

Série modulaire sur la
Sécurité informatique

Fascicule 0:

*Introduction à la série
et
Contenu des fascicules*

Guy Lépine et Frédéric Mailhot



AVRIL 2022

Note : En vue d'alléger le texte, le masculin est utilisé pour désigner les femmes et les hommes.

Document fascicule00.pdf

Version 3.14, Avril 2022

Copyright © 2022 Guy Lépine et Frédéric Mailhot,

Département de génie électrique et de génie informatique, Université de Sherbrooke.

Réalisé à l'aide de \LaTeX et TeXstudio.

Série sur la sécurité informatique

Cette série a pour objectif l'introduction à la cryptographie et la sécurité informatique. Ce vaste domaine touche à la fois la théorie des nombres, les algorithmes et méthodes de chiffrement, les systèmes logiciels et matériels en lien avec la sécurité des systèmes numériques, les différents types d'authentification, le calcul de résumés, le calcul de nombres aléatoires, etc. Tous ces éléments sont utiles à un niveau ou à un autre pour protéger les systèmes numériques (ordinateurs, téléphones, tablettes, contrôleurs matériels et autres). Cette série touche à un éventail de techniques et d'algorithmes permettant à tous ces systèmes d'opérer de façon sécuritaire, en protégeant leur intégrité, leur opération, ainsi que l'accès à leurs données. La série est composée d'une série de fascicules, chacun touchant un aspect spécifique de la sécurité informatique. Comme le domaine de la sécurité informatique évolue très rapidement, le nombre de fascicules est appelé à augmenter, pour couvrir de nouveaux concepts ou techniques. En ce moment, la série comporte huit fascicules :

Fascicule 1: Introduction à la cryptographie (Frédéric Mailhot)

Fascicule 2: Grands nombres et calculs rapides (Frédéric Mailhot)

Fascicule 3: Télématique et sécurité (Guy Lépine)

Fascicule 4: Cyberattaques et contre-mesures (Guy Lépine et Frédéric Mailhot)

Fascicule 5: Calcul de résumés (hachage) (Frédéric Mailhot)

Fascicule 6: Nombres aléatoires et pseudo-aléatoires (Frédéric Mailhot)

Fascicule 7: Techniques d'authentification (Frédéric Mailhot)

Fascicule 8: Cryptographie quantique et impact classique (Frédéric Mailhot)

Le premier fascicule couvre à la fois les techniques d'encryptage symétrique (à clé unique) et les techniques à doubles clés (privées et publiques). Il existe de nombreuses méthodes distinctes pour chacune des deux techniques, et nous présenterons les plus connues. Nous introduirons certains concepts provenant de

la théorie des nombres dans cette partie, puisqu'ils sont à l'origine de la majorité des méthodes d'encryptage à clés publiques et privées. Nous discuterons des vulnérabilités de certaines des méthodes d'encryptage et des moyens de protection. En particulier, nous présenterons plusieurs algorithmes de factorisation, dont les performances nous indiquent la taille des clés publiques/privées à utiliser pour bien sécuriser les messages cryptés. La performance des calculs effectués étant primordiale pour une utilisation efficace des méthodes d'encryptage, nous terminerons cette partie par un chapitre sur les méthodes efficaces de calcul des très grands nombres.

Le deuxième fascicule couvre les grands nombres, leur représentation ainsi qu'un ensemble de techniques de calcul rapide.

Le troisième fascicule s'attarde aux protocoles utilisés pour sécuriser les messages dans les systèmes d'information modernes. Il existe de nombreux standards qui datent de l'époque des premiers réseaux d'ordinateurs des années 1970. Depuis 1994 et la croissance explosive de l'internet, de nombreux standards et protocoles ont été proposés et mis en place pour l'échange sécurisé d'information, l'authentification d'utilisateurs, la signature électronique de documents, etc.

Le quatrième fascicule s'occupe des vulnérabilités des systèmes d'information. On y parle des vulnérabilités des systèmes d'exploitation, des problèmes liés aux liens réseau, des outils et méthodes utilisés par les gens qui tentent d'utiliser les systèmes d'autrui à mauvais escient, de même que des outils et techniques de protection.

Le cinquième fascicule touche le calcul des résumés, c'est-à-dire les techniques de hachage. On y retrouve les éléments importants de ces techniques dans un contexte de sécurité des systèmes.

Le sixième fascicule se concentre sur la génération de nombres aléatoires et pseudo-aléatoires. L'importance de ces nombres est d'abord mise en lumière, puis plusieurs techniques à la fois logicielles et matérielles de génération de ces nombres sont présentées.

Le septième fascicule touche les techniques d'authentification. Les techniques usuelles sont présentées, ainsi que des méthodes alternatives, les avantages et inconvénients de chacune étant expliqués.

Le huitième fascicule présente certaines méthodes d'encryptage basées sur les phénomènes quantiques. Cette technologie commence tout juste à être utilisable à l'extérieur des laboratoires de recherche, mais présentera des possibilités impressionnantes lorsqu'on pourra la mettre en oeuvre sur une grande échelle.

Cette série s'intéresse à deux aspects complémentaires des systèmes d'information modernes : la sécurité et l'encryptage. Il est habituel de retrouver des livres qui portent soit sur les techniques d'encryptage, leurs limites, et les mathématiques sous-jacentes, soit sur les vulnérabilités des systèmes d'information, les méthodes employées pour les utiliser, ainsi que les façons de les minimiser et de

les contrôler. Pourtant, quoiqu'il s'agisse de deux champs très distincts, ils ont une influence notable l'un sur l'autre. En effet, la cryptographie est à la base des méthodes modernes d'authentification et de sécurisation des transactions à distance, permettant la définition de protocoles de transfert où l'information n'est compréhensible que par les parties concernées. Cependant, la cryptographie n'est qu'un des éléments essentiels à la sécurité de l'information. En effet, les ordinateurs modernes sont inter-connectés par des réseaux rapides qui en facilitent l'accès. Cet accès rapide et simple aux ordinateurs permet maintenant à des individus ou organisations mal intentionnés d'utiliser les systèmes d'autrui et l'information qu'ils contiennent. La sécurisation d'un système procède donc autant des méthodes d'encryptage modernes que de la compréhension des vulnérabilités des systèmes réseautiques récents et des protocoles et techniques utilisés pour les protéger. Cette série a pour objectif de couvrir ces deux aspects complémentaires dans un ensemble de fascicules relativement indépendants qui permettent de bien appréhender le domaine.

Contexte et historique

Ce document a été écrit au départ comme support des cours GIF-630, puis GIF-380 (Encryptage et sécurité informatique), donnés sous forme d'APP (apprentissage par problème) depuis 2004 au département de génie électrique et informatique de l'université de Sherbrooke. À partir l'automne 2007, le texte a été significativement augmenté et est utilisé comme référence dans six cours gradués formant les modules de spécialisation touchant la sécurité informatique, offerts à la maîtrise et aussi au baccalauréat en génie informatique: GEI-760 (Techniques avancées de cryptographie), GEI-761 (Télématique et protocoles sécurisés), GEI-762 (Sécurité des systèmes informatiques), GEI-771 (Programmation sécurité), GEI-772 (Sécurité web) et GEI-773 (Introduction à l'investigation numérique). Ces sept cours forment une progression qui a pour objectif de familiariser les étudiants tant à la cryptographie qu'à la sécurité informatique dans son sens plus large. Au printemps 2021, il a été décidé de scinder le livre original en une série de fascicules indépendants, intégrant la couverture originale de la matière et un ensemble de sujets et méthodes connexes, le tout en permettant un accès facilité aux différents aspects de la sécurité informatique.

Remerciements

Je remercie tous les étudiants en génie informatique et électrique qui ont lu ces textes et ont indiqué des erreurs, omissions ou explications peu claires, souvent en proposant des solutions ou exposés alternatifs. En particulier, merci à Maxime Albert-Gauthier, Francis Beaulé, Arthur Carré, François Charron, Mathieu Chevalier, Jean-François Desjeans-Gauthier, Éloïse Dubé, Jean-Sébastien

Goupil, Jean-Philippe Jodoin, Mohamed Firas Kammoun, Derek Labadie, Alexandre Mathieu, Pierre-Étienne Messier, Édouard Murat, Simon Poirier et Francis Ruel. Je remercie aussi les chargés d'exercices qui ont pris la peine de lire ce document et ont proposé de nouvelles idées. À cet égard, un merci spécial va à Joël Tran. Je remercie mes collègues Ruben Gonzalez-Rubio et Bernard Beaulieu, qui ont fait d'excellents commentaires au sujet de la structure de ce texte. Les discussions portant sur la pédagogie, avec mes collègues Daniel Dalle et Noël Boutin, ont aussi eu un impact sur ce texte.

F.M.

Contenu des fascicules

Fascicule 1: Introduction à la cryptographie

1	Systèmes de cryptographie à clés symétriques	1
1.1	Chiffre de Vernam et analyse de Shannon	2
1.2	Chiffrement par flux	3
1.2.1	Utilisation de LFSR	4
1.2.2	Chiffre RC4	5
1.2.3	Chiffre A5	7
1.3	Chiffrement par bloc	7
1.3.1	Réseaux de substitution/permutation	7
1.3.2	Méthode de Feistel	11
1.3.3	Standards DES et 3-DES	11
1.3.4	Méthode IDEA	20
1.3.5	Standard AES	20
1.3.5.1	Méthode Rijndael	20
1.3.5.2	Méthodes concurrentes (Twofish, RC6, Serpent, MARS)	20
1.3.6	Mode d'opération des chiffrements par blocs	21
1.3.6.1	Mode "Electronic Codebook" (ECB)	22
1.3.6.2	Mode "Cipher Block Chaining" (CBC)	22
1.3.6.2.1	Vecteur d'Initialisation (VI)	23
1.3.6.3	Mode "Output Feedback" (OFB)	24
1.3.6.4	Mode "Counter" (CTR)	25
2	Concepts de base de la théorie des nombres	27
2.1	Introduction à DH et RSA	28
2.2	Modulos, résidus et congruences	29
2.2.1	Calcul du modulo de produits et de puissances	33
2.2.2	Méthode binaire des exposants	33
2.3	Nombres premiers	36
2.3.1	PGCD et algorithme d'Euclide	37
2.3.2	Algorithme étendu d'Euclide et inverses multiplicatifs modulo	38
2.3.3	Théorème de Fermat	41
2.3.4	Théorème de l'indicatrice d'Euler	45
2.3.5	Inverse multiplicatif - autre méthode de calcul	47

2.3.6	Nombres de Carmichael	48
2.3.7	Calcul et vérification des nombres premiers	49
2.3.7.1	Le crible d'Ératosthène	50
2.3.7.2	Test de Selfridge et Miller-Rabin	51
2.3.7.3	Algorithme AKS	54
2.3.7.4	Découverte de nombres premiers de taille arbitraire	55
2.4	Théorème du reste chinois	56
3	Concepts complémentaires de la théorie des nombres	61
3.1	Calcul de résidus quadratiques	61
3.1.1	Symboles de Legendre et de Jacobi	62
3.1.2	Calcul de la racine carrée d'un résidu	62
3.2	Courbes elliptiques	62
3.3	Factorisation de très grands nombres	63
3.3.1	Méthode ρ de Pollard	63
3.3.2	Méthode $p - 1$ de Pollard	68
3.3.3	Méthode de factorisation par courbe elliptique de Lenstra	70
3.3.4	Méthode du crible quadratique	70
3.3.4.1	Méthode de Fermat	70
3.3.4.2	Méthode de Kraitchik et de Lehmer	72
3.3.4.3	Algorithme de Dixon	72
3.3.4.4	Algorithme de Pomerance	72
3.3.4.4.1	Nombres B-smooth et choix de B	72
3.3.4.4.2	Crible quadratique	72
3.3.4.4.3	Élimination de Gauss	73
3.3.5	Autres méthodes de factorisation	73
3.4	Extraction du logarithme discret	73
4	Encryptage par clés publiques	75
4.1	Méthode de Diffie-Hellman (DH)	75
4.1.1	DH : Comment ça marche	75
4.1.2	DH : Les pièges et les solutions	76
4.2	Méthode de Elgamal	78
4.2.1	Elgamal : Comment ça marche	79
4.3	Méthode de Rivest Shamir Adleman (RSA)	79
4.3.1	RSA : Comment ça marche	79
4.3.2	RSA : Questions variées	81
4.3.2.1	Multiples de p et q	82
4.3.2.2	Encryptage et décryptage de 0, 1 et $(n - 1)$	83
4.3.2.3	Utilisation de $\phi(n)$, $\lambda(n)$ et $PPCM(p - 1, q - 1)$	83
4.3.2.4	Comment forme-t-on le message m ?	84
4.3.2.5	Choix de e	84
4.3.3	RSA : Signature électronique	86
4.3.4	RSA : Les attaques possibles	86
4.3.4.1	Factorisation du nombre n	87

4.3.4.2	Méthode du délai et autres attaques " latérales "	87
4.3.4.3	Les petits e et les petits m	88
4.3.5	RSA: Méthodes de protection	88
4.4	Méthodes à courbes elliptiques	89
4.4.1	Adaptation de la méthode Diffie-Hellman	89
4.4.2	Adaptation de la méthode Elgamal	89
4.4.3	Adaptation de la méthode Rivest Shamir Adleman (RSA)	90
A	Groupes et corps de Galois	91
B	Preuves de formules diverses	93
B.1	Calcul des combinaisons	93
B.2	Formule du binôme de Newton	93
B.3	Puissance du nombre premier p dans le nombre $N!$	95
C	Systèmes et bibliothèques de calcul de grands nombres	97
C.1	GMP	97
C.2	PARI/GP	98
C.3	Python	99
C.4	bc	99
C.5	C#: BigInteger Class	99
C.6	Big Integers in JavaScript	100
C.7	GiantInt - cross-platform C code	100
C.8	Big/Giant number package - Giant Numbers in Forth	100
C.9	java.math.BigInteger	100
D	Systèmes et bibliothèques de cryptographie	101
D.1	Crypto++	101
D.2	Apache Milagro	103
D.3	Bouncy Castle	104
	Bibliographie	112
	Index	112

Fascicule 2: Grands nombres et calculs rapides

1	Grands nombres et calculs efficaces	1
1.1	Représentation des très grands nombres	1
1.2	Calcul efficace du PGCD	2
1.2.1	Calcul binaire du PGCD	2
1.2.2	Calcul du PGCD de Lehmer	3
1.3	Méthodes efficaces de multiplication	3
1.3.1	Multiplication de Karatsuba-Ofman	3
1.3.2	Multiplication de Toom-Cook	6
1.3.3	Méthode de Schönhage-Strassen	6
1.3.4	Multiplication par transformée de Fourier rapide (FFT) .	6
1.3.5	Multiplication par transformée de la théorie des nombres (NTT)	6
1.4	Multiplication et exponentiation de Montgomery	7
	Bibliographie	17
	Index	17

Fascicule 3: Télématique et sécurité

1	Concepts de sécurité en télématique	3
1.1	Authentification des partis	3
1.2	Confidentialité des échanges	4
1.3	Intégrité des données	4
2	La sécurité à la couche liaison: 802.11i	5
2.1	Motivations	5
2.2	IEEE 802.11 (WiFi)	5
2.2.1	Description des trames 802.11	6
2.2.1.1	Trames de contrôle	7
2.2.1.2	Trames de gestion	8
2.2.1.3	Trames de données	10
2.2.2	Protocole d'association	10
2.3	Sécurité	11
2.3.1	WEP	11
2.3.2	IEEE 802.1X	13
2.3.3	IEEE 802.11i	15
2.3.3.1	WPA	15
2.3.3.2	WPA2	16
2.3.4	WPA3	18
2.3.5	WPS	18
2.4	Cryptanalyse du réseau sans-fil	18
2.4.1	SSID caché	19
2.4.2	Filtrage d'adresses MAC	19
2.4.3	WEP	19
2.4.3.1	Bombardement ARP	20
2.4.4	WPA2	20
2.4.5	WPS	20
3	La sécurité à la couche de réseau: IPSec	21
3.1	Architecture	21
3.1.1	Bases de données	21
3.2	IKEv2	22
3.2.1	Modes de protection	22
3.2.2	Établissement des associations	22
3.3	ESP	24
3.4	AH	25
4	La sécurité à la couche de transport: TLS	27
4.1	Historique	27
4.1.1	SSLv1	29
4.1.2	SSLv2	29
4.1.3	SSLv3	30
4.1.4	TLSv1.0	31

4.1.5	TLSv1.1	33
4.1.6	TLSv1.2	33
4.1.7	TLSv1.3	34
4.1.7.1	Amélioration de la sécurité de TLS	34
4.1.7.2	Amélioration de la performance de TLS	35
4.1.8	DTLS	35
4.1.9	DTLSv1.2	36
4.2	Description du protocole TLS	36
4.2.1	Protocole de message	36
4.2.2	Protocole de négociation	36
4.2.3	Protocole d'alerte	38
4.2.4	Protocole de changement de chiffrement	38
4.2.5	Protocole de données d'application	38
4.3	L'utilisation du protocole	39
4.3.1	La négociation de base	39
4.3.2	La génération des clefs	39
4.3.3	La fermeture d'une connexion TLS	42
4.3.4	Modes avancés de TLS	42
4.3.5	L'authentification du client	42
4.3.6	La réutilisation d'une session	43
4.3.7	Le mode éphémère	44
4.3.8	Protocole de négociation TLS 1.3	45
4.3.8.1	Messages d'échange de clé	46
4.3.8.2	Extensions	47
4.3.8.3	Messages des paramètres du serveur	47
4.3.8.4	Messages d'authentification	47
4.4	Les réseaux privés virtuels TLS	47
5	La sécurité la couche d'application	51
5.1	DNS	51
5.1.1	Architecture	51
5.1.2	Attaques communes	54
5.1.2.1	Empoisonnement de cache	54
5.1.2.2	Attaque par amplification	55
5.1.3	DNSSEC	56
5.1.4	DNS over TLS	58
5.1.5	RPZ	58
5.1.6	DNS over HTTPS	59
5.1.7	TSIG	59
5.1.8	Cookies de requêtes	59
6	Le déploiement de la sécurité	61
6.1	L'infrastructure à clef publique	61
6.1.1	Les systèmes de chiffrement à clef publique	61
6.1.2	L'infrastructure à clef publique	62
6.1.2.1	Composantes	62

6.1.3	Le certificat X.509	63
6.1.3.1	Les extensions	64
6.1.3.2	Émission d'un certificat	65
6.1.3.3	Validation d'un certificat	66
6.1.3.4	Révocation d'un certificat	67
6.2	DNSSEC	67
Bibliographie		75
Index		75

Fascicule 4: Cyberattaques et contre-mesures

1	Cyberattaques	1
1.1	Motivations	1
1.2	Phases d'opération	2
1.2.1	Reconnaissance	2
1.2.2	Intrusion	3
1.2.3	Exploitation	3
1.2.4	Effacement	4
1.3	Guerre cybernétique	4
1.3.1	Tensions latentes	4
1.3.2	Mobilisation	5
2	Techniques de reconnaissance	7
2.1	Reconnaissance passive	7
2.2	Reconnaissance active	7
2.2.1	Reconnaissance réseau	7
2.2.1.1	Nmap	8
2.2.1.2	Wireshark et Airpcap	13
2.2.1.3	Snort et airsnort	14
2.2.1.4	Pare-feux	14
2.2.2	Ingénierie sociale	14
3	Techniques d'intrusion	15
3.1	Dépassement de tampons	15
3.2	Subversion	15
3.3	Systèmes d'intrusion	16
3.3.1	Nessus	16
3.3.2	Metasploit	16
3.3.3	Tor	16
4	Techniques d'exploitation	17
4.1	Réseau de zombies	17
4.2	Rootkits	18
4.3	Pots de miel	18
4.4	Récupération de données confidentielles	18
5	Techniques d'effacement	19
5.1	Volatilité de l'information	19
5.2	systèmes de fichiers	19
5.3	Récupération des fichiers effacés	19
	Bibliographie	22
	Index	22

Fascicule 5: Calcul de résumés (hachage)

1	Validation des données	1
1.1	Résumé MD5	1
1.2	Résumé SHA	2
1.2.1	SHA-1	2
1.2.2	SHA-2	2
1.2.3	SHA-3	2
1.3	Résumé Blake3	2
	Bibliographie	3
	Index	3

Fascicule 6: Nombres aléatoires et pseudo-aléatoires

1	Génération de nombres aléatoires et pseudo-aléatoires	1
1.1	Principes de base	2
1.2	Générateurs sans source d'entropie externe	3
1.2.1	LFSR	3
1.2.1.1	A5/1	3
1.2.1.2	Générateur par rétrécissement	3
1.2.2	L'algorithme de Blum,Blum et Shub	3
1.2.3	Mersenne Twister	3
1.3	Générateurs avec source d'entropie externe	3
1.3.1	Fortuna	3
1.3.2	Systèmes basés sur l'incertitude quantique	3
1.3.3	Le Système Bull Mountain de Intel	4
	Bibliographie	6
	Index	6

Fascicule 7: Techniques d'authentification

1	Authentification	1
1.1	Authentification	1
1.1.1	Mots de passes	1
1.1.1.1	Tables arc-en-ciel (Rainbow tables)	1
1.1.1.2	Signatures numériques	1
1.1.2	Preuves à divulgation nulle de connaissance	1
1.1.2.1	Tentatives d'attaques	4
1.1.2.2	Le système Feige-Fiat-Shamir	5
1.1.2.3	Le système Guillou-Quisquater GQ2	5
	Bibliographie	8
	Index	8

Fascicule 8: Cryptographie quantique et impact classique

1	Cryptographie quantique	1
2	Systèmes quantiques existants	3
	Bibliographie	5
	Index	5