1.	Record Nr.	UNINA9910141045803321
	Autore	Davies Joshua Dennis
	Titolo	Implementing SSL/TLS using cryptography and PKI [[electronic resource] /] / Joshua Davies
	Pubbl/distr/stampa	Indianapolis, Ind., : Wiley Pub., Inc, 2011
	ISBN	1-283-02725-9 9786613027252 1-118-25579-8 1-118-03877-0 1-118-03875-4
	Edizione	[1st ed.]
	Descrizione fisica	1 online resource (697 p.)
	Disciplina	005.8
	Soggetti	Computer networks - Security measures World Wide Web - Security measures Computer network protocols
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa
	Livello bibliografico	Monografia
	Note generali	Description based upon print version of record.
	Nota di contenuto	Implementing SSL/TLS Using Cryptography and PKI; Contents; Introduction; Chapter 1: Understanding Internet Security; What Are Secure Sockets?; "Insecure" Communications: Understanding the HTTP Protocol; Implementing an HTTP Client; Adding Support for HTTP Proxies; Reliable Transmission of Binary Data with Base64 Encoding; Implementing an HTTP Server; Roadmap for the Rest of This Book; Chapter 2: Protecting Against Eavesdroppers with Symmetric Cryptography; Understanding Block Cipher Cryptography Algorithms; Implementing the Data Encryption Standard (DES) Algorithm; DES Initial Permutation DES Key ScheduleDES Expansion Function; DES Decryption; Padding and Chaining in Block Cipher Algorithms; Using the Triple-DES Encryption Algorithm to Increase Key Length; Faster Encryption with the Advanced Encryption Standard (AES) Algorithm; AES Key Schedule Computation; AES Encryption; Other Block Cipher Algorithms; Understanding Stream Cipher Algorithms; Understanding and Implementing the RC4 Algorithm; Converting a Block Cipher to a Stream Cipher: The OFB and

COUNTER Block-Chaining Modes; Chapter 3: Secure Key Exchange over an Insecure Medium with Public Key Cryptography

Understanding the Theory Behind the RSA AlgorithmPerforming Arbitrary Precision Binary Math to Implement Public-Key Cryptography; Implementing Large-Number Addition; Implementing Large-Number Subtraction; Implementing Large-Number Division; Comparing Large Numbers; Optimizing for Modulo Arithmetic; Using Modulus Operations to Efficiently Compute Discrete Logarithms in a Finite Field; Encryption and Decryption with RSA; Encrypting with RSA; Decrypting with RSA; Encrypting a Plaintext Message; Decrypting an RSA-Encrypted Message; Testing RSA Encryption and Decryption

Getting More Security per Key Bit: Elliptic Curve CryptographyHow Elliptic Curve Cryptography Relies on Modular Inversions; Using the Euclidean Algorithm to compute Greatest Common Denominators; Computing Modular Inversions with the Extended Euclidean Algorithm; Adding Negative Number Support to the Huge Number Library; Supporting Negative Remainders; Making ECC Work with Whole Integers: Elliptic-Curve Cryptography over Fp; Reimplementing Diffie-Hellman to Use ECC Primitives; Why Elliptic-Curve Cryptography?; Chapter 4: Authenticating Communications Using Digital Signatures

Using Message Digests to Create Secure Document SurrogatesImplementing the MD5 Digest Algorithm; Understanding MD5; A Secure Hashing Example; Securely Hashing a Single Block of Data; MD5 Vulnerabilities; Increasing Collision Resistance with the SHA-1 Digest Algorithm; Understanding SHA-1 Block Computation; Understanding the SHA-1 Input Processing Function; Understanding SHA-1 Finalization; Even More Collision Resistance with the SHA-256 Digest Algorithm; Preventing Replay Attacks with the HMAC Keyed-Hash Algorithm; Implementing a Secure HMAC Algorithm; Completing the HMAC Operation

Creating Updateable Hash Functions

Sommario/riassunto

Hands-on, practical guide to implementing SSL and TLS protocols for Internet security If you are a network professional who knows C programming, this practical book is for you. Focused on how to implement Secure Socket Layer (SSL) and Transport Layer Security (TLS), this book guides you through all necessary steps, whether or not you have a working knowledge of cryptography. The book covers SSLv2, TLS 1.0, and TLS 1.2, including implementations of the relevant cryptographic protocols, secure hashing, certificate parsing, certificate generation, and more.   Coverage includes: <li