

---

## Practical Cryptology and Web Security (A Summary of Examples in the Book)

### Chapter1: Basic Security Skills on the World Wide Web

Example: ex01-01.htm - A Simple Page  
Example: ex01-02.htm - My First Page With Security  
Example: ex01-03.htm - My First XHTML Page  
Example: ex01-04.htm - Number Systems On The Web  
Example: ex01-05.htm - ASCII Character Code  
Example: ex01-06.htm - Display A Message With ASCII Codes  
Example: ex01-07.htm - Unicode Characters  
Example: ex01-08.htm - Getting Unicode Values  
Example: ex01-09.htm - Numerical Representations Of A Message  
Example: ex01-10.htm - Implementation Of Caesar's Code  
Example: ex01-11.htm - Bitwise Operators  
Example: ex01-12.htm - The Base64 Encoding and Decoding  
    ex01-12.js - ECMAScript File For Example ex01-12.htm  
Example: ex01-13.htm - The XOR Encryption Scheme  
    ex01-13.js - External ECMAScript For ex01-13.htm  
Example: ex01-14.htm - The XOR Encryption Scheme  
    ex01-14.js - External ECMAScript For ex01-14.htm  
Example: hexlib.js - Some Hexadecimal Functions  
Example: ex01-15.htm - The PkZip/WinZip Encryption Scheme  
    ex01-15.js - ECMAScript For ex01-15.htm

### Chapter 2 Cryptology, Web Site Protections, and Attacks

Example: ex02-01.htm - Generating UNIX/LINUX Encrypted Passwords  
Example: ex02-02.htm - Testing Web Page For The Basic Authentication  
Example: ex02-03.htm - Basic HTTP Authentication I  
Example: ex02-04.htm - Basic HTTP Authentication II  
Example: ex02-05.htm - Basic HTTP Authentication III  
Example: ex02-06.htm - Digest Authentication  
Example: ex02-07.htm - Basic HTTP Authentication IV  
Example: ex02-08.htm - Generating Digest Password  
Example: ex02-09.htm - A Simple Key-Space Scheme Using For Loops  
    ex02-09.js - ECMAScript File For ex02-09.htm  
Example: ex02-10.htm - Brute-Force: Quotient&Remainder  
    ex02-10.js - ECMAScript File For ex02-10.htm  
Example: ex02-11.htm - Key Space I  
    ex02-11.js - The Brute-Force: Position Update  
Example: ex02-12.htm - md5 Password Attacks Using Brute-Force  
    ex02-12.js - The ECMAScript Program For ex02-06.htm  
Example: brute-force.c - A Brute-Force Utility For MD5

### Chapter 3 One-Way Encryptions, Hash Functions, and Message Digests

Example: ex03-01.htm - Generating DES Sub-Keys  
    ex03-01.js - ECMAScript File To Generate DES Sub-Keys  
Example: ex03-02.htm - DES Encryption On One Chunk Of Data  
    ex03-02.js - DES Encryption  
Example: ex03-03.htm - DES Decryption On One Chunk Of Data  
    ex03-03.js - DES Decryption  
Example: ex03-04.htm - The Crypt()  
    ex03-04.js - The Crypt() algorithm

---

Example: ex03-05.htm - Generating MD5 Digest  
ex03-05.js - Implementation of Message Digest md5()  
Example: ex03-06.htm - Protect Download Files Against Virus and Alterations  
Example: ex03-07.htm - md5Crypt() Page  
ex03-07.js - Implementation of md5Crypt on the Web  
Example: ex03-08.htm - Generating SHA-1 Digest  
ex03-08.js - Implementation of SHA-1 Digest  
Example: shaldriver.c - The C Program For SHA-1 Utility

## Chapter 4 Some Strong Symmetric-Key Ciphers

Example: ex04-01.htm - Generating Data For SP-Boxes  
ex04-01.js - Generating The Data For SP-Boxes  
Example: ex04-02.htm - Testing the IP Permutation Sequences  
ex04-02.js - The Permutation Sequence Of Table IP  
Example: ex04-03.js - The Optimized DES Encryption  
Example: ex04-04.js - Set Up and Scheduling Sub-Keys  
Example: ex04-05.htm - DES Encryption/Decryption Page  
ex04-05.js - DES Encryption/Decryption  
Example: ex04-06.htm - Page for DES Cipher Under CBC Mode  
ex04-06.js - The CBC Mode Of DES Encryption/Decryption  
Example: ex04-07.htm - Triple DES Encryption/Decryption Page  
Example: ex04-07.js - Triple DES Encryption/Decryption  
Example: des3driver.c - A Tri-DES Utility To Work With Files  
Example: ex04-08.htm - CAST-128 Encryption/Decryption Page  
ex04-08.js - CAST-128 Encryption/Decryption  
Example: cast128driver.c - A Utility For CAST-128  
Example: ex04-09.htm - CAST-128 Encryption/Decryption With Modes  
ex04-09.js - CAST-128 With Operation Modes

## Chapter 5 Practical Software-Based Stream Ciphers

Example: ex05-01.htm - OFB Mode As Stream Cipher Page (Not Complete)  
ex05-01.js - Implement OFB Mode As Stream Cipher  
Example: ex05-02.htm - Generating Random Keys For OTP  
ex05-02.js - Generating One-Time-Pad Keys  
Example: ex05-03.htm - A Page For OTP Encryption/Decryption  
ex05-03.js - Implement OTP Encryption/Decryption  
Example: ex05-04.htm - Generating Random Number - ex05-04.htm  
ex05-04.js - Generating Random Numbers Using LCG  
Example: ex05-05.c - Blum-Blum-Shub Pseudo-Random Number  
Example: ex05-06.htm - BBS With Web Page  
Example: ex05-07.htm - 64-Bit Multiplication Example  
Example: ex05-08.htm - The ARC4 Scheme  
ex05-08.js - The Implementation of ARC4  
Example: ex05-09.c - C Implementation of the ARC4 Scheme  
Example: rc4driver.c - A Driver Program For ARC4 Encryption/Decryption  
Example: ex05-10.htm - A Page For ISAAC Pseudo-Random Numbers  
ex05-10.js - The ISAAC Pseudo-Random Number Generator  
Example: ex05-11.htm - The ISAAC Stream Cipher  
ex05-11.js - Script For The ISAAC Stream Cipher  
Example: isaac\_driver.c - The Driver for ISAAC Stream Cipher  
Example: ex05-12.htm - SEAL2 Encryption and Decryption (Not Complete)  
ex05-12.js - SEAL2 Encryption and Decryption  
Example: seal2driver.c - The Driver For SEAL2 Stream Cipher

## Chapter 6 Block Ciphers with Variable Key-Lengths

Example: ex06-01.htm - Blowfish Scheme I  
ex06-01.js - Implementation of the Blowfish Scheme  
Example: blowfishdriver.c - Blowfish Driver Program  
Example: ex06-02.htm - Blowfish Scheme II  
Example: ex06-03.htm - Finding Digit of  $\pi$  and Blowfish Constants  
ex06-03.js - Finding Any Digit of Pi  
Example: ex06-04.htm - RC6 Scheme  
ex06-04.js - RC-6/32/20/b Encryption and Decryption  
Example: ex06-05.htm - RC6 Scheme (Hex)  
ex06-04.js - RC-6/32/20/b Encryption and Decryption  
Example: rc6driver.c - The RC6 Encryption/Decryption Driver  
Example: ex06-06.htm - Fractional To Hexadecimal Digits  
ex06-06.js - Fraction Decimal to Hexadecimal Conversion  
Example: ex06-07.htm - Generating AES Forward Tables FT0, FT1, FT2, and FT3  
Example: ex06-08.htm - AES Tables  
Example: ex06-09.htm - AES Encryption and Decryption Page  
ex06-09.js - AES Encryption and Decryption  
Example: ex06-10.htm - AES Encryption/Decryption (Hex Input)  
ex06-09.js - AES Encryption and Decryption  
Example: aesdriver.c - The AES Encryption/Decryption Driver

## Chapter 7: Encryption and Server Skills for Web Page Protection

Example: ex07-01.htm - A Simple Page To Be Encrypted  
Example: ex07-02.htm - Protecting Web Page Contents  
Example: ex07-03.htm - Generating Encrypted Web Page  
Example: ex07-04.htm - A Testing Page For Windows Script Encoder  
Example: ex07-05.htm - is the same as ex05-08.htm (RC4 Encryption)  
Example: ex07-06.htm - A Page To Be Licensed  
Example: ex07-07.htm - Software Licensing and Activation Code  
Example: ex07-08.htm - Security With Cookie  
cookie.js - Cookie Operations with ECMAScript  
Example: ex07-09.c - A C/C++ Program For CGI  
Example: ex07-10.pl - A Framework To Convert XHTML To Perl  
Example: ex07-11.php - Generating XHTML With PHP  
Example: ex07-12.htm - An HTML/XHTML Password Page  
ex07-12.pl - Perl Script for ex07-12.htm  
Example: ex07-13.php - User Authentication Using PHP  
Example: ex07-14.htm - Using File Storage With Perl  
Example: ex07-15.php - Using File Storage With PHP  
Example: ex07-16.pl - The Perl Script For ex07-16.htm  
Example: ex07-17.php - PHP Script For ex07-17.htm  
Example: ex07-18.pl - Set Up Password Account Using Perl  
Example: ex07-19.php - Set Up Password Account Using PHP  
Example: ex07-20.php - Encrypted Password in Database  
Example: ex07-21.php - Adding New Password Account  
Example: ex07-22.php - Updating and Changing Password Account

---

## Chapter 8 Practical Public-Key Security and Digital Signatures

Example: ex08-01.htm - Generating The Diffie-Hellman Public-Key  
Example: ex08-02.htm - Compute The DH Shared-Key  
Example: ex08-03.htm - Brute-Force Attack On DH Key Exchange Scheme  
Example: ex08-04.htm - The ElGamal Encryption Algorithm  
Example: ex08-05.htm - The ElGamal Decryption Algorithm  
Example: ex08-06.htm - The ElGamal Message Encryption  
Example: ex08-07.htm - ElGamal Message Decryption II  
Example: ex08-08.htm - The ElGamal Digital Signature  
Example: ex08-09.htm - Digital Signature Verification  
Example: ex08-10.htm - Generating RSA Public and Secret Keys  
Example: ex08-11.htm - Message Encryption Using RSA Scheme  
Example: ex08-12.htm - Message Decryption Using RSA Scheme  
Example: ex08-13.htm - Sending Secure Message With Signature  
Example: ex08-14.htm - Receiving RSA Secure Message  
Example: ex08-15.htm - Message Encryption With A Hybrid Scheme  
Example: ex08-16.htm - Message Decryption With A Hybrid Scheme  
Example: ex08-17.htm - Adding Two Points On An Elliptic Curve  
elliptic.js - Elliptic Curve Operations with ECMAScript  
Example: ex08-18.htm - Scalar Multiplication On An Elliptic Curve  
elliptic.js - Elliptic Curve Operations with ECMAScript  
Example: ex08-19.htm - Public-Key Of An ECC system  
elliptic.js - Elliptic Curve Operations with ECMAScript  
Example: ex08-20.htm - Elliptic Curve Encryption  
elliptic.js - Elliptic Curve Operations with ECMAScript  
Example: ex08-21.htm - ECC Decryption  
elliptic.js - Elliptic Curve Operations with ECMAScript

## Chapter 9 Security Applications with GnuPG, WinPT and Server Techniques

Example: ex09-01.gpg - Generating Public/Secret Key Pair on GnuPG  
Example: ex09-02.gpg - Displaying Keys Inside Public Key-Ring  
Example: ex09-04.gpg - The Public-Key of johnsmith (file: johnsmith.key)  
Example: ex09-05.gpg - Importing a Public-Key  
Example: ex09-06.gpg - List All Public-Keys  
Example: ex09-07.gpg - Validate and Signing an Imported Key  
Listing: ex09-08.txt - Sample Important File: mary.txt  
Example: ex09-09.gpg - The Encrypted Message File: mary.gpg  
Example: ex09-10.gpg - Decryption Using GnuPG  
Example: ex09-11.gpg - Symmetric Encryption/Decryption Using GnuPG  
Example: ex09-12.pl - A Simple Perl Script I  
Example: ex09-13.pl - A Simple Perl Script II  
Example: ex09-14.pl - An Email Framework With Perl  
Example: ex09-15.htm - A Generate Page To Send Email With Perl  
ex09-15.pl - Perl Script For ex09-15.pl  
Example: ex09-16.pl - Sending Email Using SMTP Server  
Example: ex09-17.htm - Sending Public-Key Encrypted Email With Perl  
ex09-17.pl - Sending Encrypted Email Using GnuPG and Perl  
Example: ex09-18.htm - Sending Encrypted Email  
ex09-18.php - PHP Script For Page ex09-18.htm  
Example: ex09-19.htm - Email With MIME Type  
ex09-19.pl - The Perl Script For ex09-19.htm  
Example: ex09-20.php - A PHP Program For ex09-20.htm  
ex09-20.inc - An Include File For ex09-20.php

---

**Chapter 10      SSL Security, Applications, and XML Contracts**

Example: ex10-01.ssl - Testing The OpenSSL Package  
Example: ex10-02.ssl - The Command Summary Of OpenSSL  
Example: ex10-03.ssl - Using Message Digest With OpenSSL  
Example: ex10-04.htm - Encryption/Decryption With OpenSSL  
          ex10-04.pl - Perl Script For ex10-04.htm  
Example: ex10-05.ssl - Generate RSA Private Key Using OpenSSL  
Example: ex10-06.ssl - Generate A Certificate Signing Request  
Example: ex10-07.ssl - Signing CSR With Your Own Private Key  
Example: ex10-08.ssl - Generating CA's Certificate and Private Key  
Example: ex10-09.ssl - Signing Certificate With Your Own CA  
Example: ex10-10.ssl - The Default X509 Certificate Format  
Example: ex10-11.ssl - Creating PKCS#12 Certificates  
Example: ex10-12.ssl - Integrating Apache and OpenSSL with Mod\_SSL  
Example: ex10-13.ssl - Configure and build the OpenSSL package  
Example: ex10-14.ssl - Configure Mod\_SSL for Apache  
Example: ex10-15.ssl - Building the SSL-aware Apache  
Example: ex10-16.ssl - Testing Apache - apache -h  
Example: ex10-17.ssl - Generating a Certificate for Apache server  
Example: ex10-18.ssl - Setting Configuration  
Example: ex10-19.ssl - Virtual Host Listens to Port 443  
Example: ex10-20.htm - A Page To Get Donation For Charity  
Example: ex10-21.htm - A Simple Page To Accept Donation  
Example: ex10-22.xml - My First XML Page  
Example: ex10-23.xml - XML Page With Simple XSLT Transformation  
Example: ex10-23.xsl - The XSLT Transformation File For ex10-23.xml  
Example: ex10-24.xml - XML Data For ex10-24.xsl  
Example: ex10-24.xsl - The XSLT Transformation Generating Loops  
Example: ex10-25.xml - XML Data For ex10-25.xsl  
Example: ex10-25.xsl - The XSLT Transformation with choose  
Example: ex10-26.xml - XML Data For ex10-26.htm  
Example: ex10-26.htm - Accessing XML Element With Parser  
Example: ex10-27.txt - The Help Screen of XMLSEC Library  
Example: ex10-28.xml - Input XML Page For XML Encryption  
Example: ex10-28\_tp.xml - A Simple XML Encryption Template  
Example: ex10-28\_enc.xml - The Encrypted XML Page  
Example: ex10-28.xsl - The XSLT For ex10-28.xml and ex10-28\_enc.xml  
Example: ex10-29\_tp.xml - A Simple XML Template For XML Signature  
Example: ex10-29\_signed.xml - A Simple Signed XML Page  
Example: ex10-30\_tp.xml - The XML Digital Contract <Data> Element  
Example: ex10-30.xml - Displaying XML Contract Using Parser  
Example: ex10-31.htm - XML Digital Contract With X509 Certificate