PK Yuen

Practical Cryptology and Web Security

ADDISON
WESLEY

Practical Cryptology and Web Security

Visit the *Practical Cryptology and Web Security* Companion Website at **www.pearsoned.co.uk/yuen** to find valuable **student** learning material including:

- Sample contents
- Source code for program examples from each chapter

Practical Cryptology and Web Security

Table of Contents

Cover

Practical Cryptology and Web Security

Contents

Preface

Acknowledgements

Basic security skills on the World Wide Web

- An introduction to network security
- The Web browserserver dialog
- Web page skills for message manipulation and security
- Bitwise operators and Base64 encoding/decoding
- The XOR and PkZip/WinZip encryption schemes

Cryptology, Web site protection and attacks

- An overview of cryptology
- Basic user authentication and Web site protection
- Digest user authentication
- Brute-force attacks
- Implementation and application of brute-force schemes

One-way encryptions, hashfunctions and message digests

- One-way functions and encryptions
- The single DES scheme and my first one-way encryption: Crypt()
- Hash functions and the message digest: MD5
- Applications of message digests and the md5Crypt password scheme

Pearson

Table of Contents

The secure hash algorithm

Some strong symmetric-key ciphers

An introduction to strong symmetric-key ciphers

Coding optimization of the DES scheme

Optimized DES, triple DES and some encryption tools

A DES-like cipher: CAST-128

Encryption/decryption tools with CAST-128

Practical software-basedstream ciphers

An introduction to stream ciphers

An unbreakable cipher: the one-time-pad

Techniques for generating random key-streams

Two fast and compact stream ciphers: RC4 and ISAAC

A heavyweight stream cipher: SEAL2

Block ciphers with variable key lengths

A flexible and adaptive block cipher: Blowfish

Implementation of the Blowfish scheme

A fully parameterized block cipher: RC6

A step-by-step advanced encryption standard

An optimized implementation of AES

Encryption and server skills for Web page protection

Encryption skills for Web page protection

Server technologies and security

Using server storage for security

Handling password accounts with MySQL

Practical public-key security and digital signatures

Security with public-key technology

Table of Contents

The DiffieHellman key exchange scheme

The ElGamal public-key algorithm and digital signatures

The RSA scheme, digital signature and hybrid encryption

Elliptic curves and public-key encryption/decryption

Security applications with GnuPG, WinPT and server techniques

An introduction to Gnu Privacy Guard

Using GnuPG for security applications

A graphical GnuPG interface for Windows: WinPT

Secure emailing with server technologies

Sending secure attachments with server technologies

SSL security, applications and XML contracts

Digital certificates and contracts

Basic security applications with OpenSSL

Generating and signing certificates with OpenSSL

Integrating OpenSSL and Apache to build a secure HTTPS site

XML security and XML digital contracts

Glossary

Index