

TABLE DES MATIÈRES

1. Arithmétique des entiers et complexité	1
1.1. Rappels sur l'arithmétique des entiers	1
1.1.1. Structure d'anneau euclidien	1
1.1.2. Idéaux	2
1.1.3. Divisibilité, plus grand diviseur commun, identité de Bézout	3
1.1.4. Factorisation unique	5
1.1.5. L'algorithme d'Euclide étendu	6
1.2. Quelques notions de complexité	8
1.2.1. Écriture d'un entier en base b	8
1.2.2. La taille d'un entier en informatique	10
1.2.3. Opérations élémentaires sur les bits et opérations arithmétiques sur les entiers	10
1.2.4. Complexité d'un algorithme arithmétique sur les entiers	11
1.2.5. Le problème de la factorisation	13
1.3. Deux algorithmes performants	14
1.3.1. Exponentiation rapide	14
1.3.2. Extraction de la racine carrée d'un entier	14
2. Protocoles reposant sur le problème de la factorisation	17
2.1. Arithmétique modulaire	17
2.1.1. Le groupe $\mathbb{Z}/n\mathbb{Z}$	17
2.1.2. Groupes cycliques	18
2.1.3. L'anneau $\mathbb{Z}/n\mathbb{Z}$	18
2.1.4. Le théorème des restes chinois	19
2.1.5. Le groupe $(\mathbb{Z}/n\mathbb{Z})^\times$ et la fonction indicatrice d'Euler	21
2.2. Le cryptosystème RSA	24
2.2.1. Cryptosystèmes à clé publique	24
2.2.2. Principe du protocole	25
2.2.3. Signature	26
2.2.4. Cryptanalyse	26

2.3. Symbole de Legendre et carrés dans $\mathbb{Z}/n\mathbb{Z}$	29
2.3.1. Le symbole de Legendre.....	29
2.3.2. Extraction de racines carrées dans $\mathbb{F}_p$	31
2.3.3. Carrés dans $\mathbb{Z}/n\mathbb{Z}$	31
2.4. Applications cryptographiques.....	33
2.4.1. Le cryptosystème de Rabin.....	33
2.4.2. Le protocole de Goldwasser-Micali.....	33
2.4.3. Alice et Bob jouent à pile ou face.....	33
2.5. Complément : réciprocity quadratique et symbole de Jacobi.....	34
2.5.1. La loi de réciprocity quadratique.....	34
2.5.2. Le symbole de Jacobi.....	36
2.5.3. Calcul explicite du symbole de Jacobi.....	38
3. Corps finis et logarithme discret.....	41
3.1. Rappels sur les polynômes à coefficients dans un corps.....	41
3.1.1. Structure d'anneau euclidien et propriétés arithmétiques.....	41
3.1.2. Racines et divisibilité.....	43
3.1.3. Séparabilité, le polynôme dérivé.....	44
3.2. Extensions de corps.....	44
3.2.1. Extensions de corps.....	44
3.2.2. Construction explicite d'extensions finies.....	44
3.2.3. Éléments algébriques, polynôme minimal.....	46
3.3. Corps finis.....	47
3.3.1. Caractéristique, sous-corps premier.....	47
3.3.2. Cardinal et degré.....	47
3.3.3. Le groupe multiplicatif d'un corps fini.....	48
3.3.4. L'automorphisme de Frobenius.....	50
3.3.5. Existence et unicité.....	52
3.4. Corps finis – aspect cryptographique.....	54
3.4.1. Complexité des opérations algébriques dans un corps fini.....	54
3.4.2. Le problème du logarithme discret.....	55
3.4.3. Le cryptosystème El Gamal.....	56
3.4.4. Le protocole de Diffie-Hellman.....	57
3.4.5. Protocoles de secret réparti.....	57
3.4.6. La méthode des trois échanges.....	59
3.5. Complément : attaques du problème du logarithme discret.....	60
3.5.1. Le calcul d'indice.....	60
3.5.2. L'algorithme Baby step - Giant step.....	61
A. Rappels d'algèbre.....	63
A.1. Ensembles.....	63
A.1.1. Notations.....	63
A.1.2. Relations.....	63
A.1.3. Relations d'ordre.....	64
A.1.4. Relations d'équivalence.....	64

A.2. Groupes abéliens.....	64
A.2.1. Définitions et premières propriétés.....	64
A.2.2. Sous-groupes, groupes quotient.....	66
A.2.3. Parties génératrices, groupes finiment engendrés.....	67
A.2.4. Le théorème de Lagrange.....	67
A.2.5. Homomorphismes.....	68
A.3. Anneaux.....	69
A.3.1. Anneaux et sous-anneaux.....	69
A.3.2. Idéaux et anneaux quotient.....	70
A.3.3. Homomorphismes.....	71
A.3.4. Éléments réguliers, inversibles et diviseurs de zéro.....	73
A.3.5. Idéaux premiers et maximaux.....	74