

CRYPTOGRAPHIE APPLIQUÉE

Algorithmes, protocoles et codes source en C

2^e édition

Bruce Schneier

Traduction de Laurent Viennot



Bruce Schneier

Cryptographie appliquée

Deuxième édition

Protocoles, algorithmes
et codes source en C

Traduction de Laurent Viennot



Vuibert Informatique

L'édition originale de ce livre a été publiée aux États-Unis par John Wiley & Sons, Inc., 605 Third Avenue, New York, N.Y. 10158-0012, sous le titre :

Applied Cryptography – Second Edition

© John Wiley & Sons, Inc., 1996.

Les programmes figurant dans ce livre ont pour but d'illustrer les sujets traités. Il n'est donné aucune garantie quant à leur fonctionnement une fois compilés, assemblés ou interprétés dans le cadre d'une utilisation professionnelle ou commerciale.

Conception de la couverture : Jean Widmer

Contact : informatique@vuibert.fr

Web : www.vuibert.fr

© International Thomson Publishing France, Paris, 1997

© Vuibert, Paris, 2001

ISBN 2-7117-8676-5

Toute représentation ou reproduction intégrale ou partielle, faite sans le consentement de l'auteur, ou de ses ayants droit, ou ayants cause, est illicite (loi du 11 mars 1957, alinéa 1^{er} de l'article 40). Cette représentation ou reproduction, par quelque procédé que ce soit, constituerait une contrefaçon sanctionnée par les articles 425 et suivants du Code pénal. La loi du 11 mars 1957 n'autorise, aux termes des alinéas 2 et 3 de l'article 41, que les copies ou reproductions strictement réservées à l'usage privé du copiste et non destinées à une utilisation collective d'une part, et d'autre part, que les analyses et les courtes citations dans un but d'exemple et d'illustration.

Table des matières

Préface	xiii
Comment lire ce livre	xiv
Remerciements	xvii
À propos de l'auteur	xix
1 Principes de base	1
1.1 Terminologie	1
1.2 Steganographie	9
1.3 Substitution et transposition	10
1.4 <i>Ou exclusif</i> simple	14
1.5 Masque jetable	15
1.6 Algorithmes informatiques	18
1.7 Grands nombres	18
I Protocoles cryptographiques	21
2 Briques élémentaires	23
2.1 Introduction aux protocoles	23
2.2 Communications à l'aide d'un cryptosystème à clef secrète	30
2.3 Fonctions à sens unique	31
2.4 Fonctions de hachage à sens unique	32
2.5 Communications à l'aide d'un cryptosystème à clef publique	33
2.6 Signatures numériques	37
2.7 Signatures numériques avec chiffrement	44
2.8 Générateurs aléatoires et pseudo-aléatoires	47
3 Protocoles élémentaires	51
3.1 Échange de clefs	51
3.2 Authentification	56
3.3 Authentification et échange de clefs	61
3.4 Analyse formelle des protocoles d'authentification et d'échange de clefs	70
3.5 Cryptographie à clef publique à clefs multiples	74
3.6 Secret morcelé	75
3.7 Secret réparti	77

3.8	Protection cryptographique de bases de données	80
4	Protocoles intermédiaires	81
4.1	Services de datation	81
4.2	Canal subliminal	85
4.3	Signatures numériques incontestables	87
4.4	Signatures numériques à vérificateur dédié	88
4.5	Signatures par procuration	89
4.6	Signatures collectives	90
4.7	Signatures numériques « <i>Fail-Stop</i> »	91
4.8	Calcul avec données chiffrées	92
4.9	Mise en gage	92
4.10	Jouer à pile ou face	95
4.11	Poker à l'aveugle	99
4.12	Accumulateurs à sens unique	102
4.13	Divulgateur tout ou rien de secrets	103
4.14	Dépôt de clefs	103
5	Protocoles avancés	109
5.1	Preuves à divulgation nulle	109
5.2	Identification par preuve à divulgation nulle	117
5.3	Signatures en aveugle	120
5.4	Cryptographie à clef publique à base d'identification	123
5.5	Transfert inconscient	124
5.6	Signatures inconscientes	126
5.7	Signature simultanée de contrat	127
5.8	Courrier électronique certifié	131
5.9	Échange simultané de secrets	132
6	Protocoles ésoériques	135
6.1	Élections sûres	135
6.2	Calcul réparti sûr	144
6.3	Diffusion de messages anonymes	148
6.4	Argent électronique	150
II	Techniques cryptographiques	161
7	Longueur des clefs	163
7.1	Longueur des clefs secrètes	163
7.2	Longueur des clefs publiques	170
7.3	Comparaison de la longueur des clefs secrètes et des clefs publiques	178
7.4	Attaques des anniversaires contre une fonction de hachage à sens unique	178
7.5	Quelle doit être la longueur de clef?	179
7.6	Avertissement	180

8	Gestion des clefs	181
8.1	Génération de clefs	182
8.2	Espaces des clefs non linéaires	188
8.3	Transfert de clefs	188
8.4	Vérification de clefs	190
8.5	Utilisation des clefs	192
8.6	Mise à jour des clefs	193
8.7	Stockage des clefs	193
8.8	Duplicata des clefs	194
8.9	Clefs compromises	195
8.10	Longévité des clefs	196
8.11	Destruction des clefs	197
8.12	Gestion des clefs pour la cryptographie à clef publique	198
9	Types et modes d'algorithmes	201
9.1	Carnet de codage électronique	202
9.2	Bloc rejoué	203
9.3	Mode de chiffrement avec chaînage de blocs	205
9.4	Algorithmes de chiffrement en continu	209
9.5	Chiffrement autosynchrone en continu	211
9.6	Chiffrement à rétroaction	212
9.7	Chiffrement synchrone en continu	214
9.8	Mode de rétroaction de sortie	216
9.9	Mode « compteur »	219
9.10	Autres modes	220
9.11	Choix d'un mode opératoire de chiffrement	222
9.12	Intercalation	223
9.13	Chiffrement par blocs <i>vs</i> chiffrement en continu	225
10	Utilisation des algorithmes	227
10.1	Choix d'un algorithme	228
10.2	La cryptographie à clef publique <i>vs</i> la cryptographie à clef secrète	230
10.3	Chiffrement des canaux de communication	230
10.4	Chiffrement des données à des fins de stockage	235
10.5	Chiffrement matériel <i>vs</i> chiffrement logiciel	237
10.6	Compression, codage et chiffrement	240
10.7	Détection du chiffrement	241
10.8	Cacher du texte chiffré dans du texte chiffré	242
10.9	Destruction d'information	243
III	Algorithmes cryptographiques	245
11	Rudiments mathématiques	247
11.1	Théorie de l'information	247
11.2	Théorie de la complexité	251
11.3	Théorie des nombres	256
11.4	Factorisation	271

11.5	Génération de nombres premiers	274
11.6	Logarithmes discrets dans un corps fini	278
12	Le DES	281
12.1	Historique	281
12.2	Description du DES	286
12.3	Niveau de sécurité du DES	296
12.4	Cryptanalyse différentielle et linéaire	302
12.5	Les critères réels de conception	311
12.6	Variantes du DES	312
12.7	À quel point le DES est-il sûr de nos jours?	318
13	Autres algorithmes de chiffrement par blocs	321
13.1	LUCIFER	321
13.2	MADRYGA	322
13.3	NEWDES	325
13.4	FEAL	325
13.5	REDOC	331
13.6	LOKI	332
13.7	KHUFU et KHAFRE	335
13.8	RC2	337
13.9	IDEA	338
13.10	MMB	345
13.11	CA-1.1	346
13.12	SKIPJACK	347
14	Encore d'autres algorithmes de chiffrement par blocs	351
14.1	GOST	351
14.2	CAST	354
14.3	BLOWFISH	355
14.4	SAFER	359
14.5	3-WAY	361
14.6	CRAB	362
14.7	SXAL8 et MBAL	364
14.8	RC5	364
14.9	Autres algorithmes de chiffrement par blocs	366
14.10	Théorie des algorithmes de chiffrement par blocs	366
14.11	Utilisation de fonction de hachage à sens unique	372
14.12	Choisir un algorithme de chiffrement par blocs	375
15	Combinaison d'algorithmes de chiffrement par blocs	377
15.1	Surchiffrement double	377
15.2	Surchiffrement triple	379
15.3	Doublement de la longueur de bloc	384
15.4	Autres schémas de surchiffrement	384
15.5	Troncature de clef (dans CDMF)	387
15.6	Blanchiment	387
15.7	Mise en cascade de plusieurs algorithmes	388

15.8	Combiner plusieurs algorithmes de chiffrement par blocs	389
16	Générateurs de suites aléatoires et chiffrement en continu	391
16.1	Générateurs pseudo-aléatoires de suites	391
16.2	Registres à décalage à rétroaction linéaire	395
16.3	Conception et analyse d'algorithmes de chiffrement en continu	402
16.4	Chiffrement en continu à base de RDRL	403
16.5	A5	412
16.6	HUGUES XPD/KPD	413
16.7	NANOTEQ	413
16.8	RAMBUTAN	414
16.9	Générateurs additifs	414
16.10	GIFFORD	416
16.11	ALGORITHME M	417
16.12	PKZIP	417
17	Autres algorithmes de chiffrement en continu et générateurs de suites vraiment aléatoires	419
17.1	RC4	419
17.2	SEAL	420
17.3	WAKE	423
17.4	Registres à décalage à rétroaction avec retenue	424
17.5	Chiffrement en continu à base de RDRR	427
17.6	Registres à décalage à rétroaction non linéaire	433
17.7	Autres algorithmes de chiffrement en continu	435
17.8	Approche par la théorie des systèmes	436
17.9	Approche par la théorie de la complexité	437
17.10	Autres approches à la conception d'algorithmes de chiffrement en continu	439
17.11	Chiffrement en continu en cascade	441
17.12	Choisir un algorithme de chiffrement en continu	442
17.13	Génération de plusieurs flux à partir d'un seul générateur pseudo-aléatoire de suites	442
17.14	Générateurs de suites vraiment aléatoires	444
18	Fonctions de hachage à sens unique	453
18.1	Introduction	453
18.2	SNEFRU	455
18.3	N-HASH	457
18.4	MD4	458
18.5	MD5	460
18.6	MD2	465
18.7	Algorithme sûr de hachage SHA	465
18.8	RIPE-MD	469
18.9	HAVAL	469
18.10	Autres fonctions de hachage à sens unique	470
18.11	Utilisation d'algorithmes de chiffrement par blocs	471
18.12	Utilisation d'algorithmes à clef publique	479

BIBLIOTHEQUE DU CERIST

18.13	Choix d'une fonction de hachage à sens unique	479
18.14	Codes d'authentification de messages	479
19	Algorithmes à clef publique	485
19.1	Introduction	485
19.2	Algorithmes à empilement	486
19.3	RSA	491
19.4	POHLIG-HELLMAN	499
19.5	RABIN	500
19.6	ELGAMAL	501
19.7	MCELIECE	504
19.8	Cryptosystèmes à courbes elliptiques	505
19.9	LUC	506
19.10	Automates finis	507
20	Algorithmes de signature numérique à clef publique	509
20.1	Algorithme de signature numérique DSA	509
20.2	Variantes de DSA	520
20.3	Algorithme de signature numérique GOST	522
20.4	Schémas de signature numérique à base de logarithmes discrets	523
20.5	ONG-SCHNORR SHAMIR	525
20.6	ESIGN	526
20.7	Automates cellulaires	527
20.8	Les autres algorithmes à clef publique	527
21	Schémas d'identification	531
21.1	FEIGE-FIAT-SHAMIR	531
21.2	GUILLOU-QUISQUATER	536
21.3	SCHNORR	538
21.4	Convertir un schéma d'identification en un schéma de signature numérique	540
22	Algorithmes d'échange de clefs	541
22.1	DIFFIE-HELLMAN	541
22.2	Protocole point à point	544
22.3	Protocole à trois passes de SHAMIR	544
22.4	COMSET	545
22.5	Échange de clefs chiffré	546
22.6	Négociation de clef fortifiée	550
22.7	Distribution de clef de conférence et diffusion de secret	551
23	Algorithmes spéciaux pour protocoles	555
23.1	Cryptographie à clef publique à clefs multiples	555
23.2	Algorithmes de partage de secret	556
23.3	Canal subliminal	560
23.4	Signatures numériques incontestables	565
23.5	Signatures numériques à vérificateur dédié	567
23.6	Calcul avec données chiffrées	569

23.7	Pile ou face équitable	570
23.8	Accumulateurs à sens unique	572
23.9	Divulgence tout ou rien de secrets	572
23.10	Cryptosystèmes équitables et à sûreté intégrée	575
23.11	Preuves à divulgation nulle	577
23.12	Signatures en aveugle	579
23.13	Transfert inconscient	579
23.14	Calcul réparti sûr	580
23.15	Chiffrement probabiliste	582
23.16	Cryptographie quantique	584

IV Le monde réel 587

24 Exemples de réalisation 589

24.1	Protocole IBM de gestion de clefs secrètes	589
24.2	MITRENET	590
24.3	RNIS	591
24.4	STU-III	593
24.5	KERBEROS	594
24.6	KRYPTOKNIGHT	600
24.7	SESAME	600
24.8	Architecture cryptographique commune d'IBM	601
24.9	Environnement d'authentification ISO	602
24.10	« Privacy-Enhanced Mail » (PEM)	606
24.11	« Message Security Protocol » (MSP)	612
24.12	« Pretty Good Privacy » (PGP)	613
24.13	Cartes à puce	615
24.14	« Public-Key Cryptography Standards » (PKCS)	616
24.15	Système de paiement électronique universel	618
24.16	CLIPPER	620
24.17	CAPSTONE	622
24.18	Modèle 3600 du dispositif de sécurité du téléphone d'AT&T	623

25 Politique 625

25.1	« National Security Agency » (NSA)	625
25.2	« National Computer Security Center » (NCSC)	627
25.3	« National Institute of Standards and Technology » (NIST)	628
25.4	RSA DATA SECURITY, INC.	632
25.5	« Public Key Partners » (PKP)	632
25.6	« International Association for Cryptologic Research » (IACR)	634
25.7	« RACE Integrity Primitives Evaluation » (RIPE)	634
25.8	« Conditional Access for Europe » (CAFE)	635
25.9	« ISO/IEC 9979 »	636
25.10	Groupes industriels, de défense des libertés civiles, et professionnelles	637
25.11	SCI.CRYPT	638
25.12	CYPHERPUNKS	638

25.13 Brevets	639
25.14 Réglementation américaine à l'exportation	639
25.15 Importation et exportation de cryptographie	647
25.16 Légalité	648
Postface de Matt Blaze	651
V Code source	655
DES	657
LOKI 91	675
IDEA	685
GOST	701
BLOWFISH	711
3-WAY	721
RC5	727
A5	729
SEAL	735
Lexique anglais-français	741
Bibliographie	747
Index	827