

SYSTÈMES ET RÉSEAUX



H.X. Mel & Doris Baker

La Cryptographie décryptée

Collection

Référence


CAMPUSPRESS

www.campuspress.net



-005-435-1

2-005-435-1

14/31

Table des matières

La cryptographie décryptée

H.X. Mel
Doris Baker

Avec la collaboration de
Steve Burnett et John Kinyon




CAMPUSPRESS

Retrouvez
tous nos livres sur
www.campuspress.net

Table des matières

Avant-propos	XV
e-tout	XV
Préface : Un outil pour tous	XVII
Remerciements	XIX
Introduction	1
Bienvenue en première ligne	1
Lecture rapide ?	2

Partie I. La cryptographie à clé secrète

Chapitre 1. Cadenas et clés	7
Cadenas et combinaisons	7
Termes de cryptographie	10
Créer et résoudre des puzzles	10
Résumé	11
Chapitre 2. Substitution et chiffre de César	13
Cryptanalyse du système de César	17
Le pouvoir aux masses	18
Distinguer la méthode de la clé	20
Ajout de clés	20
Une faiblesse du chiffre de César : il ne masque pas les schémas linguistiques	22
Substitutions plus complexes : la méthode de Vigenère	24
Résumé	28
Chapitre 3. Chiffrements par transposition	29
Motifs et cryptanalyse	30
Ajout de complexité	32
Transposition informatique	34

Combiner substitution et transposition	36
Résumé	38
Chapitre 4. Diffuser et désorienter : comment les cryptographes finissent par gagner la partie	39
La diffusion	40
Le cryptogramme de Polybe	41
Le principe de confusion	44
Les serrures et les clés cryptographiques	45
Résumé	47
Chapitre 5. Le standard DES n'est plus fort	49
Besoin historique d'un standard de chiffrement	50
Parcourir les clés informatiques	53
Double et Triple DES	55
Modes DES (et autres chiffrements par blocs)	56
Effet d'avalanche	56
Supplément : nombres binaires et lettres informatiques	57
Résumé	58
Chapitre 6. Evolution de la cryptographie : mondialisation	59
La cryptographie ancienne	60
Les besoins commerciaux et militaires	62
L'ère informatique	64
Résumé	66
Chapitre 7. Garanties apportées par les clés secrètes	67
La confidentialité	68
L'authentification	69
Attaque par authentification	71
Des nombres pas vraiment aléatoires	72
L'intégrité	74
Utiliser le code MAC pour s'assurer de l'intégrité du message	75
Pourquoi s'encombrer d'un code d'authentification de message ?	76
Compression de fichiers et compression MAC	77
La non-répudiation : les clés secrètes ne peuvent y parvenir	78
Résumé	79

Chapitre 8. Problèmes posés par l'échange de clés secrètes	81
Le problème et sa solution traditionnelle	82
Utilisation d'un tiers	84
Centre de distribution des clés et récupération des clés	86
Problèmes posés par l'utilisation d'un tiers	88
Augmentation du nombre de clés secrètes	88
Confiance et durée de vie	89
Résumé	90
 Partie II. Cryptographie à clé publique 	
Chapitre 9. Pionniers de la clé publique : échange public de clés secrètes	93
Recherche d'une solution innovante pour remettre la clé	93
Développement d'une solution innovante pour remettre la clé secrète	94
Première tentative : une base de données de paires clé/numéro de série	94
Deuxième tentative : base de données chiffrée de paires clé/numéro de série ..	95
L'intuition de Merkle : paire clé chiffrée/numéro de série chiffrée individuellement	97
BlackHat face à un épineux problème	99
La clé de la technologie des clés publiques	99
Nouvelle solution : la méthode de Diffie-Hellman-Merkle	101
Alice et Bob s'accordent sur une clé secrète	102
Problèmes posés par la méthode Diffie-Hellman	103
Clés distinctes pour le chiffrement et le déchiffrement	104
Résumé	106
Chapitre 10. Confidentialité obtenue grâce aux clés publiques	107
Nouveaux rebondissements en matière de sécurité	107
Garanties de confidentialité	110
Distribution des clés publiques	111
Confidentialité bidirectionnelle	112
Résumé	113
Chapitre 11. Créer des clés publiques : astuces mathématiques	115
Problème simple posé à Alice	117
Astuces mathématiques, niveau école primaire	119

Ecole primaire, toujours	120
Divisions et reste : les mathématiques modulaires	122
Inverses modulaires	125
Utiliser des inverses modulaires pour créer une clé publique	128
Synthèse	129
Mettre BlackHat devant un problème complexe et long à résoudre	129
Trappe de sortie vers le problème simple	130
Cryptographie sac à dos	132
Calculs modulo	132
Exercice : trouver quels nombres ont une somme égale à 103	132
Résumé	133
Chapitre 12. Créer des signatures numériques à l'aide de la clé privée	135
Garanties offertes par la signature écrite et numérique	136
Examiner et comparer l'authentification	138
Authentification à clé secrète	138
Authentification à clé privée	138
Authentification et intégrité grâce aux clés privées et secrètes	139
Méthodes d'authentification à clé privée	141
Le système RSA	141
L'algorithme DSA	142
Terminologie des signatures	144
La non-répudiation	144
Garanties dans les deux directions	145
Résumé des garanties fournies par la clé publique	145
Clé publique signifie clé publique/privée	146
Garantie initiée	146
Compression avant signature	147
Résumé	147
Chapitre 13. Hachages Résumés de message sans clé	149
Détecter les modifications involontaires	151
Détecter les modifications volontaires	154
Signer le résumé de message	156
Détecter la falsification de BlackHat	157

Attaques par répétition	159
Supplément : échec dans l'imitation d'un résumé de message	159
Résumé	161
Chapitre 14. Garanties apportées par les résumés de message	163
Deux types de résumés de message	163
Garanties fournies par les résumés de message sans clé	165
Unidirectionnalité	165
Résistance aux collisions	165
Résistance faible aux collisions	166
Exemples d'unidirectionnalité et de résistance faible aux collisions	167
Résistance forte aux collisions	169
Implémentations de résumés sans clé	173
Garanties apportées par les résumés de message à clé	174
Code MAC avec DES	174
Sécurité du DES-MAC	175
Compression des résumés de message	177
Comparaison des vitesses d'exécution de résumés	179
Codes MAC hachés	180
Résumé	180
Chapitre 15. Comparaison entre clés secrètes, clés publiques et résumés de message	181
Vitesse de chiffrement	182
Longueur des clés	183
Facilité de distribution des clés	183
Garanties cryptographiques	184
Clé symétrique (secrète)	185
Clé asymétrique (publique)	185
Résumé	186
Partie III. Distribution de clés publiques	
Chapitre 16. Les certificats numériques	191
Vérifier un certificat numérique	193

Attaques contre les certificats numériques	194
Attaque contre le créateur du certificat numérique	194
Créateur de certificat malveillant	194
Attaque contre l'utilisateur du certificat numérique	195
Attaque la plus désastreuse	195
Comprendre les certificats numériques : comparaison familière	195
Émetteur et sujet	196
Authentification de l'émetteur	196
Transfert de la confiance accordée, de l'utilisateur vers le sujet	197
Responsabilité limitée de l'émetteur	198
Limites de temps	199
Révoquer la confiance	199
Plusieurs certificats	200
Frais d'usage	200
Quels sont les besoins des utilisateurs de certificats numériques ?	201
Obtenir sa première clé publique	202
Certificats inclus dans votre navigateur	202
Résumé	203
Chapitre 17. Infrastructure à clés publiques X.509	205
Pourquoi employer la gestion par certificats X.509 ?	206
Qu'est-ce qu'une autorité de certification ?	207
Candidature, certification et émission	208
Révocation de certificats	211
Interrogation et envoi par préchargement : deux modèles d'envoi de la liste CRL	212
Construire des réseaux de confiance X.509	212
Certificats principaux	213
Autres risques et précautions	218
Noms distinctifs	219
Déclaration CPS	220
Données certifiées X.509	220
Protocole question/réponse	222
Résumé	222

Chapitre 18. Pretty Good Privacy et le système de confiance mutuelle	
<i>(Web of trust)</i>	225
Histoire du logiciel PGP	225
Comparaison des certificats X.509 et PGP	227
Créer des réseaux de confiance	229
Bob valide la clé d'Alice	229
Cédric valide la clé d'Alice envoyée par Bob	230
Delphine valide la clé d'Alice	232
Système de confiance mutuelle	233
Archivage et révocation des certificats PGP	234
Compatibilité entre X.509 et PGP	234
Résumé	234
 Partie IV. Systèmes employés dans le monde réel 	
Paramètres cryptographiques de courrier électronique	236
Négociation des paramètres cryptographiques des systèmes SSL et IPsec	237
Initiation par l'utilisateur du courrier électronique cryptographié, du SSL et d'IPsec	238
Chapitre 19. Le courrier électronique sécurisé	239
Messages électroniques cryptographiques génériques	240
Requérir des services cryptographiques	242
Confidentialité et authentification	244
Choix des services	244
Services de positionnement	245
Se prémunir contre les virus électroniques	246
Résumé	246
Chapitre 20. Les protocoles Secure Socket Layer et Transport Layer Security .	249
Histoire du protocole SSL	250
Vue d'ensemble d'une session SSL	251
Une session SSL en détail	252
Paramètres des salutations et ouverture de négociation	253
Accord sur les clés (échange)	255
Authentification	256
Confidentialité et intégrité	257

Variations sur le protocole TLS	258
Diffie-Hellman anonyme	259
Diffie-Hellman fixe et éphémère	259
Comparaison entre TLS, SSL v3, et SSL v2	260
Problème majeur en SSL v2	260
Problème éventuel en TLS et en SSL	260
Générer des secrets partagés	261
Bob s'authentifie auprès d'AliceDotComStocks	262
Résumé	263
Chapitre 21. Vue d'ensemble du protocole IPsec	265
Sécurité améliorée	266
Gestion des clés	267
Distribution manuelle	268
Distribution automatisée	268
IPsec, Partie 1 : authentification des utilisateurs et échange des clés à l'aide du protocole IKE	269
Accords sur les clés en protocoles SSL/TLS et IPsec	269
Association de sécurité	269
Phases	270
Nomenclature IKE	272
Avantages apportés par l'échange de clés à deux phases	273
Création de clés de chiffrement de masse pour des applications distinctes	274
IPsec, Partie 2 : confidentialité des données chiffrées en masse et intégrité du transport de messages ou de fichiers	274
Protocole et mode	276
Exemples en protocole ESP	280
Exemples en protocole AH	281
Contrôle de la gestion	283
Incompatibilités entre implémentations et complications	285
Résumé	285
Chapitre 22. Chasse-trappes cryptographiques	287
Attaque par répétition	287
Attaque du milieu	288
Vol des clés en mémoire	289

La confidentialité implique-t-elle l'intégrité ?	290
Exemple 1	290
Exemple 2: attaque par couper-coller	291
La clé publique comme outil de cryptanalyse	291
Exemple 1 : attaque du texte clair choisi	291
Standards cryptographiques des clés publiques	293
Exemple 2 : attaque de Bleichenbacher	293
BlackHat emploie la clé publique RSA privée de Bob	294
Résumé	298
Chapitre 23. Protéger ses clés	299
Les cartes à puce	300
Types de cartes à puce	301
Contenu d'une carte à puce	302
Protections et limites	302
Attaques contre les cartes à puce	302
Résumé	304
Epilogue	305
Comment se prononce Rijndael	305
Qui sont les initiateurs de cet algorithme, et d'où viennent-ils ?	305
Pourquoi le NIST a-t-il sélectionné l'algorithme Rijndael comme candidat à l'AES ?	305
Qu'en est-il des quatre autres algorithmes qui n'ont pas été retenus	306
Le standard AES remplacera-t-il le Triple DES et le DES ?	306
Le NIST s'inquiète-t-il du fait que cet algorithme n'a pas été développé aux Etats-Unis ?	306
Quelle est la taille approximative des clés du standard AES ?	306
Clés publiques d'H. X. Mel et de Doris Baker	306
Annexe A. Mathématiques des clés publiques (et notions en nombres aléatoires)	309
Lettres en tant que chiffres	309
Pourquoi tant de maths ?	311
Encore une métaphore	311
Informations préliminaires	313
Nombre inverse	313
Autres inverses	314

Informations préliminaires	
Inverses cryptographiques	315
Nombres premiers	316
Mathématiques modulaires	316
Quelques identités exponentielles	320
L'algorithme RSA	321
Deux trajets	325
Sécurité	333
Dernière question	335
Trouver des nombres premiers	336
Le test de Fermat	341
Trouver l'inverse : algorithme euclidien étendu	344
Pourquoi ça marche ?	349
Autres algorithmes à clé publique	350
L'algorithme Diffie-Hellman	350
Sécurité	354
L'algorithme DSA	354
Pourquoi l'algorithme DSA ?	357
Courbes elliptiques	358
Module premier	359
Ajouter des points	360
L'algorithme EC Diffie-Hellman	364
Sécurité	365
Autres utilisations des courbes elliptiques	366
Pourquoi la cryptographie ECC ?	366
Inconvénients	367
Autres types de courbes elliptiques	368
Autres questions de sécurité	369
Générer des nombres pseudo-aléatoires	369
Qu'est-ce que l'aléatoire ?	370
Le générateur de nombres pseudo-aléatoires	372
La graine	373
L'entropie	375
Autres graines	376
La graine en tant que clé ?	377
Résumé	377

Annexe B. (Quelques) détails sur le protocole IPsec	379
Authentification et gestion des clés IKE	379
IKE Phase 1	380
IKE Phase 2	382
Méthode PFS	384
Modes du Protocole IKE Phase 1 : agressif et principal	386
Attaque par saturation	388
Cookies prudents	388
Options d'authentification	389
Identités	389
IPsec Partie 2 : Confidentialité de masse et intégrité de message	390
Champs d'associations de sécurité	390
Numéro de séquence et antirépétition	391
Architecture	392
Combiner les associations SA	394
Contrôle de la gestion et traitement IPsec	394
Bibliographie	397
Articles	399
Ressources sur Internet	399
Sites offrant de nombreux liens utiles	399
Standards	400
Gouvernement américain	400
Didacticiels et pédagogie	400
Applications et Fournisseurs sélectionnés	401
Confidentialité	402
Actualité	402
Banquiers et avocats	402
Code informatique	403
Divers	403
Index	405