はじめに …… 003

この本について …… 009

第1部 プリミティブ：暗号の構成要素 …… 027

第1章 暗号とは何か …… 028

1.1 暗号の要（かなめ）、プロトコルの保護ということ …… 029
1.2 対称暗号：対称暗号化とは何か …… 030
1.3 ケルクホフスの原理：秘匿されるのは鍵だけ …… 033
1.4 非対称暗号：鍵は1つより2つ …… 036
1.4.1 鍵交換：共有の秘密を使う …… 037
1.4.2 非対称暗号化と対称暗号化の違い …… 041
1.4.3 デジタル署名：紙とペンを使う署名にかわるもの …… 043
1.5 暗号の分類と抽象化 …… 045
1.6 理論暗号学と現実世界の暗号学 …… 048
1.7 理論から実践へ：「きみならどうする」 …… 049
1.8 戒めの言葉をひとつ …… 055
この章のまとめ …… 056

第2章 ハッシュ関数 …… 058

2.1 ハッシュ関数とは何か …… 058
2.2 ハッシュ関数のセキュリティ特性 …… 062
2.3 ハッシュ関数のセキュリティに関する考察 …… 065
2.4 現実世界でのハッシュ関数 …… 067
2.4.1 コミットメント …… 067

2.4.2 サブリソース完全性 …… 068
2.4.3 BitTorrent …… 069
2.4.4 Tor …… 069
2.5 標準化されたハッシュ関数 …… 070
2.5.1 SHA-2 ハッシュ関数 …… 072
2.5.2 SHA-3 ハッシュ関数 …… 076
2.5.3 SHAKE と cSHAKE：2 つの可変長出力関数（XOF） …… 081
2.5.4 TupleHash によるハッシュで曖昧さを回避する …… 083
2.6 パスワードのハッシュ …… 085
この章のまとめ …… 088

16 進法について …… 060
ランダムオラクル …… 064
誕生日限界 …… 066
演習 …… 068
演習 …… 070
標準の廃止は難しい …… 071
排他的論理和の演算 …… 073
SHA-3 はランダムオラクル …… 081

第 3 章 メッセージ認証コード …… 089
3.1 ステートレス Cookie、MAC の導入となる例 …… 089
3.2 コードで見る実際の例 …… 093
3.3 MAC のセキュリティ特性 …… 095
3.3.1 認証タグの捏造 …… 095
3.3.2 認証タグの長さ …… 096
3.3.3 リプレイ攻撃 …… 097
3.3.4 一定時間で認証タグを検証する …… 099
3.4 現実世界での MAC …… 101
3.4.1 メッセージの認証 …… 101
3.4.2 鍵の導出 …… 101

3.4.3 Cookie の完全性 …… 102
3.4.4 ハッシュテーブル …… 102
3.5 メッセージ認証コード（MAC）の実際 …… 102
3.5.1 HMAC：ハッシュベースの MAC …… 103
3.5.2 KMAC：cSHAKE ベースの MAC …… 104
3.6 SHA-2 と伸長攻撃 …… 105
この章のまとめ …… 108

演習 …… 099
擬似乱数関数（PRF） …… 101
演習 …… 102

第 4 章 認証付き暗号 …… 110
4.1 暗号化アルゴリズムとは何か …… 110
4.2 AES ブロック暗号 …… 113
4.2.1 AES のセキュリティレベル …… 113
4.2.2 AES のインターフェース …… 114
4.2.3 AES の内部機構 …… 115
4.3 ペンギンの暗号化と、CBD モード …… 118
4.4 真正性の欠如、そこから生まれた AES-CBC-HMAC …… 122
4.5 一体型の構成法：認証付き暗号 …… 124
4.5.1 認証付き暗号（AEAD）とは何か …… 124
4.5.2 AES-GCM …… 126
4.5.3 ChaCha20-Poly1305 …… 131
4.6 その他の対称暗号 …… 136
4.6.1 鍵ラッピング …… 137
4.6.2 ノンス悪用に耐性の高い認証付き暗号 …… 137
4.6.3 ディスク暗号化 …… 138
4.6.4 データベース暗号化 …… 138
この章のまとめ …… 139

ビットセキュリティは上限 …… 113

ストリーム暗号 …… 128
誕生日限界を超えるセキュリティ …… 131
ノンスとカウンターのサイズ …… 133

第5章 鍵交換 …… 141

5.1 鍵交換とは何か …… 141
5.2 ディフィー・ヘルマン（DH）鍵交換 …… 145
5.2.1 群論 …… 146
5.2.2 離散対数問題：ディフィー・ヘルマンの基礎 …… 151
5.2.3 ディフィー・ヘルマンを利用している標準 …… 154
5.3 楕円曲線ディフィー・ヘルマン（ECDH）鍵交換 …… 156
5.3.1 楕円曲線とは何か …… 156
5.3.2 楕円曲線ディフィー・ヘルマン（ECDH）鍵交換のしくみ …… 161
5.3.3 楕円曲線ディフィー・ヘルマンの標準 …… 163
5.4 小部分群攻撃などのセキュリティ上の問題 …… 166
この章のまとめ …… 169

素数とは …… 147
計算的ディフィー・ヘルマンと決定的ディフィー・ヘルマン …… 153
P-256 は信頼できるか …… 165

第6章 非対称暗号とハイブリッド暗号 …… 171

6.1 非対称暗号とは何か …… 171
6.2 非対称暗号の実際と、ハイブリッド暗号 …… 174
6.2.1 鍵交換と鍵カプセル化 …… 174
6.2.2 ハイブリッド暗号 …… 176
6.3 RSA による非対称暗号化：弱点とその緩和 …… 181
6.3.1 教科書どおりの RSA …… 181
6.3.2 RSA PKCS#1 v1.5 を避けるべき理由 …… 187
6.3.3 RSA-OAEP による非対称暗号化 …… 189
6.4 ECIES を使用するハイブリッド暗号 …… 193

この章のまとめ …… 196

演習 …… 172
オイラーの定理 …… 184
RSA 群の位数 …… 185
適応的選択暗号文攻撃 …… 188
メインジャーのパディングオラクル攻撃 …… 192
鍵交換の出力で偏りを排除する …… 195
演習 …… 195

第 7 章 署名とゼロ知識証明 …… 197

7.1 署名とは何か …… 197
7.1.1 署名とその検証の実際 …… 199
7.1.2 署名の主な用途：認証付き鍵交換 …… 200
7.1.3 現実世界での使い方：公開鍵基盤 …… 202
7.2 ゼロ知識証明（ZKP）：署名の出どころ …… 203
7.2.1 シュノア識別プロトコル：対話型のゼロ知識証明 …… 204
7.2.2 非対話型ゼロ知識証明としての署名 …… 209
7.3 推奨される署名と非推奨の署名 …… 210
7.3.1 RSA PKCS#1 v1.5—おすすめできない標準 …… 212
7.3.2 RSA-PSS：向上した標準 …… 215
7.3.3 楕円曲線デジタル署名アルゴリズム（ECDSA） …… 217
7.3.4 エドワーズ曲線デジタル署名アルゴリズム（EdDSA） …… 221
7.4 署名方式の微妙で複雑な挙動 …… 225
7.4.1 署名に対する置換攻撃 …… 226
7.4.2 署名のトランザクション展性 …… 227
この章のまとめ …… 228

演習 …… 199
「RSA」が多すぎる …… 214
PSS の証明可能な安全性 …… 216
乗法と加法のどちらの記法を使うか …… 218

適応的選択平文攻撃における存在的偽造不可能性（EUF-CMA） …… 226
強力な EUF-CMA …… 228

第 8 章 ランダム性と秘密 …… 230

8.1 ランダム性とは …… 230
8.2 乱数の生成は遅いため、擬似乱数生成器（PRNG）を使う …… 234
8.3 ランダム性を取得する実際の手法 …… 238
8.4 ランダム性の生成とセキュリティの関係 …… 241
8.5 公開のランダム性 …… 245
8.6 HKDF による鍵導出 …… 248
8.7 鍵と秘密の管理 …… 253
8.8 しきい値暗号による信頼の分散 …… 254
この章のまとめ …… 258

エントロピー …… 233
デュアル EC のバックドア問題 …… 237
RDRAND をめぐる議論 …… 245
演習 …… 245
演習 …… 247
関数が本当にランダムな出力を生成するかどうかの見極め …… 252

第 2 部 プロトコル：暗号を使うレシピ …… 261

第 9 章 セキュアトランスポート …… 262

9.1 セキュアトランスポートプロトコル：SSL と TLS …… 262
9.1.1 SSL から TLS へ …… 264
9.1.2 実際に TLS を使う …… 264
9.2 TLS プロトコルのしくみ …… 267
9.2.1 TLS ハンドシェイク …… 268
9.2.2 TLS 1.3 でアプリケーションデータを暗号化するしくみ …… 286
9.3 ウェブ暗号化の現状 …… 287
9.4 その他のセキュアトランスポートプロトコル …… 291
9.5 Noise プロトコルフレームワーク：TLS にかわる最新の技術 …… 292
9.5.1 Noise にはハンドシェイクが多い …… 293
9.5.2 Noise によるハンドシェイク …… 294
この章のまとめ …… 296

バージョンの古い SSL と TLS は安全か …… 270
演習 …… 274
TLS 相互認証 …… 276
Web PKI について …… 277
エピソードを紹介 …… 280
演習 …… 282
クライアントランダムとサーバーランダム …… 285
平文の長さを隠す …… 286

第 10 章 エンドツーエンド暗号化 …… 298

10.1 なぜエンドツーエンド暗号化なのか …… 299
10.2 本来はどこにもない、「信頼の基点」 …… 301
10.3 暗号化されたメールの限界 …… 303
10.3.1 GPG か PGP か、そのしくみは？ …… 304

10.3.2 URL ユーザー間の信頼を広げる「信頼の輪」…… 307
10.3.3 鍵の検出 …… 309
10.3.4 PGP がだめなら、代替の候補は？ …… 311
10.4 セキュアメッセージング：
Signal に見る、エンドツーエンド暗号化の最新の形 …… 313
10.4.1 WOT よりユーザーフレンドリーなしくみ：
信頼するが検証する …… 315
10.4.2 X3DH：Signal プロトコルにおけるハンドシェイク …… 318
10.4.3 ダブルラチェット：
Signal で使われるポストハンドシェイクプロトコル …… 322
10.5 エンドツーエンド暗号化の現状 …… 327
この章のまとめ …… 330

演習 …… 305
演習 …… 306

第 11 章 ユーザー認証 …… 332

11.1 認証を要約すると …… 332
11.2 ユーザー認証、あるいはパスワードの排除をめざす探究 …… 334
11.2.1 ひとつのパスワードが、すべてを統べる：
シングルサインオン（SSO）とパスワードマネージャー …… 338
11.2.2 パスワードをさらしたくない場合は、
非対称パスワード認証鍵交換を使う …… 340
11.2.3 ワンタイムパスワードはパスワードではない：
対称鍵でパスワードレスを実現する …… 345
11.2.4 非対称鍵でパスワードを置き換える …… 349
11.3 ユーザー補助型認証：
人間を仲立ちにしてデバイスをペアリングする …… 353
11.3.1 事前共有鍵 …… 356
11.3.2 CPace による対称パスワード認証鍵交換 …… 358
11.3.3 鍵交換が MITM 攻撃を受けたかどうか ―
短い認証文字列（SAS）でチェック …… 359
この章のまとめ …… 363

演習 …… 336
フィッシング …… 349
演習 …… 354
エピソードを紹介 …… 362

第 12 章 暗号が通貨になる? …… 365

12.1 ビザンチン障害耐性（BFT）コンセンサスアルゴリズムの簡単な導入 …… 366
12.1.1 回復性の問題：解決策は分散プロトコル …… 367
12.1.2 信頼の問題に対処する分散化 …… 369
12.1.3 拡張性の問題：パーミッションレスで検閲耐性を備えたネットワーク …… 371
12.1 ビットコインのしくみ …… 374
12.2.1 ビットコインはユーザーの残高とトランザクションをどう処理しているか …… 374
12.2.2 デジタルの黄金時代に出現した BTC の採掘 …… 377
12.2.3 フォークの問題：マイニングにおける競合を解決する …… 382
12.2.4 マークルツリーでブロックを小さくする …… 386
12.3 暗号通貨の諸問題 …… 388
12.3.1 ボラティリティ（流動性）…… 388
12.3.2 レイテンシー …… 389
12.3.3 ブロックチェーンの大きさ …… 389
12.3.4 機密性 …… 390
12.3.5 エネルギー消費の問題 …… 390
12.4 DiemBFT：ビザンチン障害耐性（BFT）コンセンサスプロトコル …… 391
12.4.1 安全性とライブネス：BFT コンセンサスプロトコルの 2 つの特性 …… 392
12.4.2 DiemBFT プロトコルにおけるラウンド …… 393
12.4.3 DiemBFT はどの程度までの不正に耐性があるのか …… 394
12.4.4 DiemBFT の投票ルール …… 395
12.4.5 トランザクションはいつファイナライズされるか …… 396

12.4.6 DiemBFT の安全性を直観的にとらえる …… 397
この章のまとめ …… 399

第 13 章 ハードウェア暗号 …… 402

13.1 最新の暗号学的攻撃モデル …… 402
13.2 信頼できない環境：救いの手はハードウェア …… 404
13.2.1 ホワイトボックス暗号 ― 賢いとはいえない発想 …… 405
13.2.2 皆さんの財布にもある：スマートカードとセキュアエレメント …… 406
13.2.3 銀行が好むハードウェアセキュリティモジュール（HSM） …… 410
13.2.4 トラステッドプラットフォームモジュール（TPM）：セキュアエレメントの実効的な標準化 …… 413
13.2.5 信頼できる実行環境（TEE）による機密コンピューティング …… 418
13.3 どのソリューションが適しているか …… 420
13.4 漏洩耐性のある暗号：ソフトウェアでサイドチャネル攻撃を低減するには …… 422
13.4.1 一定時間のプログラミング …… 425
13.4.2 秘密を使わない！ マスキングとブラインド …… 427
13.4.3 フォールト攻撃はどうか …… 429
この章のまとめ …… 430

悪意あるメイド攻撃 …… 405
銀行とレガシー暗号 …… 408

第 14 章 耐量子暗号 …… 432

14.1 量子コンピューターとは何か、暗号学者を脅かしているのはなぜか …… 433
14.1.1 極小の世界を研究する量子力学 …… 433
14.1.2 量子コンピューターの誕生から量子超越性まで …… 437
14.1.3 グローバーとショアのアルゴリズムが暗号学にもたらす影響 …… 439
14.1.4 量子コンピューターへの対抗手段、耐量子暗号 …… 441

14.2　ハッシュベースの署名：必要なのはハッシュ関数だけ …… 442
14.2.1　ランポート署名を用いるワンタイム署名（OTS） …… 442
14.2.2　鍵が小さくなる、ヴィンターニッツのワンタイム署名（WOTS） …… 444
14.2.3　XMSS と SPHINCS+ による多数回署名 …… 446
14.3　鍵と署名が短くなる、格子暗号 …… 450
14.3.1　格子とは何か …… 451
14.3.2　LWE（誤差を伴う学習）は暗号の基礎になりうるか …… 453
14.3.3　Kyber：格子ベースの鍵交換 …… 455
14.3.4　Dilithium：格子ベースの署名方式 …… 458
14.4　パニクる必要はあるか …… 460
この章のまとめ …… 462

第 15 章　次世代の暗号技術 …… 465
15.1　大勢のほうが楽しい：セキュアマルチパーティ計算（MPC） …… 466
15.1.1　プライベートセット交差（PSI） …… 467
15.1.2　汎用 MPC …… 469
15.1.3　MPC の現状 …… 471
15.2　完全準同型暗号（FHE）と、クラウドでの暗号の将来性 …… 472
15.2.1　RSA 暗号に見る準同型暗号の例 …… 472
15.2.2　さまざまな準同型暗号 …… 473
15.2.3　完全準同型暗号への鍵、ブートストラップ …… 474
15.2.4　LWE 問題に基づく FHE …… 476
15.2.5　どこで使われているのか …… 479
15.3　汎用ゼロ知識証明（ZKP） …… 480
15.3.1　zk-SNARK のしくみ …… 483
15.3.2　証明の一部を隠す準同型コミットメント …… 484
15.3.3　準同型コミットメントを改良できる、双線形ペアリング …… 485
15.3.4　簡潔性の由来 …… 486
15.3.5　プログラムから多項式へ …… 487

15.3.6　プログラムはコンピューターのためのもの：人には演算回路が必要 …… 488
15.3.7　演算回路から R1CS へ …… 489
15.3.8　R1CS から多項式へ …… 490
15.3.9　指数を隠している多項式の評価には 2 人が必要 …… 491
この章のまとめ …… 493

第 16 章　暗号が破綻するとき …… 495

16.1　適切な暗号プリミティブや暗号プロトコルを見いだすのは、退屈な作業 …… 496
16.2　暗号プリミティブまたは暗号プロトコルをどう使うか。礼儀正しい標準と形式的検証 …… 498
16.3　適切なライブラリはどこにあるか …… 502
16.4　暗号の誤用：開発者は敵と思え …… 503
16.5　やり方を間違える：ユーザブルセキュリティ …… 505
16.6　暗号は単独で存在するわけではない …… 507
16.7　暗号を実際に扱う者としての責任：独自の暗号を作るなかれ …… 508
この章のまとめ …… 510

お別れの前に …… 496
KRACK 攻撃 …… 501
エピソードを紹介 …… 506

付録：演習の回答 …… 513

謝辞 …… 519