Preface ix

1. Introduction 1
Cryptography for the Rest of Us 2
Overview of SSL 10
Problems with SSL 12
What SSL Doesn't Do Well 20
OpenSSL Basics 21
Securing Third-Party Software 23

2. Command-Line Interface 29
The Basics 30
Message Digest Algorithms 32
Symmetric Ciphers 34
Public Key Cryptography 35
S/MIME 40
Passwords and Passphrases 42
Seeding the Pseudorandom Number Generator 43

3. Public Key Infrastructure (PKI) 45
Certificates 46
Obtaining a Certificate 55
Setting Up a Certification Authority 59

4. Support Infrastructure 74
Multithread Support 74
Internal Error Handling 81
Abstract Input/Output 86
Random Number Generation 97

Arbitrary Precision Math 103
Using Engines 109

5. SSL/TLS Programming 112
Programming with SSL 113
Advanced Programming with SSL 150

6. Symmetric Cryptography 171
Concepts in Symmetric Cryptography 171
Encrypting with the EVP API 174
General Recommendations 192

7. Hashes and MACs 193
Overview of Hashes and MACs 193
Hashing with the EVP API 195
Using MACs 200
Secure HTTP Cookies 212

8. Public Key Algorithms 217
When to Use Public Key Cryptography 218
Diffie-Hellman 219
Digital Signature Algorithm (DSA) 225
RSA 230
The EVP Public Key Interface 236
Encoding and Decoding Objects 244

9. OpenSSL in Other Languages 251
Net::SSLeay for Perl 251
M2Crypto for Python 258
OpenSSL Support in PHP 266

10. Advanced Programming Topics 275
Object Stacks 275
Configuration Files 277
X.509 280
PKCS#7 and S/MIME 296
PKCS#12 307

Appendix: Command-Line Reference 309

Index 353