1. Record Nr. UNINA9910451061503321

| | |
|---|---|
| Autore | St. Denis Tom |
| Titolo | Cryptography for developers [[electronic resource] /] / Tom St Denis, Simon Johnson |
| Pubbl/distr/stampa | Rockland, MA, : Syngress Publishing, Inc., c2007 |
| ISBN | 1-281-07185-4<br>9786611071851<br>0-08-050345-4 |
| Edizione | [1st edition] |
| Descrizione fisica | 1 online resource (449 p.) |
| Altri autori (Persone) | JohnsonSimon |
| Disciplina | 005.8/2<br>005.82 |
| Soggetti | Computer software - Development<br>Cryptography<br>Electronic books. |
| Lingua di pubblicazione | Inglese |
| Formato | Materiale a stampa |
| Livello bibliografico | Monografia |
| Note generali | Includes index. |
| Nota di contenuto | Front Cover; Cryptography for Developers; Copyright Page; Contents; Preface; Chapter 1. Introduction; Introduction; Threat Models; What Is Cryptography?; Asset Management; Common Wisdom; Developer Tools; Summary; Organization; Frequently Asked Questions; Chapter 2. ASN.1 Encoding; Overview of ASN.1; ASN.1 Syntax; ASN.1 Data Types; ASN.1 Length Encodings; ASN. 1 Boolean Type; ASN.1 Integer Type; ASN.1 BIT STRING Type; ASN.1 OCTET STRING Type; ASN.1 NULL Type; ASN.1 OBJECT IDENTIFIER Type; ASN.1 SEQUENCE and SET Types; ASN.1 PrintableString and IA5STRING Types; ASN.1 UTCTIME Type IniplementationASN.1 Length Routines; ASN.1 Primitive Encoders; Putting It All Together; Frequently Asked Questions; Chapter 3. Random Number Generation; Introduction; Measuring Entropy; How Bad Can It Be?; RNG Design; PRNG Algorithms; Putting It All Together; Frequently Asked Questions; Chapter 4. Advanced Encryption Standard; Introduction; Implementation; Practical Attacks; Chaining Modes; Putting It All Together; Frequently Asked Questions; Chapter 5. Hash Functions; Introduction; Designs of SHS and Implementation; PKCS # 5 Key Derivation; Putting It All Together |

Frequently Asked QuestionsChapter 6. Message-Authentication Code Algorithms; Introduction; Security Guidelines; Standards; Cipher Message Authentication Code; Hash Message Authentication Code; Putting It All Together; Frequently Asked Questions; Chapter 7. Encrypt and Authenticate Modes; Introduction; Design and Implementation; Putting It All Together; Frequently Asked Questions; Chapter 8. Large Integer Arithmetic; Introduction; What Are BigNums?; The Algorithms; Putting It All Together; Frequently Asked Questions; Chapter 9. Public Key Algorithms; Introduction
Goals of Public Key CryptographyRSA Public Key Cryptography; Elliptic Curve Cryptography; Putting It All Together; Frequently Asked Questions; Index

Sommario/riassunto

The only guide for software developers who must learn and implement cryptography safely and cost effectively.The book begins with a chapter that introduces the subject of cryptography to the reader. The second chapter discusses how to implement large integer arithmetic as required by RSA and ECC public key algorithms The subsequent chapters discuss the implementation of symmetric ciphers, one-way hashes, message authentication codes, combined authentication and encryption modes, public key cryptography and finally portable coding practices. Each chapter includes in-depth discussion on