Sous-groupes cycliques du Groupe Symétrique

et

Cryptographie

INTRODUCTION

L'objet de ce livre a pour but de présenter des techniques de cryptographie qui ont pour particularité d'avoir pour fondement mathématique divers résultats concernant les sous-groupes cycliques du groupe symétrique.

Le domaine technique de ces procédés de cryptographie est spécifiquement celui des procédés de chiffrement à clé secrète (cryptosystèmes symétriques) .Dans le détail les procédés cryptographiques objet de ce livre concernent des procédés de chiffrement d'un message ou d'une donnée à l'aide d'une clé secrète ainsi que l'authentification . Ils consistent en un dispositif qui utilisé dans ces différents systèmes cryptographiques symétriques permet que la clé secrète de chiffrement soit modifiable de manière publique pour chaque message chiffré ou , dans le cas de l'authentification , que la personne vérificatrice de l'identité d'une autre par un procédé de cryptographie symétrique , lors par exemple d'un protocole d'authentification par défi-réponse , n'ait pas à détenir la clé secrète de celle-ci. Selon un autre mode d'utilisation du dispositif ces techniques sont des procédés de chiffrement symétrique dans lequel la clé de chiffrement est un « carré latin » (systèmes de chiffrement symétrique associé à un carré latin donné L) .

Procédés de chiffrement symétriques. Les procédés de chiffrement symétrique ayant vocation à utiliser et intégrer le dispositif en question sont ceux qui utilisent comme clé secrète une suite aléatoire de symboles ou une permutation des symboles d'un ensemble E donné . Un exemple est le cas du masque de Vernam . Un message est donné sous forme de lettres de l'alphabet , la clé est aussi une suite de lettres aléatoires de même longueur que le message. Le chiffrement s'opère en additionnant modulo 26 les numéros d'ordre des lettres de l'alphabet : par exemple si la lettre en clair est H , de rang 7 , et clé le W de rang 22 , le chiffre est alors la lettre de rang 22 + 7 = 29 modulo 26 , soit 3 , donc la lettre D.
Un autre exemple , variante du masque de Vernam , est le chiffre XOR : un message M est donné sous forme de suite de bits , la clé K est une suite de bits aléatoire de même longueur que le message , le chiffrement s'opère en additionnant bit à bit selon la fonction XOR les bits de M et K.
Pour ce qui est des clés sous forme de permutation des symboles d'un ensemble E donné on peut citer le chiffrement en mode ECB (Electronic Code Book) qui permute un message de n bits par une permutation des n premiers entiers (une fonction de permutation) , cette permutation constituant la clé K : par exemple si K = (4 5 3 1 2) , permutation de E = {1,2,3,4,5} , et M = 10101 , alors le chiffre C de M est C = 01110 (en première position dans le cryptogramme C le bit de rang 4 de M , en seconde le bit de rang 5 de M , etc).

Les procédés cryptographiques objet de ce livre concernent donc spécifiquement des procédés symétriques de chiffrement qui reposent sur ce type de clés .Les cryptosystèmes qui ont été cités ci-dessus sont les plus simples mais le dispositif peut être intégré à des systèmes plus complexes. Ce type de clé permet aussi par ailleurs l'authentification par défi-réponse et un système de chiffrement par carré latin.

Authentification. Concernant le cas de l'authentification par défi-réponse le schéma général est le suivant : A et B possèdent une clé secrète de chiffrement K . A , « le solliciteur » veut s'identifier auprès de B qui est « le vérificateur ». B lui propose de relever un défi : chiffrer à l'aide de la clé secrète K qu'ils partagent une donnée **x** selon un procédé de chiffrement de donnée convenu à

l'avance . Si A chiffre correctement **x** cela prouve qu'il est en possession de K , ce qui l'authentifie.

Le procédé d'authentification décrit dans ce livre concerne spécifiquement une situation où un grand nombre de solliciteurs s'authentifient auprès d'un vérificateur unique . Chaque solliciteur possédant une clé secrète personnelle unique. C'est par exemple le cas de l'authentification d'une carte bancaire lors d'un paiement chez un commerçant à l'aide d'un terminal de paiement électronique (TPE) . Une authentification à distance de la carte bancaire peut être effectuée (en général pour des paiements d'un montant élevé). Cette authentification à distance est menée à l'aide d'un procédé de cryptographie symétrique utilisant un protocole « défi/réponse ».
La technique connue est la suivante : une clé secrète **k** est inscrite dans la mémoire de la puce dans sa partie illisible. Lors du paiement le terminal interroge un centre de contrôle à distance qui envoie à la carte une valeur aléatoire x . La carte calcule alors **y = *f* (k,x)** où *f* est un algorithme de calcul symétrique utilisant la clé secrète **k.** La valeur **y** , qui est le chiffre de x avec la clé **k** , est transmise au centre de contrôle qui lui-même calcule la valeur ***f* (k,x)** à l'aide de **k** qu'il détient aussi . S'il retrouve **y** cela prouve que la carte détient la clé secrète **k .** Ce qui authentifie la carte de paiement. Dans ce procédé d'authentification il est nécessaire cependant que le centre de contrôle détienne les clés secrètes **k** de toutes les cartes puisque le système cryptographique est symétrique.

Les techniques de cryptographie basées sur les sous-groupes cycliques du Groupe Symétrique permettent que le contrôleur central n'ait pas à détenir la clé secrète de chaque solliciteur , cela bien que le système soit symétrique. Chaque clé secrète et personnelle étant associée à une « information publique » , appelée clé publique, permettant au vérificateur de procéder aux calculs de vérification .

Chiffrement par carré latin . Un cas particulier d'utilisation des sous-groupes cycliques du Groupe Symétrique est celui du chiffrement par carré latin (dit aussi “cryptosystème associé à un carré latin donné L”). Un carré latin est toujours défini dans les manuels et la littérature mathématique comme un tableau ou une matrice composé de n lignes et n colonnes (carré latin d'ordre n) dans lequel chaque ligne et chaque colonne ne contiennent qu'une seule fois le même symbole , par exemple :

4	**3**	**1**	**2**
2	**1**	**4**	**3**
3	**4**	**2**	**1**
1	**2**	**3**	**4**

On peut citer comme référence documentaire , par exemple : Douglas Stinson , “Cryptographie , théorie et pratique” , 2ème édition , Vuibert , page 68 exercice 2.2 .

Le “chiffrement associé à un carré latin L” est en général défini dans les manuels par une fonction qui associe au symbole i du message , de rang j dans M, le symbole du carré latin figurant “colonne i , ligne j” , noté par exemple a_{ij} , ou L(i,j) .

Par exemple si L est le carré latin défini ci-dessus , pour des messages et cryptogrammes dont l'alphabet est {1,2,3,4} on chiffre M = 42 par **21** (chiffre de 4 = élément du carré en colonne 4 , ligne 1; chiffre de 2 = élément du carré colonne 2 ligne 2). Dans de tels cryptosystèmes la clé secrète de chiffrement est donc un carré latin choisi de manière aléatoire et cette clé est toujours définie et présentée comme un “tableau” , ou “matrice” que l'on doit visualiser pour pouvoir chiffrer. La fonction de chiffrement E est définie par référence à la matrice L : $E(i_j) = L(i,j)$. Il est

donc toujours nécessaire dans l'état de la technique existante que la clé de chiffrement soit donnée sous forme de matrice ou tableau visuel.

90 La technique de chiffrement par carré latin donnée dans ce livre permet que le carré latin ne soit plus donné sous forme de matrice à visualiser pour chiffrer et déchiffrer.

On aborde maintenant la description détaillée de ces cryptosystèmes.

PLAN

L'objet de ce livre ayant pour but de présenter des techniques de cryptographie qui ont pour particularité d'avoir pour fondement mathématique les sous-groupes cycliques du groupe symétrique il comportera trois parties .

Une partie I exposant les principes généraux et les résultats les plus communs concernant la théorie des sous-groupes cycliques du groupe symétrique.

Une partie II donnant quelques prolongements de cette théorie , prolongements spécifiques aux procédés de cryptographie objets de ce livre.

Une partie III exposant les techniques et procédés de cryptographie objet de ce livre.

Le plan détaillé du livre étant le suivant :

Partie I : MATHEMATIQUES : SOUS-GROUPES CYCLIQUES DU GROUPE SYMETRIQUE .

- § 1 - Notion de sous-groupe cyclique du groupe symétrique
- § 2 - Résultats généraux sur les sous-groupes cycliques du groupe symétrique

Partie II : PROLONGEMENTS .

- § 1 - Groupe symétrique d'un ensemble E
- § 2- Cycle d'une permutation
- § 3 - Sous-groupes cycliques de permutations
- § 4- Calcul de p^j dans G
- § 5- w-uplet du produit cartésien des disjoints d'une permutation
- § 6- Algorithme $\{p^a\} \rightarrow \lambda$
- §7- Couples de solutions d'une composition de deux bijections où les deux composantes sont inconnues
- § 8 - Formule de permutation d'une suite de symboles
- § 9- Sous-groupes cycliques du groupe symétrique et Carré Latin .

Partie III : CRYPTOGRAPHIE .

- § 1 – Procédé de chiffrement symétrique utilisant l'algorithme $\{p^a\} \rightarrow p^j$
- § 2 – Procédé de chiffrement symétrique utilisant l'algorithme $\{p^a\} \rightarrow \lambda$
- § 3 – Procédé d'authentification
- § 4 – Authentification de documents
- §5 – Chiffrement par carré latin

PARTIE I - MATHEMATIQUES : SOUS-GROUPES CYCLIQUES DU GROUPE SYMETRIQUE

Cette partie énonce les notions mathématiques à connaître pour comprendre les cryptosystèmes qui en dérivent et qui feront l'objet de ce livre en partie III.

§ 1 - Notion de sous-groupe cyclique du groupe symétrique

Soit E un ensemble fini d'éléments totalement ordonné.

On note S(E) , ou Se , le groupe symétrique de E qui est l'ensemble des bijections de E dans E muni de la loi de composition de fonctions notée o. Se muni de l'opération de composition de fonction possède une structure algébrique de groupe . On ne démontre pas ce résultat qui est connu.

L'ensemble des bijections de E dans E est aussi l'ensemble des permutations des éléments de E. Dans la suite bijection et permutation ne seront donc plus distinguées et la notation "*p*" désignera aussi bien la bijection que la permutation.

Soit *p* une bijection de E dans E .

Le Sous-Groupe cyclique **G** du groupe symétrique Se de E généré par *p* est l'ensemble des permutations $\{ p , p^2 , ... p^j,...,p^{\mathbf{a}} \}$, où $p^1 = p$, $p^2 = p \circ p$, $p^3 = p \circ p \circ p$, etc . . L'entier **a** est le ppcm des entiers représentant la longueur des cycles de *p*.

Exemple:

Soit $p = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 6 & 9 & 1 & 4 & 3 & 5 & 2 & 8 \end{pmatrix}$ une permutation de E , avec E = {1,2,3,4,5,6,7,8,9} muni de l'ordre standard des entiers naturels.

Les petits numéros au dessus de *p* sont les numéros d'ordre de chaque élément de *p* (en première position le 7 , en seconde le 6 etc.) . La suite 1 2 3 4 5 6 7 8 9 constitue donc l'ordre de E , au sens de relation d'ordre , qui est ici l'ordre standard des entiers naturels. Quand la permutation est écrite avec noté au-dessus de ses éléments leur numéro d'ordre on dit parfois qu'elle est écrite sous forme de matrice.

La bijection de E dans E associée à cette permutation est donc :

p(1) = 7
p(2) = 6
p(3) = 9
p(4) = 1
p(5) = 4
p(6) = 3
p(7) = 5
p(8) = 2
p(9) = 8

Le cycle d'une permutation p appartenant à S_e , pour un élément i de cette permutation, est la suite

(i , e_1 , e_2 , ….., $p^{h-1}(i)$) , telle que : $p^1(i) = e_1$, $p^2(i) = e_2$, ….., $p^h(i) = i$, où :

- p est la bijection de E dans E associée à la permutation S.
- p^n , pour un n quelconque , est la bijection p o p o....o p , o étant l'opération de composition de fonction itérée n-1 fois.
- h est le plus petit entier tel que $p^h(i) = i$, l'entier h étant appelé la longueur du cycle

L'élément i peut être placé au début du cycle comme à la fin , et chaque élément du cycle peut être choisi comme premier élément.

Le « cycle d'une permutation » est un concept identique à celui de « cycle d'une bijection » .La littérature mathématique appelle aussi parfois les cycles d'une permutation des « orbites » (orbite de l'élément i selon p) , ou « disjoints » du fait qu'ils opèrent une partition de E en ensembles disjoints. Ici on les appellera indifférement« cycles » , ou « disjoints » .

On peut vérifier que la permutation p ci-dessus possède deux cycles (disjoints) de longueur 4 et 5 qui sont :

(1 7 5 4) puisque $p^1(1)= 7$, $p^2(1) = \mathbf{5}$, $p^3(1) = \mathbf{4}$, $p^4(1) = \mathbf{1}$

(2 6 3 9 8) puisque $p^1(2)= \mathbf{6}$, $p^2(2) = \mathbf{3}$, $p^3(2) = \mathbf{9}$, $p^4(2) = \mathbf{8}$, $p^5(2) = \mathbf{2}$

La bijection p engendre donc le sous-groupe cyclique **G** de bijections de S_e suivant qui possède 20 éléments puisque ppcm(4,5) = 20 .

(On écrit **G** sous forme de tableau où chaque permutation p^j appartenant à **G** est une ligne du tableau).

G =

	1	2	3	4	5	6	7	8	9
p =	7	6	9	1	4	3	5	2	8
p^2 =	5	3	8	7	1	9	4	6	2
p^3 =	4	9	2	5	7	8	1	3	6
p^4 =	1	8	6	4	5	2	7	9	3
p^5 =	7	2	3	1	4	6	5	8	9
p^6 =	5	6	9	7	1	3	4	2	8
p^7 =	4	3	8	5	7	9	1	6	2
p^8 =	1	9	2	4	5	8	7	3	6
p^9 =	7	8	6	1	4	2	5	9	3
p^{10} =	5	2	3	7	1	6	4	8	9
p^{11} =	4	6	9	5	7	3	1	2	8

p^2 = (5 3 8 7 1 9 4 6 2) = p o p

p^3 = (4 9 2 5 7 8 1 3 6) = p o p o p

p^4 = (1 8 6 4 5 2 7 9 3) etc,