out of my own pocket, but there's nothing can do about it since there's only one vendor supplying the publication.

ISO/IEC 18033-2:2006, Information technology - Security techniques - Encryption algorithms - Part 2: Asymmetric ciphers ISO/IEC 27002:2005, Information technology - Security techniques - Code of practice for information security management (Redesignation of ISO/IEC 17799:2005) ISO/IEC 27002:2013, Second Edition: Information technology Security techniques Code of practice for information security controls ISO/IEC 27001:2013, Second Edition: Information technology - Security techniques - Information security management systems - Requirements ISO/IEC 27005:2011, Information technology - Security techniques - Information security risk management ISO/IEC 11770-2:1996, Information technology - Security techniques - Key management - Part 2: Mechanisms using symmetric techniques ISO/IEC 20000-1:2011, Information technology - Service management - Part 1: Service management system requirements ISO/IEC 20000-2:2012, Information technology - Service management - Part 2: Guidance on the application of service management systems Iso/Iec 19770-1:2012, Information technology - Software asset management - Part 1: Processes and tiered assessment of conformance Fundamentals Of Information Systems Security (Information Systems Security & Assurance) - Standalone book (Jones & Bartlett Learning Information Systems Security & Assurance) Approaches to Solve Big Data Security Issues and Comparative Study of Cryptographic Algorithms for Data Encryption The Mathematics of Secrets: Cryptography from Caesar Ciphers to Digital Encryption ISO/IEC 38500:2008, Corporate governance of information technology Mastering Algorithms with C: Useful Techniques from Sorting to Encryption ISO/IEC Guide 98-3:2008, Uncertainty of measurement - Part 3: Guide to the expression of uncertainty in measurement (GUM:1995) ISO/IEC 31010:2009, Risk management - Risk assessment techniques IEC 60812 Ed. 2.0 b:2006, Second Edition: Analysis techniques for system reliability - Procedure for failure mode and effects analysis (FMEA) Social Security & Medicare Facts 2016: Social Security Coverage, Maximization Strategies for Social Security Benefits, Medicare/Medicaid, Social Security Taxes, Retirement & Disability, Ser Human Systems Integration to Enhance Maritime Domain Awareness for Port/Harbour Security: Volume 28 NATO Science for Peace and Security Series - D: ... D: Information and Communication Security) ISO/TS 20022-3:2004, Financial services - UNIversal Financial Industry message scheme - Part 3: ISO 20022 modelling guidelines