

Preface

This book is about practical cryptology and security skills on the World Wide Web (Web), providing an instant course and a reference guide for university students, Web designers, young programmers and industry professionals to apply cryptographic techniques directly to applications. There is no encryption/decryption background assumed. By keeping the abstract theory and mathematics of cryptology to a minimum, students or readers with basic level of mathematics and some knowledge of HTML design or programming should be able to finish the book smoothly.

All major encryption algorithms (or ciphers) are systematically covered and implemented with Web technologies and Web pages including:

- One-Way ciphers: UNIX Crypt, MD5, MD5Crypt, and SHA
- Block ciphers: DES, Tri-DES, CAST128, Blowfish, RC6 and AES
- Stream ciphers: OTP, RC4, ISAAC, SEAL2
- Public-key ciphers: Diffie-Hellman, ElGamal, RSA, and Elliptic Curves

In some cases, coding optimization is also discussed and illustrated with examples. Studying the coding optimization of algorithms such as DES and AES imparts better knowledge of the structure of algorithm and takes the reader one step closer to professional implementations and algorithmic designs.

The subject of cryptology relates to attacks as well as encryption/decryption. Crypto-attacks such as Brute-Force (Try-Them-All) are also introduced and implemented in early chapter of the book (Chapter 2), so that security risk can be assessed in terms of the time and computational resources needed to crack a cryptographic system.

The contents and materials of each chapter are application oriented covering some of the main objectives of cryptology such as message confidentiality, authentication, data Integrity, and non-repudiation. From message encryption/decryption, password schemes, HTTP authentications, digital signatures, certificates, secure emails to SSL security, HTTPS secure Web sites, and digital contracts (XML digital contracts), over 120 fully working examples are provided; many of them are projects from industries forming a complete series of security applications on the Internet and World Wide Web.

All examples are presented in cut-and-Paste format which can be reused in your applications. Together with more than 300 illustrations and screenshots, both cryptographic encryption / decryption skills and security on the Web are demonstrated step by step.