

INFORMATIQUE
ET SYSTÈMES
D'INFORMATION

Information - Commande - Communication

Cryptographie et sécurité des systèmes et réseaux

sous la direction de
Touradj Ebrahimi
Franck Leprévost
Bertrand Warusfel

Hermes

Lavoisier

Cryptographie et sécurité des systèmes et réseaux



sous la direction de
Touradj Ebrahimi
Franck Leprévost
Bertrand Warusfel

Table des matières

Préface	17
Chapitre 1. Introduction	19
Touradj EBRAHIMI, Franck LEPRÉVOST, Bertrand WARUSFEL	
Chapitre 2. Cryptographie à clé secrète	23
Pascal BOUVRY, Jean-Guillaume DUMAS, Roland GILLARD, Jean-Louis ROCH, Sébastien VARRETTE	
2.1. Terminologie	23
2.2. Cryptanalyse et attaques sur les systèmes cryptographiques	25
2.2.1. Les grands types de menaces	25
2.2.2. Les attaques sur un chiffrement	26
2.2.3. Les principes de Kerckhoffs	26
2.3. Principe du chiffrement à clé secrète	27
2.4. Systèmes de chiffrement par blocs (<i>Block Cipher</i>)	27
2.4.1. Introduction	27
2.4.2. Les modes de chiffrement	28
2.4.2.1. Le mode ECB	28
2.4.2.2. Le mode CBC	29
2.4.2.3. Le mode CFB	29
2.4.2.4. Le mode OFB	30
2.4.2.5. Le mode CTR	30
2.4.3. Chiffrements par permutations	31
2.4.4. Chiffrements par substitution	32
2.4.4.1. Chiffrements monoalphabétiques	32
2.4.4.2. Le chiffrement affine	32
2.4.4.3. Chiffrements polyalphabétiques	33
2.4.4.4. Chiffrements tomogrammiques	36

2.4.4.5. Chiffrements polygrammiques	37
2.4.5. Enigma	38
2.4.6. Sécurité inconditionnelle et chiffrement de Vernam	39
2.4.6.1. Notion de sécurité inconditionnelle	39
2.4.6.2. Chiffrement de Vernam (<i>One Time Pad</i>)	40
2.4.7. Le système DES (<i>Data Encryption Standard</i>)	41
2.4.7.1. Algorithme général	41
2.4.7.2. Détails de la fonction $f(A, J)$	43
2.4.7.3. Détails de la diversification de clé dans DES	45
2.4.8. Le système AES (<i>Advanced Encryption Standard</i>)	48
2.4.8.1. Conventions et représentations dans AES	48
2.4.8.2. Préliminaires mathématiques : le corps \mathbb{F}_{256}	50
2.4.8.3. Description de l'algorithme de chiffrement AES	53
2.4.8.4. Détails de la diversification de la clé dans AES	58
2.4.8.5. Déchiffrement dans AES	61
2.4.8.6. Force et faiblesse de l'AES	62
2.4.9. Le système IDEA	62
2.4.9.1. Description d'une ronde	63
2.4.9.2. De la clé aux sous-clés	65
2.4.9.3. Analyse d'IDEA et PES \rightarrow IPES	65
2.4.10. Le système BLOWFISH	65
2.4.10.1. Description des sous-clés	65
2.4.10.2. Algorithme de chiffrement	66
2.4.10.3. Fabrication des sous-clés	66
2.4.11. Le système RC6	66
2.4.12. Automates cellulaires réversibles	67
2.4.12.1. Présentation	67
2.4.12.2. Automates cellulaires réversibles	68
2.4.12.3. Utilisation d'une classe d'automates réversibles pour le chiffrement	70
2.5. Cryptanalyse des chiffrements par blocs	71
2.5.1. Cryptanalyse différentielle	71
2.5.1.1. Analyse différentielle des Boîtes-S	71
2.5.1.2. Application à l'analyse d'une ronde	72
2.5.1.3. Attaque du DES à deux rondes	75
2.5.1.4. Descente dans le DES	75
2.5.1.5. Attaque sur quinze rondes	76
2.5.1.6. De quinze à seize rondes	76
2.5.1.7. Extensions	76
2.5.2. Cryptanalyse linéaire	77
2.5.2.1. Le principe	77
2.5.2.2. Analyse linéaire des Boîtes-S	78
2.5.2.3. Traduction sur la fonction de ronde f	78

2.5.2.4. Lemme d'empilement	83
2.5.2.5. Approximations linéaires pour le DES en r rondes	83
2.5.2.6. Caractéristiques en analyse linéaire	85
2.5.2.7. Attaques à textes en clair connus	86
2.5.2.8. Attaques à textes chiffrés seuls	86
2.5.2.9. Attaque finale sur seize rondes	87
2.6. Systèmes de chiffrement par flux (<i>Stream Cipher</i>)	87
2.6.1. Registres à décalage	87
2.6.2. Geffe	90
2.6.3. A5/1	90
2.6.4. RC4 (<i>Rivest</i>)	91
2.6.5. Bluetooth/E0	91
2.6.6. Automates cellulaires	92
2.6.7. Commentaire final sur les chiffrements par flux	92
2.7. Cryptanalyse des chiffrements par flux	93
2.7.1. Attaque des LFSR	93
2.7.2. Attaque par corrélation	94
2.7.3. Attaque par corrélation rapide	96
2.7.4. Critères de résistance	97
2.8. Conclusion	98
2.9. Bibliographie	99
Chapitre 3. Cryptographie à clé publique	103
Jean-Guillaume DUMAS, Franck LEPRÉVOST, Jean-Louis ROCH, Valentin SAVIN, Sébastien VARRETTE	
3.1. Motivations et principe	103
3.2. Fondements théoriques de la cryptographie à clé publique	105
3.2.1. Théorie de l'information et modélisation du secret	105
3.2.1.1. Quantité d'information et entropie	106
3.2.1.2. Propriétés de l'entropie – Entropie conjointe et conditionnelle	107
3.2.1.3. Entropie et modélisation du secret	111
3.2.2. Complexité algorithmique et fonctions à sens unique	113
3.2.2.1. Un modèle d'ordinateur : la machine de Turing	113
3.2.2.2. Classes de complexité	114
3.2.2.3. Classes de complexité et cryptographie à clé publique	118
3.2.3. Théorie des nombres et algorithmes de base en arithmétique	121
3.2.3.1. Arithmétique modulaire	121
3.2.3.2. Notion de nombre premier	123
3.2.3.3. Plus grand commun diviseur (pgcd)	124
3.2.3.4. Algorithmes d'Euclide	124
3.2.3.5. Inverse modulaire	127
3.2.3.6. Fonction indicatrice d'Euler	127

3.2.3.7. Petit théorème de Fermat	128
3.2.3.8. Exponentiation rapide	128
3.2.3.9. Théorème chinois des restes	129
3.2.3.10. Résidus quadratiques	129
3.2.3.11. Symboles de Legendre et de Jacobi	130
3.3. Le problème de la factorisation	132
3.3.1. Méthode triviale	133
3.3.2. Méthode de Fermat	134
3.3.2.1. Description de la méthode	134
3.3.2.2. Etude d'un exemple	134
3.3.2.3. Variante de la méthode de Fermat	135
3.3.2.4. Impact sur les chiffrements à clés publiques	136
3.3.3. La méthode $p - 1$ de Pollard	136
3.3.3.1. Description de la méthode	136
3.3.3.2. Etude d'un exemple	137
3.3.3.3. Impact sur les chiffrements à clés publiques	138
3.3.4. La méthode ρ de Pollard	139
3.3.4.1. Description de la méthode	139
3.3.4.2. Etude d'un exemple	141
3.3.4.3. Complexité et impact sur les chiffrements à clés publiques	141
3.3.5. La méthode du crible quadratique de Pomerance	142
3.3.5.1. Description de la méthode	142
3.3.5.2. Etude d'un exemple	144
3.4. Fonctions à sens unique – Problème du logarithme discret (DLP)	146
3.4.1. Un premier exemple de FSU : l'exponentiation modulaire	147
3.4.2. Un autre exemple de FSU basé sur la difficulté du logarithme discret	148
3.4.3. DLP par la méthode naïve d'énumération	149
3.4.4. DLP par la méthode <i>Baby-Steps Giant-Steps</i> de Shanks	150
3.4.4.1. Description de la méthode	150
3.4.4.2. Analyse de la complexité de l'algorithme	150
3.4.4.3. Etude d'un exemple	150
3.4.5. DLP par la méthode ρ de Pollard	152
3.4.5.1. Description de la méthode	152
3.4.5.2. Complexité et variantes de la méthode	154
3.4.5.3. Etude d'un exemple	155
3.4.6. DLP par réduction de Pohlig-Hellman	156
3.4.6.1. Réduction de n à p^{v_p} pour tous les p divisant n	156
3.4.6.2. Réduction de p^{v_p} à p	157
3.4.6.3. Complexité de l'algorithme de réduction de Pohlig-Hellman	158
3.4.6.4. Exemple	158
3.4.7. DLP par calcul d'indices	159

3.4.7.1. Résolution du logarithme discret pour la base de facteurs . . .	160
3.4.7.2. Construction d'éléments B -lisses et résolution du problème du logarithme discret initial	160
3.4.7.3. Complexité de l'algorithme du calcul d'indices	161
3.4.7.4. Exemple	161
3.5. Les tests de primalité probabilistes	163
3.5.1. Le test de Fermat	163
3.5.1.1. Exemple	164
3.5.1.2. Les nombres de Carmichael	164
3.5.2. Le test de Solovay-Strassen	164
3.5.2.1. Exemple	165
3.5.2.2. Probabilité d'erreur sur le résultat	165
3.5.3. Le test de Miller-Rabin	166
3.5.3.1. Exemple	166
3.5.3.2. Probabilité d'erreur sur le résultat	166
3.5.4. Le test AKS	167
3.5.5. Pratique de la génération de nombres premiers	168
3.6. Le système cryptographique à clé publique RSA	169
3.6.1. Description de RSA	169
3.6.1.1. Exemple	169
3.6.2. Efficacité et robustesse de RSA	170
3.7. Protocole d'échange de clés de Diffie-Hellman	171
3.8. Le système cryptographique à clé publique de El Gamal	172
3.8.1. Description de El Gamal dans \mathbb{Z}_p^*	172
3.8.2. Généralisation de El Gamal	173
3.9. Fonctions de hachage et signatures électroniques	173
3.9.1. Notion de fonction de hachage	173
3.9.1.1. Classification fonctionnelle	174
3.9.1.2. Construction d'une fonction de hachage	175
3.9.2. Signatures numériques	176
3.9.3. Signatures RSA	178
3.9.3.1. Génération des paramètres	178
3.9.3.2. Génération d'une signature	178
3.9.3.3. Vérification d'une signature	178
3.9.4. Signatures El Gamal	178
3.9.4.1. Génération des paramètres	179
3.9.4.2. Génération d'une signature	179
3.9.4.3. Vérification d'une signature	179
3.9.5. Le standard DSA	179
3.9.5.1. Génération des paramètres	179
3.9.5.2. Génération d'une signature	180
3.9.5.3. Vérification d'une signature	180

3.10. Conclusion	181
3.11. Bibliographie	182
✓ Chapitre 4. Architectures PKI	187
Jean-Guillaume DUMAS, Franck LEPRÉVOST, Jean-Louis ROCH, Sébastien VARRETTE	
4.1. Principe général	187
4.2. Éléments d'une infrastructure PKI	189
4.2.1. Fonctions d'une PKI	189
4.2.2. Acteurs d'une PKI	190
4.3. Les certificats	192
4.3.1. Emission d'un certificat	192
4.3.2. PGP : un premier exemple de certificat	193
4.3.3. Le certificat X.509	194
4.4. Architectures PKI hiérarchiques reposant sur X.509	198
4.4.1. Le modèle PKIX	198
4.4.2. Les fonctions d'administration	200
4.4.3. Authentification d'entités à partir de certificats	201
4.4.4. Processus de migration d'un ancien CA vers un nouveau	203
4.5. Architectures non hiérarchiques	204
4.5.1. Modèle de confiance PGP	204
4.5.2. Spooky/Sudsy	205
4.5.3. DNSSEC	206
4.6. Politique de sécurité et contre-mesures	207
4.6.1. Politique de sécurité	207
4.6.2. Modélisation de la menace et contre-mesures	208
4.7. Défauts des PKI	208
4.8. Bibliographie	208
Chapitre 5. Sécurité Unix	211
Nicolas BERNARD, Yves DENNEULIN, Sébastien VARRETTE	
5.1. Rappels sur Unix	212
5.2. Fonctionnalités et nécessités de sécurité de base	213
5.2.1. Utilisateurs et groupes	213
5.2.2. Droits d'accès aux fichiers	213
5.2.2.1. ACL	213
5.2.2.2. Fonctionnalités offertes par les systèmes de fichiers	214
5.2.2.3. Limites	214
5.2.3. Authentification	214
5.2.3.1. PAM – <i>Pluggable Authentication Modules</i>	215
5.2.3.2. NSS – <i>Name Service Switch</i>	215
5.2.3.3. Authentification BSD	216
5.2.4. Mises à jour	216

5.3. Endurcir le système	217
5.3.1. Désactiver les services non nécessaires	218
5.3.2. Protection/réseau	219
5.3.2.1. Filtres de paquets	219
5.3.2.2. <i>Tcpwrappers</i> et assimilés	220
5.3.3. Protections contre les débordements de tampons	221
5.3.3.1. A l'exécution	221
5.3.3.2. A la compilation	221
5.3.3.3. Pile non exécutable	222
5.3.4. Quotas	222
5.3.4.1. Quotas disques	222
5.3.4.2. Quotas d'exécution	222
5.3.5. Sudo	224
5.3.6. Niveaux de sécurité du noyau	224
5.3.7. Organisation des fichiers	225
5.3.7.1. Monter les partitions avec des droits restreints	225
5.3.7.2. Supprimer le répertoire /tmp	226
5.3.8. Durcir le noyau	226
5.3.9. Chiffrer les disques	228
5.4. Confinement	229
5.4.1. Limiter ce que voit un processus	230
5.4.1.1. Virtualisation	230
5.4.1.2. Filtrage des appels systèmes	231
5.4.2. Limiter l'utilisation des ressources	232
5.5. Détection d'attaques	232
5.5.1. Logs	233
5.5.1.1. Syslog	233
5.5.1.2. Gestion des logs	235
5.5.2. Intégrité des fichiers	235
5.5.3. IDS	237
5.6. Audit de sécurité, recherche de failles et analyse après intrusion	238
5.6.1. Recherche de failles	238
5.6.2. Analyse après intrusion	240
5.7. Conclusion	240
5.8. Bibliographie	241

❧ Chapitre 6. Sécurité réseau 247

Nicolas BERNARD, Pascal BOUVRY, Yves DENNEULIN, Sébastien VARRETTE

6.1. Les couches matérielles et logicielles d'un réseau	247
6.1.1. Couche matérielle	248
6.1.2. Protocoles réseau	249
6.1.2.1. Protocole de transfert	249
6.1.2.2. Protocole de contrôle	251

6.1.2.3. Communications multiples entre hôtes	252
6.1.2.4. L'importance des standards	253
6.1.2.5. Un mot sur le routage et sur les réseaux privés	255
6.1.3. Services réseaux	256
6.1.4. Applications	257
6.2. Types et sources d'attaques réseau	259
6.2.1. Les dénis de service	259
6.2.2. Les intrusions	261
6.3. Sécurisation des infrastructures	262
6.3.1. <i>Firewall</i>	263
6.3.1.1. Notion de <i>firewall</i>	263
6.3.1.2. Structuration de réseau	263
6.3.1.3. Etude de cas <i>Netfilter/Iptables</i> et PF	266
6.3.2. Interconnexion de sites	271
6.3.2.1. IPSec	271
6.3.2.2. Kerberos	272
6.3.2.3. KryptoKnight	277
6.3.2.4. LDAP	280
6.4. Sécurisation des applications	286
6.4.1. SSH	287
6.4.2. SSL/TLS	287
6.4.3. Sécurisation du courrier électronique	289
6.4.4. Sécurisation de HTTP	290
6.4.5. Sécurisation de DNS	291
6.4.6. Les <i>firewalls</i> applicatifs	292
6.4.7. Les <i>malwares</i> (virus, trojans, etc.)	292
6.5. La détection d'intrusion	293
6.6. Conclusion	295
6.7. Bibliographie	295
Index	299

Le traité Information, Commande, Communication répond au besoin de disposer d'un ensemble complet des connaissances et méthodes nécessaires à la maîtrise des systèmes technologiques.

Conçu volontairement dans un esprit d'échange disciplinaire, le traité IC2 est l'état de l'art dans les domaines suivants retenus par le comité scientifique :

- Réseaux et télécoms
- Traitement du signal et de l'image
- Informatique et systèmes d'information
- Systèmes automatisés et productique
- Management et gestion des STICS
- Cognition et traitement de l'information.

Chaque ouvrage présente aussi bien les aspects fondamentaux qu'expérimentaux. Une classification des différents articles contenus dans chacun, une bibliographie et un index détaillé orientent le lecteur vers ses points d'intérêt immédiats : celui-ci dispose ainsi d'un guide pour ses réflexions ou pour ses choix.

Les savoirs, théories et méthodes rassemblés dans chaque ouvrage ont été choisis pour leur pertinence dans l'avancée des connaissances ou pour la qualité des résultats obtenus dans le cas d'expérimentations réelles.