Chapter 6 *Data Encryption Standard (DES)* *159*

6.1 INTRODUCTION 159
History 159
Overview 160
6.2 DES STRUCTURE 160
Initial and Final Permutations 160
Rounds 163
Cipher and Reverse Cipher 167
Examples 173
6.3 DES ANALYSIS 175
Properties 175
Design Criteria 176
DES Weaknesses 177
6.4 MULTIPLE DES 181
Double DES 182
Triple DES 184
6.5 SECURITY OF DES 185
Brute-Force Attack 185
Differential Cryptanalysis 185
Linear Cryptanalysis 186
6.6 RECOMMENDED READING 186
Books 186
WebSites 186
6.7 KEY TERMS 186
6.8 SUMMARY 187
6.9 PRACTICE SET 187
Review Questions 187
Exercises 188

Chapter 7 *Advanced Encryption Standard (AES)* *191*

7.1 INTRODUCTION 191
History 191
Criteria 192
Rounds 192
Data Units 193
Structure of Each Round 195
7.2 TRANSFORMATIONS 196
Substitution 196
Permutation 202
Mixing 203
Key Adding 206
7.3 KEY EXPANSION 207
Key Expansion in AES-128 208
Key Expansion in AES-192 and AES-256 212
Key-Expansion Analysis 212
7.4 CIPHERS 213
Original Design 213
Alternative Design 214

7.5 EXAMPLES 216
7.6 ANALYSIS OF AES 219
Security 219
Implementation 219
Simplicity and Cost 220
7.7 RECOMMENDED READING 220
Books 220
WebSites 220
7.8 KEY TERMS 220
7.9 SUMMARY 220
7.10 PRACTICE SET 221
Review Questions 221
Exercises 222

Chapter 8 *Encipherment Using Modern Symmetric-Key Ciphers 225*

8.1 USE OF MODERN BLOCK CIPHERS 225
Electronic Codebook (ECB) Mode 226
Cipher Block Chaining (CBC) Mode 228
Cipher Feedback (CFB) Mode 231
Output Feedback (OFB) Mode 234
Counter (CTR) Mode 236
8.2 USE OF STREAM CIPHERS 238
RC4 238
A5/1 242
8.3 OTHER ISSUES 244
Key Management 244
Key Generation 244
8.4 RECOMMENDED READING 245
Books 245
WebSites 245
8.5 KEY TERMS 245
8.6 SUMMARY 245
8.7 PRACTICE SET 246
Review Questions 246
Exercises 247

Part 2 *Asymmetric-Key Encipherment 249*

Chapter 9 *Mathematics of Cryptography 251*

9.1 PRIMES 251
Definition 251
Cardinality of Primes 252
Checking for Primeness 253
Euler's Phi-Function 254
Fermat's Little Theorem 256
Euler's Theorem 257
Generating Primes 258

→ U 3

→ U 4

9.2 PRIMALITY TESTING 260
Deterministic Algorithms 260
Probabilistic Algorithms 261
Recommended Primality Test 266
9.3 FACTORIZATION 267
Fundamental Theorem of Arithmetic 267
Factorization Methods 268
Fermat Method 269
Pollard $p-1$ Method 270
Pollard rho Method 271
More Efficient Methods 272
9.4 CHINESE REMAINDER THEOREM 274
Applications 275
9.5 QUADRATIC CONGRUENCE 276
Quadratic Congruence Modulo a Prime 276
Quadratic Congruence Modulo a Composite 277
9.6 EXPONENTIATION AND LOGARITHM 278
Exponentiation 279
Logarithm 281
9.7 RECOMMENDED READING 286
Books 286
WebSites 286
9.8 KEY TERMS 286
9.9 SUMMARY 287
9.10 PRACTICE SET 288
Review Questions 288
Exercises 288

Chapter 10 *Asymmetric-Key Cryptography* *293*

10.1 INTRODUCTION 293
Keys 294
General Idea 294
Need for Both 296
Trapdoor One-Way Function 296
Knapsack Cryptosystem 298
10.2 RSA CRYPTOSYSTEM 301 ✓
Introduction 301
Procedure 301
Some Trivial Examples 304
Attacks on RSA 305
Recommendations 310
Optimal Asymmetric Encryption Padding (OAEP) 311
Applications 314
10.3 RABIN CRYPTOSYSTEM 314
Procedure 315
Security of the Rabin System 317
10.4 ELGAMAL CRYPTOSYSTEM 317 ✓
ElGamal Cryptosystem 317
Procedure 317

Proof 319
Analysis 319
Security of ElGamal 320
Application 321
10.5 ELLIPTIC CURVE CRYPTOSYSTEMS 321
Elliptic Curves over Real Numbers 321
Elliptic Curves over GF(p) 324
Elliptic Curves over GF(2^n) 326
Elliptic Curve Cryptography Simulating ElGamal 328
10.6 RECOMMENDED READING 330
Books 330
WebSites 330
10.7 KEY TERMS 331
10.8 SUMMARY 331
10.9 PRACTICE SET 333
Review Questions 333
Exercises 334

end [illegible]

Part 3 *Integrity, Authentication, and Key Management* 337

Chapter 11 *Message Integrity and Message Authentication* 339

11.1 MESSAGE INTEGRITY 339
Document and Fingerprint 340
Message and Message Digest 340
Difference 340
Checking Integrity 340
Cryptographic Hash Function Criteria 340
11.2 RANDOM ORACLE MODEL 343
Pigeonhole Principle 345
Birthday Problems 345
Attacks on Random Oracle Model 347
Attacks on the Structure 351
11.3 MESSAGE AUTHENTICATION 352
Modification Detection Code 352
Message Authentication Code (MAC) 353
11.4 RECOMMENDED READING 357
Books 357
WebSites 357
11.5 KEY TERMS 357
11.6 SUMMARY 358
11.7 PRACTICE SET 358
Review Questions 358
Exercises 359

Chapter 12 *Cryptographic Hash Functions* 363

12.1 INTRODUCTION 363
Iterated Hash Function 363
Two Groups of Compression Functions 364

12.2 SHA-512 367
Introduction 367
Compression Function 372
Analysis 375
12.3 WHIRLPOOL 376
Whirlpool Cipher 377
Summary 384
Analysis 384
12.4 RECOMMENDED READING 384
Books 384
WebSites 384
12.5 KEY TERMS 385
12.6 SUMMARY 385
12.7 PRACTICE SET 386
Review Questions 386
Exercises 386

Chapter 13 *Digital Signature 389*

13.1 COMPARISON 390
Inclusion 390
Verification Method 390
Relationship 390
Duplicity 390
13.2 PROCESS 390
Need for Keys 391
Signing the Digest 392
13.3 SERVICES 393
Message Authentication 393
Message Integrity 393
Nonrepudiation 393
Confidentiality 394
13.4 ATTACKS ON DIGITAL SIGNATURE 395
Attack Types 395
Forgery Types 395
13.5 DIGITAL SIGNATURE SCHEMES 396
RSA Digital Signature Scheme 396
ElGamal Digital Signature Scheme 400
Schnorr Digital Signature Scheme 403
Digital Signature Standard (DSS) 405
Elliptic Curve Digital Signature Scheme 407
13.6 VARIATIONS AND APPLICATIONS 409
Variations 409
Applications 411
13.7 RECOMMENDED READING 411
Books 411
WebSites 411
13.8 KEY TERMS 412

→ SLE
end of U4

13.9 SUMMARY 412
13.10 PRACTICE SET 413
Review Questions 413
Exercises 413

Chapter 14 *Entity Authentication* *415*

14.1 INTRODUCTION 415
Data-Origin Versus Entity Authentication 415
Verification Categories 416
Entity Authentication and Key Management 416
14.2 PASSWORDS 416
Fixed Password 416
One-Time Password 419
14.3 CHALLENGE-RESPONSE 421
Using a Symmetric-Key Cipher 421
Using Keyed-Hash Functions 423
Using an Asymmetric-Key Cipher 424
Using Digital Signature 425
14.4 ZERO-KNOWLEDGE 426
Fiat-Shamir Protocol 427
Feige-Fiat-Shamir Protocol 429
Guillou-Quisquater Protocol 429
14.5 BIOMETRICS 430
Components 431
Enrollment 431
Authentication 431
Techniques 432
Accuracy 433
Applications 434
14.6 RECOMMENDED READING 434
Books 434
WebSites 434
14.7 KEY TERMS 434
14.8 SUMMARY 435
14.9 PRACTICE SET 435
Review Questions 435
Exercises 436

Chapter 15 *Key Management* *437*

15.1 SYMMETRIC-KEY DISTRIBUTION 438
Key-Distribution Center: KDC 438
Session Keys 439
15.2 KERBEROS 443
Servers 444
Operation 445
Using Different Servers 445
Kerberos Version 5 447
Realms 447

15.3 SYMMETRIC-KEY AGREEMENT 447
Diffie-Hellman Key Agreement 447
Station-to-Station Key Agreement 451
15.4 PUBLIC-KEY DISTRIBUTION 453
Public Announcement 453
Trusted Center 453
Controlled Trusted Center 454
Certification Authority 454
X.509 456
Public-Key Infrastructures (PKI) 458
15.5 RECOMMENDED READING 461
Books 461
WebSites 461
15.6 KEY TERMS AND CONCEPTS 462
15.7 SUMMARY 462
15.8 PRACTICE SET 463
Review Questions 463
Exercises 463

Part 4 *Network Security* *465*

Chapter 16 *Security at the Application Layer: PGP and S/MIME* *467*

16.1 E-MAIL 467
E-mail Architecture 467
E-mail Security 469
16.2 PGP 470
Scenarios 470
Key Rings 472
PGP Certificates 475
Key Revocation 482
Extracting Information from Rings 482
PGP Packets 484
PGP Messages 490
Applications of PGP 492
16.3 S/MIME 492
MIME 492
S/MIME 498
Applications of S/MIME 502
16.4 RECOMMENDED READING 502
Books 502
WebSites 502
16.5 KEY TERMS 502
16.6 SUMMARY 503
16.7 EXERCISES 503
Review Questions 503
Exercises 504

Chapter 17 *Security at the Transport Layer: SSL and TLS 507*

17.1 SSL ARCHITECTURE 508
Services 508
Key Exchange Algorithms 509
Encryption/Decryption Algorithms 511
Hash Algorithms 512
Cipher Suite 512
Compression Algorithms 513
Cryptographic Parameter Generation 513
Sessions and Connections 515
17.2 FOUR PROTOCOLS 517
Handshake Protocol 518
ChangeCipherSpec Protocol 525
Alert Protocol 526
Record Protocol 526
17.3 SSL MESSAGE FORMATS 529
ChangeCipherSpec Protocol 530
Alert Protocol 530
Handshake Protocol 530
Application Data 537
17.4 TRANSPORT LAYER SECURITY 538
Version 539
Cipher Suite 539
Generation of Cryptographic Secrets 539
Alert Protocol 542
Handshake Protocol 543
Record Protocol 543
17.5 RECOMMENDED READING 545
Books 545
WebSites 545
17.6 KEY TERMS 545
17.7 SUMMARY 545
17.8 PRACTICE SET 546
Review Questions 546
Exercises 546

Chapter 18 *Security at the Network Layer: IPSec 549*

18.1 TWO MODES 550
Comparison 552
18.2 TWO SECURITY PROTOCOLS 552
Authentication Header (AH) 552
Encapsulating Security Payload (ESP) 554
IPv4 and IPv6 555
AH versus ESP 555
Services Provided by IPSec 555
18.3 SECURITY ASSOCIATION 557
Idea of Security Association 557
Security Association Database (SAD) 558

18.4 SECURITY POLICY 560
Security Policy Database 560
18.5 INTERNET KEY EXCHANGE (IKE) 563
Improved Diffie-Hellman Key Exchange 563
IKE Phases 566
Phases and Modes 566
Phase I: Main Mode 567
Phase I: Aggressive Mode - 573
Phase II: Quick Mode 575
SA Algorithms 577
18.6 ISAKMP 578
General Header 578
Payloads 579
18.7 RECOMMENDED READING 588
Books 588
WebSites 588
18.8 KEY TERMS 588
18.9 SUMMARY 589
18.10 PRACTICE SET 589
Review Questions 589
Exercises 590

Appendix A *ASCII 593*

Appendix B *Standards and Standard Organizations 595*

B.1 INTERNET STANDARDS 595
Maturity Levels 595
Requirement Levels 597
Internet Administration 597
B.2 OTHER STANDARD ORGANIZATIONS 599
NIST 599
ISO 599
ITU-T 599
ANSI 600
IEEE 600
EIA 600

Appendix C *TCP/IP Protocol Suite 601*

C.1 LAYERS IN THE TCP/IP 602
Application Layer 602
Transport Layer 602
Network Layer 603
Data Link Layer 604
Physical Layer 604
C.2 ADDRESSING 604
Specific Address 604
Port Address 604
Logical Address 605
Physical Address 605

Appendix D *Elementary Probability 607*

D.1 INTRODUCTION 607
Definitions 607
Probability Assignment 608
Axioms 609
Properties 609
Conditional Probability 609
D.2 RANDOM VARIABLES 610
Continuous Random Variables 610
Discrete Random Variables 610

Appendix E *Birthday Problems 611*

E.1 FOUR PROBLEMS 611
First Problem 611
Second Problem 612
Third Problem 612
Fourth Problem 613
E.2 SUMMARY 614

Appendix F *Information Theory 615*

F.1 MEASURING INFORMATION 615
F.2 ENTROPY 616
Maximum Entropy 616
Minimum Entropy 617
Interpretation of Entropy 617
Joint Entropy 617
Conditional Entropy 617
Other Relations 618
Perfect Secrecy 618
F.3 ENTROPY OF A LANGUAGE 619
Entropy of an Arbitrary Language 619
Entropy of the English Language 619
Redundancy 619
Unicity Distance 620

Appendix G *List of Irreducible and Primitive Polynomials 621*

Appendix H *Primes Less Than 10,000 623*

Appendix I *Prime Factors of Integers Less Than 1000 627*

Appendix J *List of First Primitive Roots for Primes Less Than 1000 631*

Appendix K *Random Number Generator 633*

K.1 TRNG 633