

Devoir à la maison

à rendre le lundi 21 février 2011

Exercice 1 (3 points).

1. En utilisant les propriétés des congruences, déterminez successivement les restes de la division euclidienne par 17 des entiers suivants : 100 ; 61 ; 161 ; 6100 ; 61^2 ; 33^{343} .

Solution.

- $100 = 17 \times 5 + 15$ donc $100 \equiv 15 \pmod{17}$
- $61 = 17 \times 3 + 10$ donc $61 \equiv 10 \pmod{17}$
- $161 \equiv 100 + 61 \equiv 15 + 10 \equiv 25 \equiv 8 \pmod{17}$
- $6100 \equiv 100 \times 61 \equiv 15 \times 10 \equiv 150 \equiv 14 \pmod{17}$
- $61^2 \equiv 10^2 \equiv 100 \equiv 15 \pmod{17}$
- $33^{343} \equiv (-1)^{343} \equiv (-1)^{2 \times 171 + 1} \equiv 1^{171} \times (-1) \equiv -1 \equiv 16 \pmod{17}$

2. Calculez le PGCD de 385 et 1365.

Solution. On utilise l'algorithme d'Euclide :

$$\begin{aligned} 1365 - 385 \times 3 &= 210 \\ 385 - 210 \times 1 &= 175 \\ 210 - 175 \times 1 &= 35 \\ 175 - 35 \times 5 &= 0 \end{aligned}$$

Le PGCD est le dernier reste non nul, donc $\text{PGCD}(385, 1365) = 35$.

3. Calculez l'inverse de 125 modulo 242.

Solution. On utilise l'algorithme d'Euclide étendu :

	242	1	0
	125	0	1
$242 - 125 \times 1 =$	117	$1 - 0 \times 1 = 1$	$0 - 1 \times 1 = -1$
$125 - 117 \times 1 =$	8	$0 - 1 \times 1 = -1$	$1 - (-1) \times 1 = 2$
$117 - 8 \times 14 =$	5	$1 - (-1) \times 14 = 15$	$-1 - 2 \times 14 = -29$
$8 - 5 \times 1 =$	3	$-1 - 15 \times 1 = -16$	$2 - (-29) \times 1 = 31$
$5 - 3 \times 1 =$	2	$15 - (-16) \times 1 = 31$	$-29 - 31 \times 1 = -60$
$3 - 2 \times 1 =$	1	$-16 - 31 \times 1 = -47$	$31 - (-60) \times 1 = 91$
$2 - 1 \times 2 =$	0		

On trouve $242 \times (-47) + 125 \times 91 = 1$, soit $125 \times 91 = 1 + 242 \times 47$. On a donc $125 \times 91 \equiv 1 \pmod{242}$.

L'inverse de 125 modulo 242 est 91.

Exercice 2 (3 points).

1. Montrez que pour tout entier naturel n , $12n + 1$ et $30n + 2$ sont premiers entre eux.

Solution. On remarque que $5 \times (12n + 1) + (-2) \times (30n + 2) = 1$. On reconnaît une identité de Bézout, et on en déduit que $12n + 1$ et $30n + 2$ sont premiers entre eux pour tout entier naturel n .

2. En supposant que $n \geq 1$, en est-il de même pour $4n$ et $n + 1$?

Solution.

Pour $n = 1$, on a $4n = 4$ et $n + 1 = 2$: ils ne sont pas premiers entre eux.

Pour $n = 2$, on a $4n = 8$ et $n + 1 = 3$: ils sont premiers entre eux.

Pour $n = 3$, on a $4n = 12$ et $n + 1 = 4$: ils ne sont pas premiers entre eux.

Donc $4n$ et $n + 1$ ne sont pas toujours premiers entre eux.

3. Donnez un couple d'entiers relatifs (x, y) solution de l'équation diophantienne

$$345x + 714y = 3$$

Solution.

$$\begin{array}{r|l}
 714 & 1 \\
 345 & 0 \\
 714 - 345 \times 2 = 24 & 1 - 0 \times 2 = 1 \\
 345 - 24 \times 14 = 9 & 0 - 1 \times 14 = -14 \\
 24 - 9 \times 2 = 6 & 1 - (-14) \times 2 = 29 \\
 9 - 6 \times 1 = 3 & -14 - 29 \times 1 = -43 \\
 6 - 3 \times 2 = 0 & 29 - (-60) \times 1 = 89
 \end{array}$$

On obtient $714 \times (-43) + 345 \times 89 = 3$. On peut donc prendre $x = 89$ et $y = -43$.

Exercice 3 (3 points).

1. Donnez tous les nombres inversibles dans $\mathbb{Z}/25\mathbb{Z}$. Justifiez votre réponse.

Solution. 1,2,3,4,6,7,8,9,11,12,13,14,16,17,18,19,21,22,23,24

Ce sont tous les nombres inférieurs à 25 et premiers avec 25.

2. Résoudre l'équation $5x \equiv 11$ dans $\mathbb{Z}/77\mathbb{Z}$.

Solution. Il y a une solution unique car 5 et 77 sont premiers entre eux.

Pour calculer cette solution, on a besoin de l'inverse de 5 modulo 77.

$$\begin{array}{r|l}
 77 & 1 \\
 5 & 0 \\
 77 - 5 \times 15 = 2 & 1 - 0 \times 15 = 1 \\
 5 - 2 \times 2 = 1 & 0 - 1 \times 2 = -2 \\
 2 - 1 \times 2 = 0 & 1 - (-2) \times 2 = 5
 \end{array}$$

On obtient $77 \times (-2) + 5 \times 31 = 1$, donc l'inverse de 5 modulo 77 est 31.

La solution de l'équation est alors $x \equiv 31 \times 11 \pmod{77} \equiv 341 \pmod{77} \equiv 33 \pmod{77}$.

On peut vérifier que $5 \times 33 \equiv 165 \pmod{77} \equiv 11 \pmod{77}$.

3. Quel est le nombre de solutions dans $\mathbb{Z}/77\mathbb{Z}$ de l'équation $11x \equiv 6$? Justifiez votre réponse.

Solution. 11 n'est pas premier avec 77, donc il n'y a pas une solution unique : il peut y avoir aucune solution ou alors plusieurs solutions.

Soit $x \in \mathbb{Z}/77\mathbb{Z}$. On effectue la division euclidienne de x par 7, et on obtient $x = 7q + r$ avec $0 \leq r < 7$. On calcule $11x \equiv 11(7q + r) \equiv 77q + 11r \equiv 11r \pmod{77}$. Par conséquent, il suffit de regarder ce qui se passe pour les restes r :

r	$11r$	$11r \pmod{77}$
0	0	0
1	11	11
2	22	22
3	33	33
4	44	44
5	55	55
6	66	66

On ne trouve jamais 6, donc l'équation $11x \equiv 6$ n'a aucune solution dans $\mathbb{Z}/77\mathbb{Z}$.

Exercice 4 (5 points). On rappelle la correspondance habituelle entre les lettres de l'alphabet $\{A, B, C, \dots, Z\}$ et les nombres $\{0, 1, 2, \dots, 25\}$.

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

1. On utilise la clé de chiffrement $f_1(x) \equiv 17x + 5 \pmod{26}$.

(a) Chiffrer le message EXAMEN.

Solution.

	E	X	A	M	E	N
x	4	23	0	12	4	13
$17x + 8$	73	396	5	209	73	226
$f_1(x)$	21	6	5	1	21	18
	V	G	F	B	V	S

- (b) Vérifier que la clé de déchiffrement associée à f_1 est $g_1(x) \equiv 23x + 15 \pmod{26}$.

Solution.

$$g_1(f_1(x)) \equiv 23(17x + 5) + 15 \equiv 391x + 130 \equiv 1x + 0 \equiv x \pmod{26}$$

- (c) Déchiffrer le message WLEHKV.

Solution.

	<i>W</i>	<i>L</i>	<i>E</i>	<i>H</i>	<i>K</i>	<i>V</i>
x	22	11	4	7	10	21
$19x + 4$	521	268	107	176	245	498
$g_1(x)$	1	8	3	20	11	4
	<i>B</i>	<i>I</i>	<i>D</i>	<i>U</i>	<i>L</i>	<i>E</i>

2. La fonction $f_2(x) \equiv 13x + 18 \pmod{26}$ est-elle une clé de chiffrement valide ? Pourquoi ?

Solution. Non car 13 n'est pas premier avec 26, donc 13 n'est pas inversible modulo 26. Par conséquent, on ne pourra pas calculer la clé de déchiffrement correspondante, ou de façon équivalente, plusieurs lettres seront chiffrées par la même lettre, ce qui rendra le déchiffrement des cryptogrammes impossible.

3. Calculer la clé de déchiffrement g_3 associée à la clé de chiffrement $f_3(x) \equiv 15x + 11 \pmod{26}$

Solution. Si on note $g_3(x) = a'x + b' \pmod{26}$ la fonction de déchiffrement, on doit avoir $g_3(f_3(x)) \equiv x \pmod{26}$.

Ce qui donne $a'(15x + 11) + b' \equiv x \pmod{26}$. On en déduit que
$$\begin{cases} 15a' \equiv 1 \pmod{26} \\ 11a' + b' \equiv 0 \pmod{26} \end{cases}$$

La première équation signifie que a' est l'inverse de 15 modulo 26.

$$\begin{array}{r|l} 26 & 1 \\ 15 & 0 \\ 26 - 15 \times 1 = 11 & 1 - 0 \times 1 = 1 \\ 15 - 11 \times 1 = 4 & 0 - 1 \times 1 = -1 \\ 11 - 4 \times 2 = 3 & 1 - (-1) \times 2 = 3 \\ 4 - 3 \times 1 = 1 & -1 - 3 \times 1 = -4 \\ 3 - 1 \times 3 = 0 & \end{array} \quad \begin{array}{l} 0 \\ 1 \\ -1 \\ 2 \\ -5 \\ 7 \end{array}$$

On obtient $26 \times (-4) + 15 \times 7 = 1$, donc $a' = 7$.

De la seconde équation, on tire $b' \equiv -11a' \equiv -11 \times 7 \equiv -77 \equiv 1 \pmod{26}$.

Finalement, on a $g_3(x) = 7x + 1 \pmod{26}$.

On peut vérifier qu'on a bien $g_3(f_3(x)) \equiv 7(15x + 11) + 1 \equiv 105x + 78 \equiv 1x + 0 \equiv x \pmod{26}$.

4. Sachant que dans un chiffrement affine inconnu, la lettre E est chiffrée par O et que la lettre H est chiffrée par J, déterminer la fonction de chiffrement f_4 correspondante.

Solution. Notons $f_4(x) = ax + b \pmod{26}$ la fonction de chiffrement inconnue. On sait que :

	<i>E</i>	<i>H</i>
x	4	7
$f_4(x)$	14	9
	<i>O</i>	<i>J</i>

On obtient donc le système
$$\begin{cases} 4a + b \equiv 14 \pmod{26} \\ 7a + b \equiv 9 \pmod{26} \end{cases}$$

En soustrayant la première équation à la deuxième, on trouve $3a \equiv -5 \equiv 21 \pmod{26}$. On a besoin de l'inverse de 3 modulo 26, à savoir 9 (car $3 \times 9 - 26 \times 1 = 1$). On trouve alors $a \equiv 9 \times 21 \equiv 189 \equiv 7 \pmod{26}$.

Pour trouver b , on reporte la valeurs de a , par exemple dans la première équation, et on obtient $b \equiv 14 - 4 \times 7 \equiv 14 - 28 \equiv -14 \equiv 12 \pmod{26}$.

Finalement, on a $f_4(x) = 7x + 12 \pmod{26}$.

On peut vérifier que $f_4(4) \equiv 7 \times 4 + 12 \equiv 14 \pmod{26}$, donc E est bien chiffré par O et $f_4(7) \equiv 7 \times 7 + 12 \equiv 61 \equiv 9 \pmod{26}$, donc H est bien chiffré par J.

Exercice 5 (6 points). Il s'agit dans cet exercice de déterminer un entier naturel n dont l'écriture décimale du cube se termine par 2009, c'est-à-dire tel que $n^3 \equiv 2009 \pmod{10000}$.

1. Déterminer le reste de la division euclidienne de 2009^2 par 16. En déduire que $2009^{8001} \equiv 2009 \pmod{16}$.

Solution. On a $2009 = 125 \times 16 + 9$.

Donc $2009^2 \equiv 9^2 \equiv 81 \equiv 1 \pmod{16}$

Donc $2009^{8001} \equiv 2009^{2 \times 4000 + 1} \equiv (2009^2)^{4000} \times 2009 \equiv 1^{4000} \times 2009 \equiv 2009 \pmod{16}$

2. On considère la suite (u_n) définie sur \mathbb{N} par
$$\begin{cases} u_0 = 2009^2 - 1 \\ u_{n+1} = (u_n + 1)^5 - 1 \end{cases}$$
. Calculer u_1 , u_2 et u_3 .

Solution.

$$u_1 = (u_0 + 1)^5 - 1 = (2009^2 - 1 + 1)^5 - 1 = 2009^{10} - 1$$

$$u_2 = (u_1 + 1)^5 - 1 = (2009^{10} - 1 + 1)^5 - 1 = 2009^{50} - 1$$

$$u_3 = (u_2 + 1)^5 - 1 = (2009^{50} - 1 + 1)^5 - 1 = 2009^{250} - 1$$

3. Vérifier que $u_{n+1} = u_n \times (u_n^4 + 5 \times (u_n^3 + 2u_n^2 + 2u_n + 1))$ pour tout $n \in \mathbb{N}$.

Solution. On utilise la formule $(a+b)^5 = a^5 + 5a^4b + 10a^3b^2 + 10a^2b^3 + 5ab^4 + b^5$ (triangle de Pascal ou binôme de Newton).

$$u_{n+1} = (u_n + 1)^5 - 1 = (u_n)^5 + 5(u_n)^4 + 10(u_n)^3 + 10(u_n)^2 + 5(u_n) + 1 - 1 = u_n \times ((u_n)^4 + 5(u_n)^3 + 10(u_n)^2 + 10(u_n) + 5) = u_n \times (u_n^4 + 5 \times (u_n^3 + 2u_n^2 + 2u_n + 1))$$

4. Montrer que u_0 est divisible par 5, u_1 est divisible par 25, u_2 est divisible par 125 et u_3 est divisible par 625.

Solution.

- $u_0 \equiv 2009^2 - 1 \equiv 4^2 - 1 \equiv 16 - 1 \equiv 1 - 1 \equiv 0 \pmod{5}$ donc u_0 est divisible par 5.
- En utilisant la question précédente : $u_1 = u_0 \times (u_0^4 + 5 \times (u_0^3 + 2u_0^2 + 2u_0 + 1))$. On voit que u_1 est un produit de deux facteurs. Le premier est u_0 qui est divisible par 5 et le second est $u_0^4 + 5 \times (u_0^3 + 2u_0^2 + 2u_0 + 1)$, qui est aussi divisible par 5 (puisque u_0 est divisible par 5). Finalement, u_1 est divisible par $5 \times 5 = 25$.
- De même, on a $u_2 = u_1 \times (u_1^4 + 5 \times (u_1^3 + 2u_1^2 + 2u_1 + 1))$, où le premier facteur u_1 est divisible par 25 et le second facteur $u_1^4 + 5 \times (u_1^3 + 2u_1^2 + 2u_1 + 1)$ est divisible par 5. Donc u_2 est divisible par $25 \times 5 = 125$.
- Enfin, on a $u_3 = u_2 \times (u_2^4 + 5 \times (u_2^3 + 2u_2^2 + 2u_2 + 1))$, où le premier facteur u_2 est divisible par 125 et le second facteur $u_2^4 + 5 \times (u_2^3 + 2u_2^2 + 2u_2 + 1)$ est divisible par 5. Donc u_3 est divisible par $125 \times 5 = 625$.

5. En déduire que $2009^{8001} \equiv 2009 \pmod{625}$

Solution. On a $u_3 \equiv 0 \pmod{625}$ donc $2009^{250} \equiv 1 \pmod{625}$.

Donc $2009^{8001} \equiv 2009^{32 \times 625 + 1} \equiv 1^{32} \times 2009 \equiv 2009 \pmod{625}$.

6. Conclure, c'est-à-dire déterminer un entier naturel n dont l'écriture décimale du cube se termine par 2009.

Solution.

- On a vu dans les questions précédentes que $2009^{8001} \equiv 2009 \pmod{16}$ et $2009^{8001} \equiv 2009 \pmod{625}$, autrement dit que $2009^{8001} - 2009$ est divisible par 16 et par 625. Or $16 = 2^4$ et $625 = 5^4$ sont premiers entre eux, donc $2009^{8001} - 2009$ est aussi divisible par $16 \times 625 = 10000$, c'est-à-dire que $2009^{8001} \equiv 2009 \pmod{10000}$.
- De plus, $8001 = 3 \times 2667$, donc $2009^{8001} = (2009^{2667})^3$.
- Finalement, on a $(2009^{2667})^3 \equiv 2009 \pmod{10000}$, et on peut conclure que

$$n = 2009^{2667}$$

répond à la question.

Partie facultative : Chiffrement par substitution

- Un chiffrement par substitution simple consiste à remplacer chaque lettre par une autre, selon une méthode décidée à l'avance.
- Un chiffrement affine correspond à un cas particulier où la substitution se calcule à l'aide d'une fonction affine.

Exercice 6 (Chiffrer/Déchiffrer). Dans le cas général, il n'y a pas de fonction mathématique simple permettant de chiffrer chaque lettre, c'est pourquoi on donne la table de chiffrement en entier. On utilise la substitution suivante :

A	B	C	D	E	F	G	H	I	J	K	L	M
S	C	W	U	D	X	B	F	Y	T	G	Z	I

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
H	O	J	N	K	A	M	L	P	E	Q	R	V

1. Chiffrer le message : FACILE.

Solution. Le cryptogramme est : XSWYZD

2. Écrire la table de déchiffrement correspondante.

Solution. La table de déchiffrement est :

A	B	C	D	E	F	G	H	I	J	K	L	M
S	G	B	E	W	H	K	N	M	P	R	U	T

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Q	O	V	X	Y	A	J	D	Z	C	F	I	L

3. Déchiffrer le message DAASY.

Solution. Le message déchiffré est : ESSAI

Exercice 7 (D'où vient ce nom ?). Expliquer pourquoi les chiffrements par substitution font partie des méthodes dites à clé secrète.

Solution. Avant de pouvoir échanger des messages secrets, il faut que les deux correspondants se mettent d'accord sur les clés de chiffrement/déchiffrement qu'ils vont utiliser et ensuite ils doivent garder ces clés rigoureusement secrètes pour assurer la sécurité des leurs échanges.

Exercice 8 (Cette fois, ce n'est pas faible). Combien y-a-t-il de chiffrements par substitution simples différents ?

Solution. Pour fabriquer un chiffrement par substitution simple, il suffit de choisir quelle lettre remplacera le A, quelle lettre remplacera le B, et ainsi de suite jusqu'à Z, en prenant soin de ne pas choisir deux fois la même lettre (sinon on ne pourra plus déchiffrer les messages). Pour choisir la lettre qui va chiffrer la lettre A, il y a 26 possibilités. Ensuite pour choisir la lettre qui va chiffrer B, il reste 25 possibilités. Puis il en reste 24 pour C, etc. Finalement, pour Y il reste deux possibilités et pour Z il ne reste plus qu'une seule possibilité.

Au final, il y a donc $26 \times 25 \times 24 \times \dots \times 2 \times 1 = 26! \simeq 4.10^{26}$ chiffrements différents.

À noter que parmi les chiffrements par substitution simple, il y a les 26 chiffrements par décalage et les 312 chiffrements affines.

Exercice 9 (Décryptage). Le cryptogramme suivant a été obtenu à l'aide d'un chiffrement par substitution simple inconnu :

RC IZQKOGJZCKVYD DTO SUD PDT PYTIYKRYUDT PD RC IZQKO-
GRGJYD T'COOCIVCUO C KZGODJDZ PDT XDTTCJDT (CTTSZCUO
IGUBYPDUOYCRYOD, CSOVDUOYIYOD DO YUODJZYOD) DU T'-
CYPCUO TGSLDUO PD TDIZDOT GS IRDT. DRRD DTO SOYRYTDD
PDKSYT R'CUOYWSYOD, XCYT IDZOCYUDT PD TDT XDOVG-
PDT RDT KRST YXKGZOCUODT, IGXXD RC IZQKOGJZCKVYD
CTQXDOZYWSD, U'GUO WSD WSDRWSDT PYMCYUDT P'CU-
UDDT P'DHYTODUID. AYDU WS'DXYUDXXDUO TOZCODJYWS,
RC IZQKOGJZCKVYD DTO ZDTODD KDUPCUO OZDT RGUJODXKT
SU CZO, KGSZ UD PDLDUYZ SUD TIYDUID WS'CS HHD TY-
DIRD. CLDI R'CKKCZYOYGU PD R'YUBGZXCOYWS, TGU SOYRYT-
COYGU TD PDXGIZCOYTD PD KRST DU KRST.

1. Que deviennent les méthodes de décryptage utilisées précédemment ?

Solution. On ne connaît pas le type de la fonction de chiffrement (comme un décalage ou une fonction affine), donc on ne peut pas calculer les paramètres de cette fonction. D'autre part, le nombre de possibilités est trop grand pour envisager de toutes les essayer en un temps raisonnable, même avec un ordinateur.

2. Décrypter le message proposé.

Solution.

LA CRYPTOGRAPHIE EST UNE DES DISCIPLINES DE LA CRYPTOLOGIE S'ATTACHANT A PROTEGER DES MESSAGES (ASSURANT CONFIDENTIALITE, AUTHENTICITE ET INTEGRITE) EN S'AIDANT SOUVENT DE SECRETS OU CLES. ELLE EST UTILISEE DEPUIS L'ANTIQUITE, MAIS CERTAINES DE SES METHODES LES PLUS IMPORTANTES, COMME LA CRYPTOGRAPHIE ASYMETRIQUE, N'ONT QUE QUELQUES DIZAINES D'ANNEES D'EXISTENCE. BIEN QU'EMINEMENT STRATEGIQUE, LA CRYPTOGRAPHIE EST RESTEE PENDANT TRES LONGTEMPS UN ART, POUR NE DEVENIR QU'UNE SCIENCE QU'AU XXE SIECLE. AVEC L'APPARITION DE L'INFORMATIQUE, SON UTILISATION SE DEMOCRATISE DE PLUS EN PLUS.

3. Décrire la méthode utilisée.

Solution. On peut utiliser l'analyse des fréquences pour essayer de repérer la traduction de certaines lettres, et bien sûr s'aider des indices trouvés dans le texte (les mots d'une ou deux lettres, les mots avec apostrophe, etc.). Comme le cryptogramme est relativement long, on peut espérer que les fréquences calculées seront relativement proches des fréquences théoriques en Français. On trouve très facilement sur Internet des sites de cryptographie qui permettent de calculer les fréquences des lettres dans un texte, fournissent des tables de fréquences des lettres (ou des groupes de lettres) dans la langue française, et divers outils d'aide au décryptage. Ensuite, c'est une affaire d'astuce et de persévérance.

On peut par exemple commencer comme ceci :

La longueur du texte est de 484 caractères (en enlevant les espaces et les signes de ponctuation). Les fréquences (en %) des différentes lettres du cryptogramme sont les suivantes :

Lettre	Fréquence
a	0,2066
b	0,4132
c	7,2314
d	17,3554
e	0,000000
f	0,000000
g	4,1322
h	0,6198
i	3,7190
j	1,8595
k	3,9256
l	0,6198
m	0,2066

Lettre	Fréquence
n	0,000000
o	9,5041
p	3,7190
q	1,0331
r	4,5455
s	4,9587
t	9,2975
u	7,4380
v	1,2397
w	1,8595
x	2,6860
y	8,4711
z	4,9587

À titre de comparaison, les fréquences des lettres dans la langue française sont données (en %) dans la table suivante :

Lettre	Fréquence
a	8,25
b	1,25
c	3,25
d	3,75
e	17,75
f	1,25
g	1,25
h	1,25
i	7,25
j	0,75
k	0,00
l	5,75
m	3,25

Lettre	Fréquence
n	7,25
o	5,75
p	3,75
q	1,25
r	7,25
s	8,25
t	7,25
u	6,25
v	1,75
w	0,00
x	0,00
y	0,75
z	0,00

On peut déjà déduire que la lettre D représente probablement un E. En effet, E est de très loin la lettre la plus commune en Français avec une fréquence de 17,75%, et la lettre D a une fréquence de 17,36% dans le cryptogramme. La lettre isolée C dans le cryptogramme ne peut représenter que A ou Y. Sa fréquence est 7,2%, ce qui est proche de la fréquence de A en Français (8,25%), mais pas de celle de Y (0,75%). Donc C représente probablement un A.

etc.

À la fin, on obtient la table de déchiffrement :

A	B	C	D	E	F	G	H	I	J	K	L	M
B	F	A	E			O	X	C	G	P	V	Z

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	T	D	Y	L	U	S	N	H	Q	M	I	R

Les lettres E,F et N n'apparaissent pas dans le cryptogramme. On sait qu'elle doivent correspondre aux lettres J, K et W (qui n'apparaissent pas dans le message en clair), mais on ne sait pas exactement comment.