

NIELS FERGUSON,
BRUCE SCHNEIER

Cryptographie

En pratique



Vuibert Informatique

BIBLIOTHEQUE DU CERIST

Cryptographie

En pratique

BIBLIOTHEQUE DU CERIST

NIELS FERGUSON,
BRUCE SCHNEIER

Cryptographie

En pratique



Vuibert Informatique

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

Practical Cryptography

© Wiley & Sons, 2003.

© Vuibert, Paris, 2004

ISBN 2-7117-4820-0

ISSN 1767-1485

Dans la même collection :

Management avec Excel, J. Akoka, I. Comyn-Wattiau, D. Briolat, 2-7117-8699-4

Conception des bases de données relationnelles, J. Akoka, I. Comyn-Wattiau, 2-7117-8678-1

La programmation, Brian W. Kernighan, Rob Pike, 2-7117-8670-6

Client/serveur à 3 niveaux, Jerri Edwards, 2-7117-8656-0

Test logiciel, John Watkins, 2-7117-4806-5

Contact : informatique@vuibert.fr

Web : www.vuibert.fr

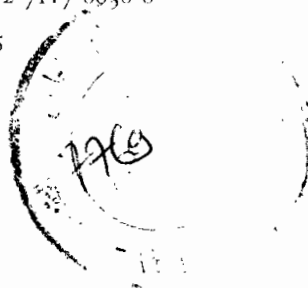


Illustration de la couverture : Didier Thimonier.

Cet ouvrage a été achevé d'imprimer par Grapho 12 à Saint-Rémy en août 2004.

Les programmes et exemples figurant dans ce livre ont pour but d'illustrer les sujets traités. Il n'est donné aucune garantie quant à leur utilisation dans le cadre d'une activité professionnelle ou commerciale.

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	XV
1 Notre philosophie	1
1.1 Les dangers de la performance	1
1.2 Les dangers de la fonctionnalité	4
2 Le contexte de la cryptographie	5
2.1 Le rôle de la cryptographie	5
2.2 La règle du maillon le plus faible	6
2.3 un environnement hostile	8
2.4 Paranoïa pratique	9
2.4.1 Attaque	10
2.5 Modèle de menace	11
2.6 La cryptographie n'est pas toujours la solution	13
2.7 La cryptographie est difficile	14
2.8 La cryptographie est facile	15
2.9 Bibliographie	15
3 Introduction à la cryptographie	17
3.1 Chiffrement	17
3.1.1 Le principe de Kerckhoffs	18
3.2 Authentification	19
3.3 Chiffrement à clé publique	21
3.4 Signatures numériques	22
3.5 Infrastructure à clé publique	23
3.6 Attaques	24
3.6.1 Texte chiffré seul	25
3.6.2 Texte en clair connu	25
3.6.3 Texte en clair choisi	25
3.6.4 Texte chiffré choisi	26
3.6.5 Attaques par différenciation	26
3.6.6 Attaque de l'anniversaire	27
3.6.7 Attaque <i>meet in the middle</i>	28

3.6.8	Autres types d'attaques	29
3.7	Niveau de sécurité	29
3.8	Performance	30
3.9	Complexité	31
I	Sécurité des messages	33
4	Chiffrement par bloc	35
4.1	Qu'est-ce que le « chiffrement par bloc » ?	35
4.2	Les types d'attaque contre le chiffrement par bloc	36
4.3	Le chiffrement par bloc idéal	37
4.4	La sécurité du chiffrement par bloc	38
4.4.1	Parité d'une permutation	40
4.5	Chiffrements par bloc réels	41
4.5.1	DES	42
4.5.2	AES	44
4.5.3	Serpent	47
4.5.4	Twofish	48
4.5.5	Les autres finalistes AES	50
4.5.6	Attaque par résolution d'équations	50
4.5.7	Quel chiffrement par bloc choisir ?	51
4.5.8	Quelle taille de clé choisir ?	52
5	Modes de chiffrement par bloc	55
5.1	Bourrage	55
5.2	ECB	56
5.3	CBC	57
5.3.1	Vecteur d'initialisation fixe	57
5.3.2	Vecteur d'initialisation compteur	57
5.3.3	Vecteur d'initialisation aléatoire	58
5.3.4	Vecteur d'initialisation généré par nonce	58
5.4	OFB	60
5.5	CTR	61
5.6	Nouveaux modes	62
5.7	Quel mode utiliser ?	63
5.8	Fuite d'information	64
5.8.1	Probabilité de collision	65
5.8.2	Comment gérer les fuites d'information	66
5.8.3	À propos de nos mathématiques	67
6	Fonctions de hachage	69
6.1	Sécurité des fonctions de hachage	70
6.2	Fonctions de hachage réelles	71
6.2.1	MD5	72

6.2.2	SHA-1	73
6.2.3	SHA-256, SHA-384 et SHA-512	73
6.3	Faibles des fonctions de hachage	74
6.3.1	Extensions de longueur	74
6.3.2	Collision de message partielle	75
6.4	Corriger les faibles	76
6.4.1	Une correction approfondie	76
6.4.2	Une correction plus efficace	77
6.5	Quelle fonction de hachage choisir ?	78
6.6	Travaux futurs	79
7	Codes d'authentification de message	81
7.1	Ce que fait un MAC	81
7.2	Le MAC idéal	81
7.3	Sécurité du MAC	82
7.4	CBC-MAC	83
7.5	HMAC	84
7.5.1	HMAC ou SHA _d	85
7.6	UMAC	86
7.6.1	Taille de MAC	87
7.6.2	Quel UMAC ?	87
7.6.3	Flexibilité de plateforme	88
7.6.4	Quantité d'analyse	89
7.6.5	Pourquoi mentionner UMAC ?	89
7.7	Quel MAC choisir ?	89
7.8	Utiliser un MAC	90
8	Le canal sécurisé	93
8.1	Définition du problème	93
8.1.1	Rôles	93
8.1.2	Clé	94
8.1.3	Messages ou flot	94
8.1.4	Propriétés de sécurité	95
8.2	Ordre de l'authentification et du chiffrement	96
8.3	Schéma d'ensemble	98
8.3.1	Numéros de message	98
8.3.2	Authentification	99
8.3.3	Chiffrement	99
8.3.4	Format	100
8.4	Détails	100
8.4.1	Initialisation	100
8.4.2	Envoyer un message	101
8.4.3	Recevoir un message	102
8.4.4	Ordre des messages	104
8.5	Alternatives	104

8.6	Conclusion	105
9	Considérations sur l'implémentation (I)	107
9.1	Créer des logiciels corrects	108
9.1.1	Spécifications	109
9.1.2	Tester et corriger	110
9.1.3	Laxisme	110
9.1.4	Que faire?	111
9.2	Créer des logiciels sûrs	111
9.3	Garder des secrets	112
9.3.1	Effacer l'état	112
9.3.2	Fichier de <i>swap</i>	114
9.3.3	Mémoire cache	116
9.3.4	Rétention de données par la mémoire	116
9.3.5	Accès par d'autres programmes	119
9.3.6	Intégrité des données	119
9.3.7	Que faire?	120
9.4	Qualité du code	120
9.4.1	Simplicité	121
9.4.2	Modularisation	121
9.4.3	Assertions	122
9.4.4	Débordement de tampon	123
9.4.5	Test	121
9.5	Attaques par canal caché	124
9.6	Conclusion	125
II	Négociation de clés	127
10	Générer l'aléatoire	129
10.1	Hasard véritable	130
10.1.1	Des données réellement aléatoires	131
10.1.2	Données pseudo-aléatoires	131
10.1.3	Données réellement aléatoires et générateurs de nombres pseudo-aléatoires	132
10.2	Attaque type contre un générateur de nombres pseudo-aléatoires	133
10.3	Fortuna	134
10.4	Le générateur	134
10.4.1	Initialisation	136
10.4.2	Réensemencer	137
10.4.3	Générer les blocs	137
10.4.4	Générer des données aléatoires	138
10.4.5	Vitesse du générateur	139
10.5	Accumulateur	139
10.5.1	Sources d'entropie	139

10.5.2	Réservoirs d'entropie	140
10.5.3	Considérations d'implémentation	142
10.5.4	Initialisation	144
10.5.5	Obtenir les données aléatoires	145
10.5.6	Ajouter un événement	146
10.6	Fichier de graine	147
10.6.1	Création du fichier de graine	148
10.6.2	Mettre à jour le fichier de graine	148
10.6.3	Quand lire et écrire le fichier de graine ?	149
10.6.4	Sauvegardes	149
10.6.5	Atomicité des mises à jour du système de fichiers	150
10.6.6	Premier démarrage	150
10.7	Que faire ?	151
10.8	Choisir des éléments aléatoires	151
11	Nombres premiers	155
11.1	Divisibilité et nombres premiers	155
11.2	Générer de petits nombres premiers	158
11.3	Calculs modulo un nombre premier	159
11.3.1	Addition et soustraction	160
11.3.2	Multiplication	160
11.3.3	Groupes et corps finis	161
11.3.4	L'algorithme du PGCD	162
11.3.5	L'algorithme d'Euclide étendu	163
11.3.6	Travailler modulo 2	164
11.4	Grands nombres premiers	164
11.4.1	Test de primalité	167
11.4.2	Évaluer des puissances	170
12	Diffie-Hellman	173
12.1	Groupes	174
12.2	Protocole de Diffie-Hellman	175
12.3	Attaque de l'intercepteur	176
12.4	Pièges	177
12.5	Nombres premiers sûrs	178
12.6	Utiliser un sous-groupe plus petit	179
12.7	Taille de p	180
12.8	Règles pratiques	182
12.9	Ce qui pourrait aller mal	183
13	RSA	187
13.1	Introduction	187
13.2	Le théorème des restes chinois	187
13.2.1	Formule de Garner	188
13.2.2	Généralisations	189

13.2.3	Utilisations	190
13.2.4	Conclusion	191
13.3	Multiplication modulo n	191
13.4	Définition de RSA	192
13.4.1	Signatures numériques avec RSA	192
13.4.2	Exposants publics	192
13.4.3	Clé privée	193
13.4.4	Taille de n	195
13.4.5	Générer les clés RSA	195
13.5	Pièges de RSA	197
13.6	Chiffrement	198
13.7	Signatures	200
14	Introduction aux protocoles cryptographiques	203
14.1	Rôles	203
14.2	Confiance	201
14.2.1	Risque	205
14.3	Motivation	205
14.4	La notion de confiance dans les protocoles cryptographiques	207
14.5	Messages et étapes	208
14.5.1	La couche transport	208
14.5.2	Identification de protocole et de message	209
14.5.3	Encodage de message et analyse lexicale	210
14.5.4	État d'exécution du protocole	210
14.5.5	Erreurs	211
14.5.6	Rejeu et relance	212
15	Protocole de négociation de clés	215
15.1	Le contexte	215
15.2	Première tentative	216
15.3	Les protocoles ne meurent jamais	217
15.4	Une convention d'authentification	218
15.5	Deuxième tentative	218
15.6	Troisième tentative	220
15.7	Notre protocole final	221
15.8	Différents points de vue sur le protocole	223
15.8.1	Le point de vue d'Alice	223
15.8.2	Le point de vue de Bob	223
15.8.3	Le point de vue de l'attaquant	223
15.8.4	Compromission de clé	224
15.9	Complexité du protocole	225
15.9.1	Astuces d'optimisation	226
15.10	Complexité du protocole	226
15.11	Négociation de clés avec un mot de passe	228

16 Considérations sur l'implémentation (II)	229
16.1 Arithmétique des grands nombres entiers	229
16.1.1 Wooping	231
16.1.2 Vérifier les calculs de DH	233
16.1.3 Vérifier le chiffrement RSA	234
16.1.4 Vérifier les signatures RSA	234
16.1.5 Conclusion	234
16.2 Multiplication rapide	235
16.3 Attaques par canal caché	236
16.3.1 Contre-mesures	237
16.4 Protocoles	238
16.4.1 Protocoles au-dessus d'un canal sécurisé	238
16.4.2 Recevoir un message	239
16.4.3 Temporisations	240
 III Gestion de clés	 243
17 L'horloge	245
17.1 Utilisations d'une horloge	245
17.1.1 Expiration	245
17.1.2 Valeur unique	245
17.1.3 Uniformité	246
17.1.4 Transactions en temps réel	246
17.2 Utiliser la puce d'horloge temps réel	247
17.3 Dangers pour la sécurité	247
17.3.1 Retarder l'horloge	247
17.3.2 Arrêter l'horloge	248
17.3.3 Avancer l'horloge	249
17.4 Concevoir une horloge fiable	249
17.5 Le problème du « même état »	250
17.6 L'heure	252
17.7 Conclusion	253
 18 Serveurs de clés	 255
18.1 Les bases	255
18.2 Kerberos	256
18.3 Solutions plus simples	256
18.3.1 Connexion sécurisée	257
18.3.2 Création de clé	258
18.3.3 Régénération de clé	258
18.3.4 Autres propriétés	258
18.4 Que choisir ?	259

19 La PKI rêvée	261
19.1 Très brève présentation des PKI	261
19.2 Exemples de PKI	262
19.2.1 PKI universelle	262
19.2.2 Accès à un réseau privé virtuel	262
19.2.3 Banque électronique	262
19.2.4 Capteurs de raffinerie	262
19.2.5 Organisme de carte de crédit	263
19.3 Détails supplémentaires	263
19.3.1 Certificats multiniveaux	263
19.3.2 Expiration	264
19.3.3 Autorité d'enregistrement indépendante	265
19.4 Conclusion	266
20 Réalité des PKI	267
20.1 Noms	267
20.2 Autorité	269
20.3 Confiance	270
20.4 Autorisation indirecte	271
20.5 Autorisation directe	271
20.6 Systèmes de créances	272
20.7 Le rêve amendé	274
20.8 Révocation	275
20.8.1 Liste de révocation	275
20.8.2 Expiration rapide	276
20.8.3 La révocation est nécessaire	277
20.9 Pourquoi donc utiliser une PKI?	277
20.10 Que choisir?	278
21 PKI : Aspects pratiques	281
21.1 Format des certificats	281
21.1.1 Langage d'autorisation	281
21.1.2 La clé racine	282
21.2 La vie d'une clé	283
21.3 Pourquoi les clés s'usent-elles	284
21.4 Que faire?	285
22 Conserver les secrets	287
22.1 Disque	287
22.2 Mémoire humaine	288
22.2.1 Salage et extension	289
22.3 Stockage portable	291
22.4 Dispositif de sécurité	292
22.5 Interface utilisateur sécurisée	293
22.6 Biométrie	294

22.7	Inscription unique	295
22.8	Risque de perte	296
22.9	Partage de secret	296
22.10	Destruction de secrets	297
22.10.1	Papier	298
22.10.2	Stockage magnétique	298
22.10.3	Stockage à semiconducteur	299
IV	Annexes	301
23	Standards	303
23.1	Le processus de standardisation	303
23.1.1	Le standard	305
23.1.2	Fonctionnalités	305
23.1.3	Sécurité	305
23.2	SSL	306
23.3	Standardisation par la compétition : AES	307
24	Brevets	309
24.1	État antérieur de la technique	309
24.2	Extensions	310
24.3	Imprécision	310
24.4	Lire des brevets	311
24.5	Autorisation	311
24.6	Brevets défensifs	313
24.7	Améliorer le système de brevets	313
24.8	Avertissement	314
25	Implication d'experts	315
	Bibliographie	319
	Index	327