بسم الله الرحمن الرحيم

الأستاذ، سعد شكري
باكالوريا علوم رياضية

Professeur, Saad Choukri
Terminale SM

الموضوع 1 في الحسابيات. التشفير

ملخص، يقدم هذا الموضوع أربع طرق للتشفير مبنية على الحسابيات في $\mathbb{Z}$، تشفير يوليوس قيصر بالإزاحة، ونظام RSA المعتمد على الأعداد الأولية ومبرهنة فيرما، والتشفير التآلفي $x \mapsto ax + b$ بتردد 26، والتشفير بالضرب. في كل نظام نشفر كلمات ونفك شفرات أخرى باستعمال الموافقات ومبرهنة بوزو وخوارزمية أقليدس.

تقديم، التشفير علم يهم ابتكار أنظمة شيفرات (فن سري) أو فك شيفرات لرسائل أو نصوص سرية، ويبحث هذا العلم في الكتابات السرية أو الخفية.

الهدف من التشفير هو تمكين شخصين من التواصل بينهما بلغة سرية، أحدهما مرسل والآخر مستقبل. المرسل يبعث رسالة باستعمال فن أو نظمة تشفير بوضع تعليمات خاصة لا يمكن كشفها وتضمن أكبر قدر من السرية. أما المستقبل للرسالة فيملك وحده مفتاح فك الشيفرة أو الفن.

اصطلاح، فيما يلي، سنعتمد المصطلحات التالية،

- «تحديد كلمة بالمرموز» يعني تشفير هذه الكلمة في نظمة تشفير.
- «تحديد كلمة بالواضح» يعني فك الشيفرة لهذه الكلمة في نظمة تشفير.

1. نظمة تشفير يوليوس قيصر (Jules César)

تعتمد نظمة تشفير يوليوس قيصر على «الإزاحة الحسابية» للحروف الأبجدية وذلك كالتالي،

- نرقم الحروف A و B و C و ... و Z على التوالي من 0 إلى 25،

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

- نشفر كل عدد x من هذه اللائحة بالعدد $r(x)$ بحيث $r(x)$ هو باقي قسمة $x + k$ على 26، و k هو مفتاح التشفير الذي يحتفظ به سرا، أي أن $x + k \equiv r(x)\ [26]$.

1) تشفير

(a) تحقق أن الكلمة بالمرموز الموافقة للكلمة بالواضح SECRET هي JVTIVK في الحالة $k = 17$.

(b) حدد الكلمة بالمرموز الموافقة للكلمة بالواضح CRYPTAGE حيث مفتاح التشفير هو $k = 19$.

2) فك تشفير

(a) باعتبار $x \equiv r(x) - k \ [26]$، تحقق أن الكلمة بالواضح الموافقة للكلمة بالمرموز PHVVDJH هي MESSAGE حيث مفتاح التشفير هو $k = 3$.

(b) فك تشفير الجملة OH PHVVDJH] HQ FRGHU GH DUW O HVW FUBSWDJH [حيث مفتاح التشفير هو $k = 3$.

2. نظمة التشفير RSA

تقديم، تم اختراع هذه النظمة من طرف ثلاثة رياضيين، Rivest Ron و Shamir Adi و Len Adleman. وتعتبر هذه النظمة للتشفير الأكثر فعالية من حيث ضمان السرية نظرا للصعوبات التي تطرحها على مستوى فك التشفير، وهي الأكثر استعمالا حاليا في عدة مجالات. وما يجعل هذه النظمة فريدة من نوعها هو أن خوارزمية التشفير التي تعتمدها وكذلك مفتاح التشفير معلومان من طرف العموم، ولكن شخصا واحدا فقط هو الذي يمكنه فك الشيفرة. وتعتمد هذه النظمة على الخاصيتين (P_1) و (P_2) التاليتين، p و q عددان صحيحان طبيعيان ومختلفان وأوليان و $n = pq$، و e عدد صحيح طبيعي بحيث $1 < e < (p-1)(q-1)$ و e أولي مع $(p-1)(q-1)$.

(P_1) يوجد عدد صحيح وحيد d بحيث $1 < d < (p-1)(q-1)$ و $ed \equiv 1 \ [(p-1)(q-1)]$.

(P_2) $\left(\forall (a,b) \in \mathbb{N}^2\right) \quad b \equiv a^e \ [n] \ \Rightarrow \ a \equiv b^d \ [n]$.

مثال، يريد مصطفى بعث الرسالة «NON» لأحمد. طريقة التشفير وفك التشفير هما كالتالي،

- **إنشاء مفتاح التشفير العمومي من طرف أحمد.** يختار أحمد p و q ويحسب الجداء $n = pq$ ويختار e ثم يرسل لمصطفى المفتاح $(\text{RSA}; n; e)$ عبر البريد الإلكتروني (مثلا)، ولكن يحتفظ سرا بـ p و q و d. اختار أحمد $p = 13$ و $q = 17$ و $e = 5$ (لدينا $n = pq = 221$ و $(p-1)(q-1) = 192$ و $5 \wedge 192 = 1$).

- **تشفير الرسالة من طرف مصطفى.** في نظمة التشفير RSA يتم ترقيم الحروف الأبجدية A و B و ... و Z من 1 إلى 26. يكتب مصطفى أولا الرسالة «NON» على الشكل «14 15 14» (حسب الترقيم بلائحة الحروف). يحسب مصطفى باقي قسمة كل من 14^e و 15^e على n فيجد، $14^5 \equiv 131 \ [221]$ و $15^5 \equiv 19 \ [221]$. يرسل مصطفى لأحمد الرسالة المشفرة «131 19 131».

- **فك الشيفرة للكلمة «131 19 131» من طرف أحمد.** أحمد الذي وحده يعلم p و q، عليه أولا حساب d حيث $1 < d < 192$ و $ed \equiv 1 \ [(p-1)(q-1)]$، أي $ed \equiv 1 \ [192]$، إذن

$(\exists q \in \mathbb{Z})\ 5d - 192q = 1$). باستعمال خوارزمية أقليدس، يمكن أحمد من حل هذه المعادلة الديوفانتية فيوجد $d = 77$. يبقى إذن على أحمد تحديد باقي قسمة كل من 131^{77} و 19^{77} على 221. وجد أحمد $131^{77} \equiv 14\ [221]$ و $19^{77} \equiv 15\ [221]$، وبالاعتماد على الخاصية (P_2) يحصل أحمد على الرسالة «14 15 14» الموافقة للكلمة «NON».

تمرين، أعط طريقة تشفير وفك التشفير للكلمة «NON» باستعمال المفتاح $(\mathrm{RSA}; n; e) = (\mathrm{RSA}; 323; 7)$.

3. نظمة التشفير التآلفي

تعتمد هذه النظمة على تشفير كل عدد x $(0 \leqslant x \leqslant 25)$ بالعدد $r(x)$ باقي قسمة $ax + b$ على 26 حيث a أولي مع 26 و $b \in \mathbb{N}$، أي،

$$\begin{cases} r(x) \equiv ax + b\ [26] \\ a \wedge 26 = 1 \end{cases}$$

الزوج (a, b) هو مفتاح التشفير الذي يحتفظ به سرا.

طريقة تحديد x لفك التشفير. لدينا $a \wedge 26 = 1$، إذن حسب مبرهنة بوزو، يوجد عددان صحيحان a' و v بحيث $aa' + 26v = 1$، أو أيضا $aa' \equiv 1\ [26]$ (العدد a' يسمى مقلوب a في الموافقة بتردد 26). بما أن، $r(x) \equiv ax + b\ [26]$ (1)، فإن، $a'r(x) \equiv x + a'b\ [26]$، إذن، $x \equiv a'r(x) - a'b\ [26]$ (2). إذن التحويل التآلفي (1) يمكن من التشفير، والتحويل التآلفي (2) يمكن من فك التشفير وهو التحويل العكسي للتحويل (1).

1) تشفير

(a) تحقق أن الكلمة بالمرموز الموافقة للكلمة بالواضح MATH باستعمال مفتاح التشفير $(a, b) = (7, 10)$ هي الكلمة QKNH.

(b) شفر الكلمة GEOMETRIE في نظمة التشفير التآلفي ذات المفتاح السري $(a, b) = (11, 3)$.

2) فك تشفير

(a) نعتبر الكلمة بالمرموز JEAOSUM في نظمة التشفير التآلفي ذات المفتاح السري $(a, b) = (7, 10)$.

- تحقق أن، $7a' \equiv 1\ [26]$ و $x \equiv \big(r(x) - 10\big)a'\ [26]$ (انظر العلاقة (2) أعلاه).
- باستعمال خوارزمية أقليدس، حدد a' ثم تحقق من النتائج المتوصل إليها بالجدول التالي، محددا الكلمة بالواضح الموافقة للكلمة بالمرموز المقترحة.

الحروف بالواضح	A	B	C	D	E	F	G	H	I	J	K	L	M
وترقيمها	0	1	2	3	4	5	6	7	8	9	10	11	12
الحروف بالمرموز	10	17	24	5	12	19	0	7	14	21	2	9	16
وترقيمها	K	R	Y	F	M	T	A	H	O	V	C	J	Q

N	O	P	Q	R	S	T	U	V	W	X	Y	Z	الحروف بالواضح
13	14	15	16	17	18	19	20	21	22	23	24	25	وترقيمها
23	4	11	18	25	6	13	20	1	8	15	22	3	الحروف بالمرموز
X	E	L	S	Z	G	N	U	B	I	P	W	D	وترقيمها

(b) فك تشفير الكلمة KJAMRZM في نظمة التشفير التآلفي ذات المفتاح السري $(a, b) = (7, 10)$.

4. التشفير بعملية الضرب

تقتضي طريقة التشفير للكلمة ORDINATEUR في نظمة التشفير بالضرب في 7 (مثلا) ضرب رتبة كل حرف من هذه الكلمة في لائحة الحروف الأبجدية (رتبة A هي 1 ورتبة Z هي 26) في 7 ثم تحديد بواقي قسمات هذه الجداءات على 26. اللائحة L المكونة من هذه البواقي تسمى تشفيرا لهذه الكلمة في نظمة التشفير بالضرب ذات المفتاح السري 7.

(1) (a) حدد رتبة حروف الكلمة ORDINATEUR في لائحة الحروف الأبجدية.

(b) حدد اللائحة L ثم أعط الكلمة بالمرموز الموافقة لها.

(2) (a) تحقق أن $26 \wedge 7 = 1$ وحدد عددين صحيحين طبيعيين u و v بحيث $7u - 26v = 1$.

(b) كون اللائحة L' المكونة من بواقي قسمات جداءات أعداد اللائحة L في u على 26. هل يمكن القول إن L' هو مفتاح فك التشفير؟

(3) فك تشفير الرسالة،

7 9 23 16	1 23 16	14 3 24 3 12 16 3

باعتبار مفتاح التشفير هو 11.

Sujet d'étude 1 en Arithmétique. La cryptographie

Résumé, Ce sujet présente quatre méthodes de chiffrement fondées sur l'arithmétique dans $\mathbb{Z}$, le chiffrement de Jules César par décalage, le système RSA reposant sur les nombres premiers et le théorème de Fermat, le chiffrement affine $x \mapsto ax+b$ modulo 26 et le chiffrement multiplicatif. Pour chaque système, on chiffre des mots et on en déchiffre d'autres à l'aide des congruences, du théorème de Bézout et de l'algorithme d'Euclide.

Présentation, la cryptographie est la science qui s'intéresse à la conception de systèmes de chiffrement (un art secret) ou au déchiffrement de messages ou de textes secrets ; elle étudie les écritures secrètes ou cachées.
Le but de la cryptographie est de permettre à deux personnes de communiquer dans un langage secret, l'une étant l'émetteur et l'autre le récepteur. L'émetteur envoie un message à l'aide d'un procédé ou d'un système de chiffrement, en fixant des instructions particulières impossibles à découvrir et qui garantissent le plus haut degré de confidentialité. Le récepteur du message est seul à détenir la clé de déchiffrement.
Terminologie, dans la suite, on adopte les termes suivants,

- « déterminer le mot codé » signifie chiffrer ce mot dans un système de chiffrement ;
- « déterminer le mot en clair » signifie déchiffrer ce mot dans un système de chiffrement.

1. Le chiffrement de Jules César

Le chiffrement de Jules César repose sur un « décalage arithmétique » des lettres de l'alphabet, de la manière suivante,

- on numérote les lettres A, B, C, ..., Z respectivement de 0 à 25,

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

- on code chaque nombre x de ce tableau par le nombre $r(x)$, reste de la division de $x+k$ par 26, où k est la clé de chiffrement gardée secrète, c'est-à-dire $x+k \equiv r(x)\ [26]$.

1) Chiffrement

(a) Vérifier que le mot codé correspondant au mot en clair SECRET est JVTIVK lorsque $k = 17$.

(b) Déterminer le mot codé correspondant au mot en clair CRYPTAGE lorsque la clé de chiffrement est $k = 19$.

2) Déchiffrement

(a) Sachant que $x \equiv r(x) - k$ [26], vérifier que le mot en clair correspondant au mot codé PHVVDJH est MESSAGE lorsque la clé de chiffrement est $k = 3$.

(b) Déchiffrer la phrase [OH FUBSWDJH HVW O DUW GH FRGHU HQ PHVVDJH] dont la clé de chiffrement est $k = 3$.

2. Le système de chiffrement RSA

Présentation, ce système a été inventé par trois mathématiciens, Ron Rivest, Adi Shamir et Len Adleman. Il est considéré comme le système de chiffrement le plus efficace pour garantir la confidentialité, en raison des difficultés qu'il oppose au déchiffrement, et c'est le plus utilisé actuellement dans de nombreux domaines. Ce qui le rend unique, c'est que l'algorithme de chiffrement et la clé de chiffrement sont connus de tous, mais qu'une seule personne peut déchiffrer. Ce système repose sur les deux propriétés (P_1) et (P_2) suivantes.
p et q sont deux entiers naturels premiers distincts, $n = pq$, et e est un entier naturel tel que $1 < e < (p-1)(q-1)$ et e premier avec $(p-1)(q-1)$.

(P_1) Il existe un unique entier d tel que $1 < d < (p-1)(q-1)$ et $ed \equiv 1\ [(p-1)(q-1)]$.

(P_2) $\big(\forall (a,b) \in \mathbb{N}^2\big) \quad b \equiv a^e\ [n] \ \Rightarrow\ a \equiv b^d\ [n]$.

Exemple, Mustapha veut envoyer le message « NON » à Ahmed. Le chiffrement et le déchiffrement se font ainsi,

- **Création de la clé publique par Ahmed.** Ahmed choisit p et q, calcule le produit $n = pq$, choisit e puis envoie à Mustapha la clé (RSA; n; e) par courrier électronique (par exemple), mais garde secrets p, q et d. Ahmed a choisi $p = 13$, $q = 17$ et $e = 5$ (on a $n = pq = 221$, $(p-1)(q-1) = 192$ et $5 \wedge 192 = 1$).

- **Chiffrement du message par Mustapha.** Dans le système RSA, les lettres A, B, ..., Z sont numérotées de 1 à 26. Mustapha écrit d'abord le message « NON » sous la forme « 14 15 14 » (selon la numérotation de l'alphabet). Mustapha calcule les restes des divisions de 14e et 15e par n et trouve, $14^5 \equiv 131$ [221] et $15^5 \equiv 19$ [221]. Mustapha envoie à Ahmed le message chiffré « 131 19 131 ».

- **Déchiffrement du mot « 131 19 131 » par Ahmed.** Ahmed, seul à connaître p et q, doit d'abord calculer d tel que $1 < d < 192$ et $ed \equiv 1\ [(p-1)(q-1)]$, c'est-à-dire $ed \equiv 1\ [192]$; donc $(\exists q \in \mathbb{Z})\ 5d - 192q = 1$. L'algorithme d'Euclide permet à Ahmed de résoudre cette équation diophantienne et il trouve $d = 77$. Il reste à Ahmed à déterminer les restes des divisions de 131^{77} et 19^{77} par 221. Ahmed trouve $131^{77} \equiv 14\ [221]$ et $19^{77} \equiv 15\ [221]$; grâce à la propriété (P_2), il obtient le message « 14 15 14 » correspondant au mot « NON ».

Exercice, donner le chiffrement et le déchiffrement du mot « NON » avec la clé $(\text{RSA}; n; e) = (\text{RSA}; 323; 7)$.

3. Le chiffrement affine

Ce système consiste à coder chaque nombre x $(0 \leqslant x \leqslant 25)$ par le nombre $r(x)$, reste de la division de $ax + b$ par 26, où a est premier avec 26 et $b \in \mathbb{N}$, c'est-à-dire

$$\begin{cases} r(x) \equiv ax + b\ [26] \\ a \wedge 26 = 1 \end{cases}$$

Le couple (a, b) est la clé de chiffrement, gardée secrète.

Détermination de x pour le déchiffrement. On a $a \wedge 26 = 1$; donc, d'après le théorème de Bézout, il existe deux entiers a' et v tels que $aa' + 26v = 1$, ou encore $aa' \equiv 1\ [26]$ (l'entier a' est appelé inverse de a modulo 26). Comme, (1) $r(x) \equiv ax + b\ [26]$, on a, $a'r(x) \equiv x + a'b\ [26]$, donc, (2) $x \equiv a'r(x) - a'b\ [26]$. Ainsi la transformation affine (1) permet de chiffrer, et la transformation affine (2), réciproque de (1), permet de déchiffrer.

1) Chiffrement

(a) Vérifier que le mot codé correspondant au mot en clair MATH avec la clé $(a, b) = (7, 10)$ est QKNH.

(b) Chiffrer le mot GEOMETRIE dans le système affine de clé secrète $(a, b) = (11, 3)$.

2) Déchiffrement

(a) On considère le mot codé JEAOSUM dans le système affine de clé secrète $(a, b) = (7, 10)$.

- Vérifier que, $7a' \equiv 1\ [26]$ et $x \equiv \big(r(x) - 10\big)a'\ [26]$ (voir la relation (2) ci-dessus).
- À l'aide de l'algorithme d'Euclide, déterminer a', puis vérifier les résultats obtenus à l'aide du tableau suivant, en déterminant le mot en clair correspondant au mot codé proposé.

Lettres en clair	A	B	C	D	E	F	G	H	I	J	K	L	M
et leurs rangs	0	1	2	3	4	5	6	7	8	9	10	11	12
Lettres codées	10	17	24	5	12	19	0	7	14	21	2	9	16
et leurs rangs	K	R	Y	F	M	T	A	H	O	V	C	J	Q

Lettres en clair	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
et leurs rangs	13	14	15	16	17	18	19	20	21	22	23	24	25
Lettres codées	23	4	11	18	25	6	13	20	1	8	15	22	3
et leurs rangs	X	E	L	S	Z	G	N	U	B	I	P	W	D

(b) Déchiffrer le mot KJAMRZM dans le système affine de clé secrète $(a, b) = (7, 10)$.

4. Le chiffrement multiplicatif

Pour chiffrer le mot ORDINATEUR dans le système de chiffrement par multiplication par 7 (par exemple), on multiplie par 7 le rang de chaque lettre de ce mot dans l'alphabet (le rang de A est 1, celui de Z est 26), puis on détermine les restes des divisions de ces produits par 26. La liste L formée de ces restes est appelée chiffrement de ce mot dans le système multiplicatif de clé secrète 7.

(1) (a) Déterminer le rang des lettres du mot ORDINATEUR dans l'alphabet.

(b) Déterminer la liste L, puis donner le mot codé correspondant.

(2) (a) Vérifier que $26 \wedge 7 = 1$ et déterminer deux entiers naturels u et v tels que $7u - 26v = 1$.

(b) Former la liste L' des restes des divisions par 26 des produits par u des nombres de la liste L. Peut-on dire que L' est la clé de déchiffrement ?

(3) Déchiffrer le message

14 3 24 3 12 16 3 | 1 23 16 | 7 9 23 16

sachant que la clé de chiffrement est 11.

Summary, This topic presents four encryption methods based on arithmetic in $\mathbb{Z}$, Julius Caesar's shift cipher, the RSA system based on prime numbers and Fermat's theorem, the affine cipher $x \mapsto ax + b$ modulo 26 and the multiplicative cipher. For each system, words are encrypted and others decrypted using congruences, Bézout's theorem and the Euclidean algorithm.

Introduction, cryptography is the science concerned with designing cipher systems (a secret art) or breaking the ciphers of secret messages or texts; it studies secret or hidden writing.
The aim of cryptography is to allow two people to communicate in a secret language, one being the sender and the other the receiver. The sender transmits a message using a cipher method or system, setting special instructions that cannot be uncovered and that guarantee the highest degree of secrecy. Only the receiver of the message holds the key to decipher it.
Terminology, in what follows we use the following terms,

- "determining the encoded word" means encrypting this word in a cipher system;
- "determining the plain word" means decrypting this word in a cipher system.

1. Julius Caesar's cipher

Julius Caesar's cipher relies on an "arithmetic shift" of the letters of the alphabet, as follows,

- the letters A, B, C, ..., Z are numbered from 0 to 25 respectively,

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

- each number x of this table is encoded by the number $r(x)$, the remainder of the division of $x + k$ by 26, where k is the encryption key kept secret, that is $x + k \equiv r(x)$ [26].

1) Encryption

(a) Check that the encoded word corresponding to the plain word SECRET is JVTIVK when $k = 17$.

(b) Determine the encoded word corresponding to the plain word CRYPTAGE when the encryption key is $k = 19$.

2) Decryption

(a) Given that $x \equiv r(x) - k$ [26], check that the plain word corresponding to the encoded word PHVVDJH is MESSAGE when the encryption key is $k = 3$.

(b) Decrypt the sentence [OH FUBSWDJH HVW O DUW GH FRGHU HQ PHVVDJH] whose encryption key is $k = 3$.

2. The RSA cipher system

Introduction, this system was invented by three mathematicians, Ron Rivest, Adi Shamir and Len Adleman. It is regarded as the most effective cipher system for guaranteeing secrecy, because of the difficulties it raises for decryption, and it is currently the most widely used in many fields. What makes it unique is that its encryption algorithm and encryption key are public, yet only one person is able to decrypt. The system relies on the following two properties (P_1) and (P_2).
p and q are two distinct prime natural numbers, $n = pq$, and e is a natural number such that $1 < e < (p-1)(q-1)$ and e is coprime with $(p-1)(q-1)$.

(P_1) There exists a unique integer d such that $1 < d < (p-1)(q-1)$ and $ed \equiv 1\ [(p-1)(q-1)]$.

(P_2) $\big(\forall (a,b) \in \mathbb{N}^2\big) \quad b \equiv a^e\ [n] \ \Rightarrow\ a \equiv b^d\ [n]$.

Example, Mustapha wants to send the message "NON" to Ahmed. Encryption and decryption proceed as follows,

- **Creation of the public key by Ahmed.** Ahmed chooses p and q, computes the product $n = pq$, chooses e and sends Mustapha the key $(\text{RSA}; n; e)$ by e-mail (for example), but keeps p, q and d secret. Ahmed chose $p = 13$, $q = 17$ and $e = 5$ (we have $n = pq = 221$, $(p-1)(q-1) = 192$ and $5 \wedge 192 = 1$).

- **Encryption of the message by Mustapha.** In the RSA system, the letters A, B, ..., Z are numbered from 1 to 26. Mustapha first writes the message "NON" as "14 15 14" (according to the numbering of the alphabet). Mustapha computes the remainders of the divisions of 14^e and 15^e by n and finds, $14^5 \equiv 131\ [221]$ and $15^5 \equiv 19\ [221]$. Mustapha sends Ahmed the encrypted message "131 19 131".

- **Decryption of the word "131 19 131" by Ahmed.** Ahmed, the only one who knows p and q, must first compute d such that $1 < d < 192$ and $ed \equiv 1\ [(p-1)(q-1)]$, that is $ed \equiv 1\ [192]$; hence $(\exists q \in \mathbb{Z})\ 5d - 192q =$

1. The Euclidean algorithm allows Ahmed to solve this Diophantine equation and he finds $d = 77$. It remains for Ahmed to find the remainders of the divisions of 131^{77} and 19^{77} by 221. Ahmed finds $131^{77} \equiv 14\ [221]$ and $19^{77} \equiv 15\ [221]$; using property (P_2), he obtains the message "14 15 14" corresponding to the word "NON".

Exercise, give the encryption and decryption of the word "NON" using the key $(\text{RSA}; n; e) = (\text{RSA}; 323; 7)$.

3. The affine cipher

This system encodes each number x $(0 \leqslant x \leqslant 25)$ by the number $r(x)$, the remainder of the division of $ax + b$ by 26, where a is coprime with 26 and $b \in \mathbb{N}$, that is

$$\begin{cases} r(x) \equiv ax + b\ [26] \\ a \wedge 26 = 1 \end{cases}$$

The pair (a, b) is the encryption key, kept secret.

Finding x to decrypt. We have $a \wedge 26 = 1$; hence, by Bézout's theorem, there exist two integers a' and v such that $aa' + 26v = 1$, or equivalently $aa' \equiv 1\ [26]$ (the integer a' is called the inverse of a modulo 26). Since, (1) $r(x) \equiv ax + b\ [26]$, we get, $a'r(x) \equiv x + a'b\ [26]$, hence, (2) $x \equiv a'r(x) - a'b\ [26]$. Thus the affine transformation (1) is used to encrypt, and the affine transformation (2), the inverse of (1), is used to decrypt.

1) Encryption

(a) Check that the encoded word corresponding to the plain word MATH with the key $(a, b) = (7, 10)$ is QKNH.

(b) Encrypt the word GEOMETRIE in the affine system with secret key $(a, b) = (11, 3)$.

2) Decryption

(a) Consider the encoded word JEAOSUM in the affine system with secret key $(a, b) = (7, 10)$.

- Check that, $7a' \equiv 1\ [26]$ and $x \equiv \big(r(x) - 10\big)a'\ [26]$ (see relation (2) above).
- Using the Euclidean algorithm, determine a', then check the results obtained with the following table, determining the plain word corresponding to the given encoded word.

Plain letters	A	B	C	D	E	F	G	H	I	J	K	L	M
and their ranks	0	1	2	3	4	5	6	7	8	9	10	11	12
Encoded letters	10	17	24	5	12	19	0	7	14	21	2	9	16
and their ranks	K	R	Y	F	M	T	A	H	O	V	C	J	Q

Plain letters	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
and their ranks	13	14	15	16	17	18	19	20	21	22	23	24	25
Encoded letters	23	4	11	18	25	6	13	20	1	8	15	22	3
and their ranks	X	E	L	S	Z	G	N	U	B	I	P	W	D

(b) Decrypt the word KJAMRZM in the affine system with secret key $(a, b) = (7, 10)$.

4. The multiplicative cipher

To encrypt the word ORDINATEUR in the multiplicative cipher system with multiplier 7 (for example), the rank of each letter of the word in the alphabet (A has rank 1, Z has rank 26) is multiplied by 7, then the remainders of the divisions of these products by 26 are determined. The list L formed by these remainders is called the encryption of the word in the multiplicative system with secret key 7.

(1) (a) Determine the ranks of the letters of the word ORDINATEUR in the alphabet.

(b) Determine the list L, then give the corresponding encoded word.

(2) (a) Check that $26 \wedge 7 = 1$ and find two natural numbers u and v such that $7u - 26v = 1$.

(b) Form the list L' of the remainders of the divisions by 26 of the products by u of the numbers in the list L. Can we say that L' is the decryption key?

(3) Decrypt the message

14 3 24 3 12 16 3 | 1 23 16 | 7 9 23 16

given that the encryption key is 11.