Thème : Quelques applications des congruences

Activité 7. Chiffrement de Hill et chiffrement RSA

Exercice 1 : *Le chiffrement de Hill*

Prérequis : Congruences – Opérations sur les matrices – Connaissances sur les tableurs.

Objectif : Montrer un exemple de chiffrement à clé privée qui résiste à l'analyse fréquentielle.

L'étude de la fréquence d'apparition de certaines lettres permet aisément de trouver des correspondances et de déchiffrer les messages. Il fallut alors construire des chiffrements dans lesquels une même lettre était chiffrée différemment selon son emplacement dans le message. De tels chiffrements modifient les fréquences des lettres chiffrées par rapports à celles des lettres en clair. Ainsi, *Lester Hill*, mathématicien cryptographe américain (1891-1961) publie en 1929 un article où il détaille un nouveau chiffrement. Son idée est de continuer à utiliser des décalages, mais en effectuant ces décalages simultanément sur des groupes de *m* lettres. Bien sûr, plus *m* est grand, plus le déchiffrement est difficile !

Le principe du chiffrement de Hill est le suivant :
On numérote de 0 à 25 et dans l'ordre alphabétique les 26 lettres de l'alphabet français.
On fixe une valeur de m. Dans cette activité on prendra $m = 2$, c'est-à-dire qu'on découpera les mots en couples de 2 lettres en clair $(L_1\ ;\ L_2)$, $(L_3\ ;\ L_4)$, $(L_5\ ;\ L_6)$ etc.

- On se donne une matrice carrée $A = \begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{pmatrix}$.
- Une matrice colonne $U = \begin{pmatrix} n_1 \\ n_2 \end{pmatrix}$ contient les rangs du couple de lettres $(L_1\ ;\ L_2)$ en clair.
- On obtient la matrice $V = \begin{pmatrix} p_1 \\ p_2 \end{pmatrix}$ en faisant le produit matriciel $V = A \times U$.
- On obtient la matrice $W = \begin{pmatrix} n'_1 \\ n'_2 \end{pmatrix}$ où n'_1 et n'_2 sont les restes de la division euclidienne respectivement de p_1 et p_2 par 26.
- Les nombres n'_1 et n'_2 représentent alors les rangs d'un couple de lettres $(L'_1\ ;\ L'_2)$ chiffrées.

En associant le couple $(L'_1\ ;\ L'_2)$ à $(L_1\ ;\ L_2)$, on effectue le chiffrement de Hill défini par la matrice $\begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{pmatrix}$.
La matrice $\begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{pmatrix}$ est la *clé secrète* du chiffrement de Hill. Elle n'est connue que de l'expéditeur et du destinataire.

Partie A : *Chiffrement*

On utilise la clé de chiffrement $A = \begin{pmatrix} 3 & 5 \\ 6 & 11 \end{pmatrix}$.

1) Faire le tableau des rangs *n* des vingt-six lettres de l'alphabet puis chiffrer le mot « CD ».
2) Chiffrer ensuite le mot « AX ».
3) Peut-on dire que, dans le chiffrement de Hill, deux lettres distinctes sont chiffrées par deux lettres distinctes ?
4) On utilise un tableur pour chiffrer et déchiffrer plus rapidement. Réaliser le tableau ci-dessous en utilisant les fonctions du tableur **CODE, MOD, CAR**. Les valeurs des éléments de la matrice $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$ doivent pouvoir être changées dans les cellules C1, E1, C2 et E2 et le tableau être recalculé automatiquement.

	A	B	C	D	E	F	G
1	Clé	$a\,11=$	3	$a\,12=$	5		
2		$a\,21=$	6	$a\,22=$	11		
3	Couples de Lettres en clair	A	C	E	G	I	K
4		B	D	F	H	J	L
5	Rang $n\,1$	0	2	4	6	8	10
6	Rang $n\,2$	1	3	5	7	9	11
7	$p\,1$	5	21	37	53	69	85
8	$p\,2$	11	45	79	113	147	181
9	Rang $n'1$	5	21	11	1	17	7
10	Rang $n'2$	11	19	1	9	17	25
11	Couples de lettres chiffrées	**F**	**V**	**L**	**B**	**R**	**H**
12		**L**	**T**	**B**	**J**	**R**	**Z**

- **CODE** renvoie le rang du caractère.

=CODE(B3) affiche le rang du caractère situé en B3. Attention : dans le jeu de caractères informatiques, la lettre A majuscule a le rang 65. Dans notre cas, il faudra donc utiliser =CODE(B3)-65 pour que A ait le rang 0.

- **MOD** renvoie le reste d'une division.

=MOD(B7;26) renvoie le reste de la division de l'entier présent en B7 par 26.

- **CAR** renvoie le caractère spécifié par un rang.

=CAR(65) affiche le caractère de rang 65 du jeu de caractères c'est-à-dire A. Dans notre cas, il faudra donc utiliser =CAR(B9+65) pour afficher le caractère correspondant au rang présent en B9.

A l'aide de cette feuille de calcul, chiffrer le mot « NOMBRE ».

Partie B : *Déchiffrement*

On reçoit le message chiffré « **FYPFTQ** » et on connait la clé de chiffrement $A = \begin{pmatrix} 3 & 5 \\ 6 & 11 \end{pmatrix}$ qui a été utilisée pour le chiffrer.

1) Donner les trois matrices $W_1 = \begin{pmatrix} n'_1 \\ n'_2 \end{pmatrix}$ $W_2 = \begin{pmatrix} n'_3 \\ n'_4 \end{pmatrix}$ et $W_3 = \begin{pmatrix} n'_5 \\ n'_6 \end{pmatrix}$ qui contiennent les rangs des lettres du message chiffré.

2) On veut, à partir des matrices W_1, W_2, W_3 retrouver les matrices $U_1 = \begin{pmatrix} n_1 \\ n_2 \end{pmatrix}$, $U_2 = \begin{pmatrix} n_3 \\ n_4 \end{pmatrix}$ et $U_3 = \begin{pmatrix} n_5 \\ n_6 \end{pmatrix}$ des rangs des lettres du message en clair correspondant.

   a) Soit la matrice $C = \begin{pmatrix} 11 & -5 \\ -6 & 3 \end{pmatrix}$. Calculer le produit $C \times A$.

   b) En déduire que la matrice A est inversible.

   c) On appelle A^{-1} la matrice inverse de A. Calculer A^{-1}

   d) Calculer les produits $A^{-1} \times W_1$, $A^{-1} \times W_2$ et $A^{-1} \times W_3$.

   e) L'utilisation de la clé A^{-1} permet-elle de déchiffrer le message « **FYPFTQ** » ?

3) Vérifier que l'utilisation de la clé $9C$ permet de déchiffrer le message « **FYPFTQ** ».

4) La clé $9C$ permet-elle de déchiffrer tous les messages qui ont été chiffrés avec la clé A ?

5) Déchiffrer le message « **MPYORQZL** ».

Exercice 2 : *Le chiffrement RSA*

Prérequis : Congruences

Objectif : Montrer un exemple de chiffrement à clé publique.

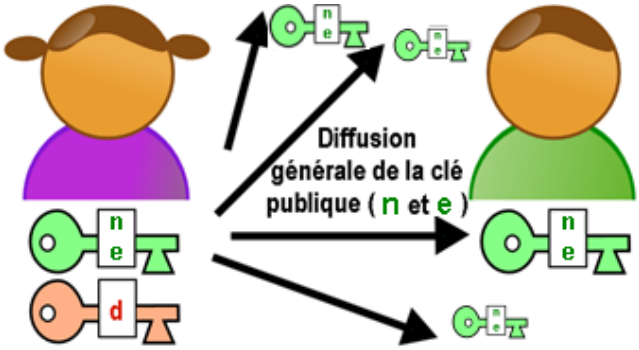
Origine

- Les initiales des noms des inventeurs ont donné l'acronyme RSA : **R**ivest, **S**hamir, **A**dleman.
- En 1978, le principe du système RSA est publié dans la revue « Association for Computing Machinery ».

Principe

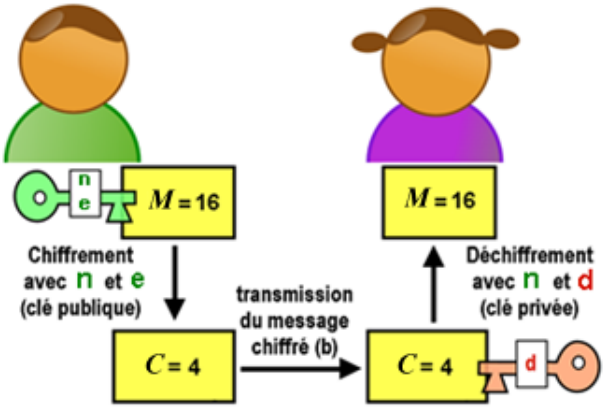
Bob souhaite transmettre un message confidentiel à Alice. Le principe est expliqué sur un exemple (en rouge ce qui est secret, en vert ce qui est public).

1ère étape : Construction d'une clé publique $(n\ ;\ e)$ et d'une clé privée $(n\ ;\ d)$ par Alice



- Alice choisit au hasard deux nombres premiers p et q qu'elle garde secrets.
  Exemple : $p = 3$ et $q = 11$.
- Elle calcule $n = p \times q$ et $m = (p-1)(q-1)$
  Exemple : $n = 33 \quad m = 2 \times 10 = 20$.
- Elle choisit un entier e (l'exposant de chiffrement) **premier avec m** et **compris entre 1 et m**.
  Exemple : $e = 3$.
- Elle calcule un exposant de **d**échiffrement d (qui est un inverse de e modulo m). C'est sa clé privée qu'elle garde secrète. **Exemple :** $d = 7$ car $7 \times 3 \equiv 1 \quad (20)$.
- Elle publie la clé publique (n, e) qu'elle envoie à Bob ainsi qu'à d'autres correspondants éventuels.

2ème étape : Chiffrement par Bob



- Bob veut envoyer à Alice la lettre P en clair, codée par le code en clair $M_i = 16$ (rang dans l'alphabet).
- Il utilise l'algorithme de chiffrement :
  $M_i \longmapsto C_i$ tel que $C_i \equiv {M_i}^3 \quad (n)$ avec $0 \leq C_i < n$.
  Exemple : $16^3 \equiv 4 \quad (33)$ donc $C_i = 4$.

3ème étape : Déchiffrement par Alice

- Alice reçoit le code chiffré $C_i = 4$.
- Elle utilise l'algorithme de déchiffrement qui a besoin de sa clé privée $(n\ ;\ d)$:
  $C_i \longmapsto M_i$ tel que $M_i \equiv {C_i}^d \quad (n)$ avec $0 \leq M_i < n$.
  Exemple : $4^7 \equiv 16 \quad (33)$ donc $M_i = 16$.
- Alice trouve bien $M_i = 16$ qui est le code de la lettre en clair P de Bob. C'est la seule à pouvoir déchiffrer puisqu'elle est la seule à connaitre $d = 7$, un inverse de $e = 3$ modulo $m = 20$.

Sécurité et intérêt

La sécurité repose sur la rapidité à calculer le produit $pq = n$ de deux nombres premiers très grands, alors qu'il est très long de factoriser n en produit $p \times q$ qui, seuls, permettent de calculer $m = (p-1)(q-1)$. Connaitre l'exposant de déchiffrement d nécessite de connaitre m. Son grand avantage par rapport à un chiffrement à clé secrète est qu'il est inutile d'envoyer aux correspondants une clé de façon confidentielle.

Un exemple

Partie A : Alice décide de choisir $(n\ ;\ e) = (21\ ;\ 5)$ comme clé publique.

1) a) Peut-elle faire ce choix ?
   b) Expliquer pourquoi ce choix de clé publique ne garantit pas la sécurité du message.

2) a) Rappeler les valeurs de p, q, m.
   b) Démontrer que l'équation (E) $5d \equiv 1 \ \ (m)$ admet des solutions.
   c) Trouver une solution particulière de l'équation (E).
   d) En déduire les solutions de l'équation (E).
   e) Parmi les clés suivantes déterminer celle qu'Alice peut choisir comme clé privée :
   $$(21\,;6)\ ;\ (21\,;11)\ ;\ (21\,;13)\ ;\ (21\,;15)\ ;\ (21\,;17)\ ;\ (21\,;19).$$

Dans la suite de la *partie A*, on admet qu'Alice choisit la seule clé privée possible parmi les propositions précédentes.

3) Bob veut envoyer à Alice le message (M) : PAL. Il va utiliser la clé publique (21 ; 5).
   a) Associer à chaque lettre du message, sa **place** dans l'alphabet. Par exemple la lettre C est codée par 3. Obtenir ainsi trois entiers naturels M_1, M_2, M_3.
   b) Déterminer C_1, C_2, C_3 vérifiant $C_i \equiv {M_i}^5 \ \ (21)$ avec $0 \leq C_i < n$.
   c) En déduire le message chiffré (C) que Bob envoie à Alice.

4) Alice reçoit le message (C) : 4 1 3. Elle veut déchiffrer ce message.
   a) Déterminer M_1, M_2, M_3 vérifiant $M_i \equiv {C_i}^{17} \ \ (21)$ avec $0 \leq M_i < n$.
   b) En déduire le message en clair que Bob a envoyé à Alice.

Partie B : Alice a choisi (55 ; 3) comme clé privée. Elle reçoit de la part de Bob le message (C) :

10 1 7 25 24 18 5 9 49

Le message étant un peu long, on va utiliser les listes du menu STAT de la calculatrice pour son déchiffrement.

- Remplir la Liste1 avec les entiers naturels de 1 à 54.
- Remplir la Liste2 avec (Liste1)^3.
- Remplir la Liste3 en tapant : (Liste2)$-55 *$PartieEntière((Liste2)/55).

1) Que calcule la formule rentrée dans Liste3 ?

2) Ecrire le début des listes Liste1 Liste2 Liste3.

3) Déchiffrer le message reçu.

Partie C : Alice a choisi (221 ; 35) comme clé privée. Elle reçoit de la part de Bob le message (C) :

126 164 208 164 76 76 1 184 164 27 164
76 1 200 41 111 166 164 41 86 200 185 86 1 152 1 76

1) Utiliser une méthode analogue à celle de la partie B pour déchiffrer ce long message.
   Que constatez-vous ? Expliquez ce résultat.

2) Pour résoudre ce problème, on utilise un algorithme de calcul des restes dans la division euclidienne par 221 des puissances successives de ${C_i}^1$ jusqu'à ${C_i}^{35}$ et qui affiche le reste de la division de C^{35} par 221.

   a) Justifier que :
   si $C^{n-1} \equiv R\ (221)$ alors $C^n \equiv R \times C\ (221)$.

   b) Compléter l'algorithme ci-contre qui à toute valeur de C entrée par l'utilisateur permet d'afficher le reste de la division euclidienne par 221 de C^{35}.

3) Entrer le programme correspondant dans la calculatrice. Déchiffrer le message reçu par Alice.

ENTREE :
C entier naturel
TRAITEMENT ET SORTIE :
Saisir …
R prend la valeur …
Pour *I* allant de 1 à …
… prend la valeur $R \times C - 221 \times$partEnt$(R \times C/221)$
Fin Pour
Afficher …