Cryptographie

IUT Informatique de Bordeaux - Année Spéciale

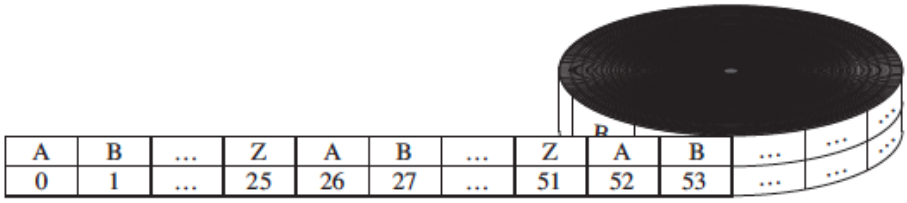
29 septembre 2015

1 Le codage affine

1.1 Introduction

1.1.1 La bande de papier infinie

Imaginons une bande de papier infinie sur laquelle, on place les lettres de l'alphabet dans l'ordre alphabétique puis arrivé à Z, on recommence à A comme le suggère la figure ci-dessous :

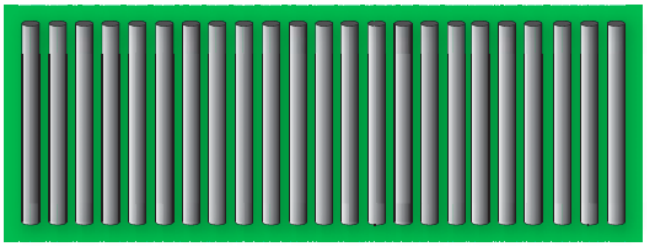


A	B	...	Z	A	B	...	Z	A	B	...	...	...
0	1	...	25	26	27	...	51	52	53	...	...	...

Vérifiez qu'en 79ème position, on retrouvera une lettre B.
Quelle sera la lettre située en 212ème position ?
Quelles seront les positions des huit premières lettres G que nous rencontrerons en déroulant la bande ?

1.1.2 Le jeu de Fort Boyard

Dans une épreuve de ce jeu télévisé, un candidat est opposé au « maître des Jeux ». Face à un alignement de bâtonnets (ici : 23), chacun doit, à tour de rôle, retirer 1, 2 ou 3 bâtonnets, au choix. Celui qui retire le dernier bâtonnet a perdu.



Montrer que, pour gagner, le candidat doit laisser, à chaque étape, un nombre de bâtonnets dont le reste par la division par 4 est de 1.

Définition 1. On fixe un entier naturel n, supérieur ou égal à 2. On dit que deux nombres x et y sont **congrus modulo n**, et on note $x \equiv y(modn)$ ou $x \equiv y\,[n]$s'ils ont le même reste dans leurs divisions respectives par n c'est à dire que **x-y est divisible par n.**

La congruence est compatible avec l'addition, la soustraction, la multiplication, l'exponentiation mais pas la division .

Exercice 1. Application de la définition

1. Montrer que $365 \equiv 15 \equiv 1 \pmod 7$.
2. Montrer que $18 \equiv -17 \pmod 7$.
3. Déterminer si 17 est congru à 5 modulo 6 et si 24 et 14 sont congrus modulo 6.
4. Donner les entiers congrus à 0 mod 3, ceux congrus à 1 mod 3 et ceux congrus à 2 mod 3. Que constatez-vous ?

1.2 Congruence et cryptographie affine

1.2.1 Le code de César

Le premier des systèmes de codage est emprunté à Jules César. Un principe commun à tous ces modes de codage est de transformer chaque lettre de l'alphabet ou chaque signe du système symbolique utilisé en un nombre ;" le chiffrement".

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Dans ce cryptage simpliste, chaque lettre de l'alphabet était remplacée par la lettre située trois rangs plus loin dans l'alphabet (A $\rightarrow$ D ; B $\rightarrow$ E ...) quand cela était possible ; aux trois dernières lettres X, Y, Z correspondaient les trois premières A, B, C.

Cela peut se décrire facilement en terme de congruence : soit M l'équivalent numérique d'une lettre de l'alphabet en clair et M' l'équivalent numérique de la lettre codée correspondante. On a :

$$M' \equiv M + 3 (mod 26)$$

La correspondance obtenue ainsi entre l'alphabet et son code est donnée par :

Alphabet en clair	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
Alphabet codé	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	0	1	2
	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Exercice 2. Codons et décodons d'après César

Coder à la main le message suivant : TU QUOQUE MI FILI

Décoder à la main le message suivant : DYHFDHVDUPRULWXULWHVDOXWDQW

Le principe du décodage est tout aussi simple

Si M' est le symbole d'une lettre codée, M le symbole de la lettre en clair lui correspondant, on a :

$$M \equiv M'\text{–}3 (mod 26) \; ou \; M \equiv M' + 23 (mod 26)$$

Avec les même notations, on peut généraliser à :

$$M' \equiv M + k (mod 26)$$

où k est la clé du codage.

Il y a 26 transformations de ce type incluant "le codage de César" pour k = 3 et "la transformation identique" pour k = 0.

Exercice 3. Sachant que la clé de cryptage est k = 12, décrypter XQETAYYQEODAUQZFQZOQCGUXEPQEUDQZF

Même en ne connaissant pas la clé de cryptage, décrypter :

ARZDVIRZJDZVLOVKIVCVGIVDZVIUREJLE MZCCRXVHLVCVJVTFEURIFDV

1.2.2 Le codage affine (introduction)

On peut généraliser le codage précédent en considérant des transformations du type :

$$M' \equiv a \cdot M + b (mod 26)$$

que l'on appelle transformations affines.

Comme l'on travaille "modulo 26", on peut se contenter de choisir les entiers a et b compris entre 0 et 25.

Exercice 4. Montrer que si l'on choisit a = 3 et b = 5, alors le caractère codé "L" correspond au caractère "C" en clair.

Exercice 5. Le but de cet exercice est d'observer l'influence du choix des clés a et b dans le codage d'un caractère.

Avec a = 1, b = 0, on obtient un joli codage !

Avec a = 2, b = 0, coder le A et le N.

Il est donc nécessaire de trouver une condition pour a (et pour b alors ?) pour que le codage puisse être décoder sans ambiguité : un codage bijectif . Nous verrons ceci sous peu.

Exercice 6. Crypter, à la main, le message "Le roi est mort" à l'aide de la transformation affine avec a = 3, b = 5.

Exercice 7. Crypter la phrase "C'est un trou de verdure où chante une rivière" avec les clés de cryptage a = 7 et b = 19.

Montrer que les clés a = 15 et b = 1 permettent de décrypter la phrase obtenue afin de retrouver en clair la phrase d'Arthur Rimbaud.

1.2.3 Des outils pour ce codage : PGDC, Algorithme d'Euclide, identité de Bezout

Définition 2. On dit que deux nombres entiers relatifs non nuls a et b sont **premiers entre eux** lorsqu'ils n'admettent pas de diviseur commun autre que 1.

Définition 3. On dit que deux nombres entiers relatifs non nuls a et b sont premiers entre eux lorsque leur PGDC(plus grand diviseur commun) est égal à 1.

Exercice 8. Déterminer : a) PGDC(35, 84) b) PGDC(39, 52) c) PGDC(48, 54) d) PGDC(60, 45)

Les couples de nombres suivants sont-ils premiers entre eux ? a) 122 et 49 b) 352 et 33

L'**algorithme (d'Euclide)** suivant permet de calculer le PGCD de deux nombres

$$\begin{aligned} 4539 &= 2 \times 1958 + 623 \ (r_0 = 623) \\ 1958 &= 3 \times 623 + 89 \ (r_1 = 89) \\ 623 &= 7 \times 89 + 0 \ (r_2 = 0) \end{aligned}$$

Le **dernier reste non nul est le PGCD** des deux nombres du départ. Ainsi $PGCD(4359, 1958) = 89$.

Exercice 9. À l'aide de l'algorithme d'Euclide, déterminer le PGDC des couples de nombres : a) 777 et 441 b) 2004 et 9185 c) 1600 et 259

Théorème 1 (Egalité de Bezout)**.** *Soit a et b deux entiers relatifs non nuls et D leur PGDC. Il existe deux entiers relatifs u et v tel que au + bv = D.*

Exemple 1. Nous avons montré que PGDC(4539, 1958) = 89. L'encadré précédent affirme donc qu'il existe donc deux entiers u et v tels que : 4539u + 1958v = 89. Pour contrôle, u = -3 et v = 7 vérifient bien cette condition.

Comment obtenir ces 2 entiers u et v ?En partant de l'avant dernière ligne de l'algorithme d'Euclide, on exprime systématiquement le reste :

$$\begin{aligned} 89 &= 1968 - 3 \times 623 \\ 89 &= 3 \times (4539 - 2 \times 1968) = 3 \times 4539 - 6 \times 1968 \end{aligned}$$

Exercice 10. À l'aide de l'algorithme d'Euclide, montrer que PGDC(62, 43) = 1 puis en déduire les 2 valeurs entières u et v vérifiant : 62u + 43v = 1

En utilisant l'algorithme d'Euclide, démontrer que 383 et 127 sont premiers entre eux, puis déterminer des entiers relatifs u et v tels que 383u + 127v = 1

Théorème de Bezout : Soit a et b deux entiers relatifs non nuls. a et b sont premiers entre eux $\Leftrightarrow$ il existe deux entiers relatifs u et v tels que au + bv = 1

1.2.4 Retour sur le codage affine

Exercice 11. Montrer que le choix de la clé a = 13 induit que toutes les lettres pair seront codées de la même façon.

On rappelle qu'un tel choix de clé ne convient pas, car on doit exiger qu'à deux lettres différentes au départ correspondent deux lettres codées différentes. Qu'est-ce que cette condition implique pour les valeurs possibles de a ?

Théorème 2. *La condition nécessaire et suffisante pour satisfaire à cette exigence est que a soit premier avec 26*

Recherchons maintenant une clé de décodage :

Nous savons que

a est premier avec 26, donc, d'après Bezout, il existe a' et v tel que : $a \cdot a' + 26v = 1$ ou, modulo 26 : Il existe a' tel que

$$a \cdot a' \equiv 1(mod 26)$$

On dit alors que a' est un inverse de a modulo 26.

Soit M' une lettre codée, correspondant en clair à M. On connaît M', on veut retrouver M. On sait (quand on est dans le secret du codage)

$$\begin{aligned} M' &= aM + b[26] \\ M' - b &= aM[26] \\ a'(M' - b) &= a'aM[26] \\ M &= a'M' - a'b[26] \end{aligned}$$

Ce qui montre l'existence d'une transformation affine de décodage, réciproque de la transformation affine de codage.

Exemple 2. On considère la phrase

$$LACLEESTDANSLABOITE$$

que nous codons à l'aide de la transformation affine

$$M' = 7M + 10(mod 26)$$

Nous obtiendrons :

$$JKYJMMGNFKXGJKREONM$$

Pour trouver a' (l'inverse de a mod 26), une des deux clés du décodage, on va utiliser l'algorithme de Bezout avec 7 et 26 premiers entre eux

$$\begin{aligned} 7a' &\equiv 1[26] \\ 7a' &= 1 + 26k \\ 7a' - 26k &= 1 \end{aligned}$$

En utilisant l'algorithme d'Euclide , on obtient : a' = -11 ≡ 15 (mod 26)

On obtient b' grâce à la relation :

$$b' = -a' \cdot b = 11 \cdot 10 = 110 \equiv 6(mod 26)$$

Ainsi donc, la clé de décodage est :

$$M' \equiv 15 \cdot M + 6(mod 26)$$

Exercice 12. On considère les clés de cryptage affine : a = 11 et b = 22. On s'intéresse alors aux clés de décryptage a' et b'.

Montrer que a' = 19 est l'inverse de a mod 26.

Montrer que b' = 24 est l'autre clé.

Montrer que le cryptage affine de la lettre "C" correspond à "S", puis que les clés de décryptage a' = 19 et b' = 24 retransformer bien "S" en "C".

Exercice 13. On sait que Roméo a envoyé à Juliette le message crypté suivant : "ZXTHAWBNJQBDQIEZMBJOHADRDQIIZB" habituellement, il utilise toujours les mêmes clés : a = 19 et b = 3

Calculer a' puis b'.

Déterminer la lettre en clair correspondant à la première lettre cryptée Z.

1.2.5 Complément

Supposons que nous ayons à décoder le message suivant : "YMQMGGKAMMGNNELGMYZMN" En sachant qu'il a été codé au moyen d'une transformation affine.

les lettres de l'alphabet n'apparaissent pas avec la même fréquence dans une langue donnée !

C'est ainsi qu'en français, la lettre la plus fréquente est le E suivi du S puis du A. Avec un peu de chance, cet ordre "fréquentiel" va être suivi, à quelque chose près, par les lettres du texte à décoder : ceci sera d'autant plus vrai que le texte sera long

Ici, dans le court message que nous avons à décrypter, la lettre la plus fréquente est le M qui apparaît six fois, suivi du G qui apparaît quatre fois. Faisons alors l'hypothèse que le M correspond au E et le G au S.

Les paramètres de décryptage, a' et b' doivent alors vérifier les deux équations :

$4 \equiv 12a' + b'(mod 26)$ (équation 1 traduisant la transformation du M en E)
$18 \equiv 6a' + b'(mod 26)$ (équation 2 traduisant la transformation du G en S)

Nous sommes donc ramenés à résoudre un système de 2 équations à 2 inconnues modulo 26. Ces équations sont souvent désignées par le terme de Diophantiennes (du nom du mathématicien grec Diophante vers 350 qui a beaucoup travaillé à la résolution de ce genre d'équations).

Les règles élémentaires de calcul sur des congruences de même module nous permettent d'opérer quasiment comme pour la résolution d'équations classiques mais nous ne pouvons faire de divisions,

$$\begin{aligned} 4 &\equiv 12a' + b'(mod 26) \\ 18 &\equiv 6a' + b'(mod 26) \end{aligned}$$

En soustrayant les deux lignes :

$$-14 \equiv 6a'(mod 26)$$

soit, l'existence d'un entier relatif k tel que :

$$\begin{aligned} -14 &= 6\text{a'}+26\text{k} \\ 13k + 3a' &= -7 \\ 3a' &\equiv 6(mod 13) \text{ en multipliant par 9} \\ a' &\equiv 2mod(13) \end{aligned}$$

On en déduit donc que $a' \in \{2, 15\}$. Or a'doit être premier avec 26 donc $a' = 15$

On déduit facilement que b' = 6.

Exercice 14. "Casser" cette épitaphe célèbre

OFVVFSGBXVGPBPWXGDHQXFRMXMPDOEFSGX
BXVGWRPZRPGFOOKXSMWXSDHQKXMFSSXXVZRPWFCXBR
VFAXRSXVVXXSFDBBROXWFVPYPXHXOFKGPX
ORPVVFADRXVXBDRCKPGMRSOKXHPXKMRCXGOXSMFSGWFMDRUPXHX
PWOFVVFXSBDKXWXVXOGPXHXMXVFCPXFCFSGMXOKXSMKXRSXXODRVX
XGBPSZFSVOWRVGFKMPWXRGRSQXWXSIFSGZRP
FOKXVFCDPKFGGXPSGWFHDPGPXMXWFTXIPSFWMXVDSOXKX
OXKPGMRSXHDKGHFWEXRKXRVX VDSOXKXWRPVRKCXBRGZRFGKXFSSXXV
MXGDRGBXBPMXMRPVVDSFTX

1.2.6 Un exemple de cryptage polyalphabétique

un système de codage proposé par Blaise de Vigenère qui a publié en particulier un "Traité des chiffres" (1586) Son procédé emprunte à celui de César en le complexifiant : on opère des translations sur les lettres du texte à coder en fonction d'un mot-clé indiquant les translations à opérer selon le rang des lettres dans le texte. Illustrons-en le principe avec un exemple : le mot-clé est CODE.

Alphabet	C	E	M	E	S	S	A	G	E	E	S	T	T	O	P	S	E	C	R	E	T
en clair	2	4	12	4	18	18	0	6	4	4	18	19	19	14	15	18	4	2	17	4	19
Clé	C	O	D	E	C	O	D	E	C	O	D	E	C	O	D	E	C	O	D	E	C
codé	2	14	3	4	2	14	3	4	2	14	3	4	2	14	3	4	2	14	3	4	2
Alphabet	4	18	15	8	20	6	3	10	6	18	21	23	21	2	18	22	6	16	20	8	21
codé	E	S	P	I	U	G	D	K	G	S	V	X	V	C	S	W	G	Q	U	I	V

Pour finir, décrypter le message suivant sachant que la clé de cryptage était "BIENVU" : "OMQNIKVMDCVMMMWVOYBZWPMSQBSTMUQPMPV" Exercice 4.26 :

2 Le Codage RSA

Rappels :

— Deux nombres d et e sont dits inverses modulo n si : $d \cdot e \equiv 1 (mod\, n)$.

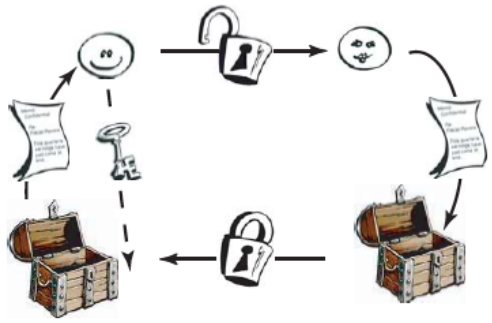
— d admet un inverse modulo n ssi d et n sont premiers entre eux

Exercice 15. Déterminer l'inverse de 7 modulo 20 (sans utiliser Bezout).

Définition 4. On appelle **exponentiation modulaire** les calculs du type : $a^b (mod\, n)$

2.1 Introduction

En 1976, Whitfield Diffie et Martin Hellman proposent une nouvelle façon de chiffrer, qui contourne le problème de la divulgation des clés. Schématiquement,un ami doit vous faire parvenir un message très important par la poste, mais vous n'avez pas confiance en votre facteur que vous soupçonnez d'ouvrir vos lettres. Comment être sûr de recevoir ce message sans qu'il soit lu ? Vous commencez par envoyer à votre ami un cadenas sans sa clé, mais en position ouverte. Celui-ci glisse alors le message dans une boîte qu'il ferme à l'aide du cadenas, puis il vous envoie cette boîte. Le facteur ne peut pas ouvrir cette boîte, car la seule clé le permettant est en votre possession.



La cryptographie à clé publique repose exactement sur ce principe. Mais il s'agira de créer deux clés différentes : une permettant de crypter (clé publique) et une deuxième, ne pouvant de déduire de la précédente permettant de décrypter le message (clé privée).

Mathématiquement, on dispose d'une fonction P sur les entiers, qui possède une fonction réciproque S. On suppose qu'on peut fabriquer un tel couple (P, S), mais que connaissant uniquement P, il est impossible (ou du moins très difficile) de retrouver S.

P est la clé publique, que vous pouvez révéler à quiconque. Si Alice veut vous envoyer un message, elle le code à l'aide de P et vous le transmet, sans aucune précaution. S est la clé secrète, elle reste en votre seule possession. Vous décodez le message en calculant : S(P(message M)) = message M'. La connaissance de P par un tiers ne compromet pas la sécurité de l'envoi des messages codés, puisqu'elle ne permet pas de retrouver S. Il est possible de donner librement P, qui mérite bien son nom de clé publique.

Bien sûr, il reste une difficulté : comment trouver de telles fonctions P et S ?

Diffie et **Hellman** n'ont pas eux-mêmes proposé de fonctions satisfaisantes, mais dès 1977, R. **Rivest**, A. **Shamir** et L. **Adleman** trouvent une solution possible, la plus utilisée à ce jour, la cryptographie RSA.

2.1.1 Principe mathématique

— Il est "facile" de fabriquer de grands nombres premiers p et q (pour fixer les idées, 100 chiffres).

— Étant donné un nombre entier n = p · q produit de 2 grands nombres premiers, il est très difficile de retrouver les facteurs p et q.

Illustrons tout ceci :

Alice doit envoyer un message à Bob, elle a donc besoin de la clé publique RSA de Bob. Voici les différentes étapes :

1. Bob fabrique les clés
   (a) Il choisit p et q deux grands nombres premiers (plus de 100 chiffres).
   (b) Il calcule $n = p \cdot q$. Le nombre n, le modulo RSA, a environ 200 chiffres. Il est publique alors que p et q sont gardés secrets.
   (c) Il calcule $\varphi(n) = (p-1)(q-1)$, qui s'appelle la fonction d'Euler, et qui doit rester secret. Retrouver $\varphi(n)$ sans connaître p et q est aussi difficile que de factoriser n.
   (d) Il choisit e en s'assurant que $PGDC(e, \varphi(n)) = 1$. Il s'agira de l'exposant d'encryptage RSA.
   (e) Il calcule d, inverse de e modulo $\varphi(n)$ et garde secret le couple (n , d). Il s'agira de la clé privée RSA. Il la garde secrète afin de pouvoir décoder par la suite le message transmis par Alice.
   (f) Il transmet (ou publie dans un annuaire) le couple (n , e). Ce couple s'appelle la clé publique RSA.
2. Alice utilise la clé publique.
   (a) Elle convertit son message "texte" en un nombre P compris entre 0 et n.
   (b) Elle calcule $M' \equiv M^e (mod\, n)$ et envoie ce message crypté M'.
3. Bob décode le message d'Alice avec sa clé secréte
   (a) il calcule $M \equiv (M')^d (mod\, n)$ à l'aide de sa clé privée d. Ceci lui permet de retrouver le message d'origine car : $(M')^d \equiv (M^e)^d (mod\, n) \equiv M^{ed} (mod\, n) \equiv M (mod\, n)$.
   (b) Il reconvertit ce nombre en un message clair.

Exemple 3. Une compagnie veut instaurer un système de commandes sur Internet. Elle instaure donc un cryptage à clé publique (RSA) pour la transmission du numéro de carte de crédit. Le numéro de carte de crédit est un numéro de 16 chiffres auquel on ajoute les 4 chiffres qui correspondent à la date d'expiration, soit un nombre de 20 chiffres.

La compagnie choisit donc p et q deux grands nombres premiers1.

p = 97609597511111112041886431

q = 83455239986783412564911111.

Ceci donne n = 8146032385303115441215786494344903355990022301484 1

$\varphi(n)$ = 814603238530311544121578468369652837704469246373 00.

La compagnie choisit sa clé d'encryptage

e = 45879256903

et calcule son inverse $d (mod\, \varphi(n))$:

d = 614249316518661714502675899921801756121167475740167.

Un client a le numéro de carte de crédit : 1234 5678 9098 7654 et la date d'expiration de sa carte est le 01/06. On doit donc envoyer le message M = 12345678909876540106.

Le programme d'envoi calcule $M' \equiv M^e (mod\, n)$:

M' = 625176510626059110979407460361990023455526694648 5.

Le nombre M' est transmis.

À la réception la compagnie calcule : $(M')^d \equiv 12345678909876540106 (mod\, n)$. Qui correspond donc bien au n° de la carte de crédit ainsi que sa date d'expiration. Dans la réalité, les entiers p et q choisis ne sont pas encore assez grands et un ordinateur pourrait factoriser n dans un temps convenable.

Exercice 16. Effectuer la démarche de cryptage avec la clé (n,e) proposée : (51201345568138081747, 158792633) sur le même numéro de carte de crédit M.

Calculer M' le message crypté correspondant à ce numéro.

Vérifier que la clé ci-dessous permet de retrouver le numéro. d = 39115303732664896793

Alice a pris connaissance de la clé publique de Bob : (253, 3), où 253 correspond à n et 3 à e. Elle veut lui envoyer le message OUI. Elle chiffre le message selon le code standard : 14 pour O, 20 pour U et 8 pour I.

	O	U	I
M	14	20	08
$M' \equiv M^3 (mod 253)$	214	157	006

Le message codé est donc 214 157 006.

2.2 Encryptage d'un message par blocs (digrammes)

Supposons que la clé publique de Bob soit (1943 , 5). Alice veut lui envoyer le message : OKPOURLUNDI en utilisant le code standard sur 26 lettres. Elle convertit ces lettres en chiffres comme d'habitude :

Lettre	O	K	P	O	U	R	L	U	N	D	I	/
M	14	10	15	14	20	17	11	20	13	03	08	00

Afin d'obtenir exactement 6 blocs de 2 lettres, elle ajoute deux zéros à la fin du chiffre.
Alice va numériser les digrammes de la manière suivante :

— Le digramme OK devient $d1 = 14 \times 26^1 + 10 = 374$.

— Le digramme PO devient $d2 = 15 \times 26^1 + 14 = 404$.

— Etc...

En utilisant la clé publique de Bob, elle obtient ainsi :

	OK	PO	UR	LU	ND	I/
M	374	404	537	306	341	208
$M' = M^5 (mod\ 1943)$	1932	635	68	1705	71	660
conversion	CWY	YL	CQ	CNP	CT	ZK

Elle peut envoyer le message soit directement sous sa forme numérique : 1932 635 68 1705 71 660 soit en convertissant ces nombres, selon le même principe, en lettres :

— $1932 = 2 \times 26^2 + 22 \times 26 + 8$qui correspond au trigramme CWY

— $635 = 24 \times 26 + 11$ qui correspond au digramme YL.

— Etc...

Elle enverra donc le message : CWY YL CQ CNP CT ZK
Bob recevant ce message, il le décrypte à l'aide de sa clé privée (n = 1943, d = 1109) :

M'	1932	635	68	1705	71	660
$M = (M')^{1109} (mod\ 1943)$	374	404	537	306	341	208
décomposition	$14 \cdot 26 + 10$	$15 \cdot 26 + 14$	$20 \cdot 26 + 17$	$11 \cdot 26 + 20$	$13 \cdot 26 + 03$	$08 \cdot 26 + 00$
	OK	PO	UR	LU	ND	IA

Le A terminal étant dû à la technique d'encryptage, il doit donc être supprimé.