République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université Batna-2
Faculté des Mathématiques et de l'Informatique
Dép. Informatique

TD Nº 01

Exercice 01 :

A- Soit les messages suivants :
1- « 90% of the time is spent in 10% of the code. » Dixit Robert Sedgewick
2- Il existe 10 types de personnes ceux qui comprennent l'informatique et les autres.
3- Instead of thinking about things, think about possibilities.
4- « Un problème sans solution est un problème mal posé. » Dixit Albert Einstein

Si l'on sait qu'une transmission sécurisée entre Alice et Bob se fait via le chiffre de César, avec une clé de chiffrement K=3 ; et que$\forall\, c \in M_i \; alors \; c \in \{\overline{A-Z}; \overline{a-z}; \overline{0-9}\}$, calculer alors les M_i' correspondants tel que $M_i' = C_k(M_i)$.

B- Si pour des raisons de sécurité, Alice et Bob décident de changer la clé de chiffrement K=-3 ; et décident de continue leur échange, quels seraient alors les M_i' correspondants aux messages suivant :
1- « Si tu révèles ton secret au vent, tu ne dois pas lui reprocher de le révéler à l'arbre. » Dixit Gibran Khalil Gibran.

2- « Il faut toujours se réserver le droit de rire le lendemain de ses idées de la veille. » Dixit Napoléon Bonaparte

Exercice 02 :

A- Alice et Bob décident de changer de méthode de chiffrement. Ils optent pour un chiffrement par transposition, et utilisent la clé **K**=*grain*.
1- « La valeur d'un homme tient dans sa capacité à donner et non dans sa capacité à recevoir » Dixit Albert Einstein
2- « Cookie : Anciennement petit gâteau sucré, qu'on acceptait avec plaisir. Aujourd'hui : petit fichier informatique drôlement salé, qu'il faut refuser avec véhémence. » Dixit Luc Fayard

B- Alice et Bob s'échange les messages suivants en utilisant toujours la même technique mais avec la clé K=*crypto*. Retrouver alors les messages en clair :
1- « efinn□oiartmql,u□eaii□nmasrtiua□otnianmuegt□lea□pasusine□cdeclcaul.pn□□oet□uetr upel□sle□tptpt□□eln□uistgleile□.n□t» Dixit Bernard Werber
2- «Uopnr□gemrma□rfionmuiaqteta□if□u□cqeeso□uv□ail□uvi□dztfe□□da□ei,rpe□acs□veq □uoo□uvsuqzl□eufl'□ia□es.s» Dixit Loi Murphy

Exercice 03 :

Alice et Bob décident de numériser leurs procédures de Chiffrement/Déchiffrement ; écrivez alors un programme permettant à Alice et Bob d'échanger des messages chiffrés et de les déchiffrer tout en ayant la possibilité à chaque fois de choisir la méthode (entre substitution et transposition) et de pouvoir changer la clé.

République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université Batna-2
Faculté des Mathématiques et de l'Informatique
Dép. Informatique

Solution TD Nº 01

Exercice 01 :

A- Puisqu'on utilise juste l'alphabet$\{\overline{A-Z};\overline{a-z};\overline{0-9}\}$ avec une clé K=3 on aura :

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
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

Et pour les chiffres

0	1	2	3	4	5	6	7	8	9
3=(0+3)mod10	4	5	6	7	8	9	0=(7+3)mod10	1	2

Les caractères spéciaux restent tells qu'ils sont, ils ne font pas partie de l'alphabet avec lequel on travaille.

1- **C** (« 90% of the time is spent in 10% of the code. ») = «23% qh vjg vkog ku urgpv kp 43% qh vjg eqfg . »
B- Une variante du chiffrement de César avec un décalage à gauche (K=-3)

Commented [DJR1]: Je démarre la solution avec les étudiants et je les laisse finir le chiffrement du message, une fois terminé, au tableau qlq'un le fait on corrige ensemble et on passe au deuxième message et ainsi de suite.

Exercice 02 :

A- Transposition = changer de position (Le principe : Ordonner la matrice dans laquelle est mis le msg suivant l'ordre alphabétique des caractères de la première ligne (et donc du mot clé)

g	**r**	**a**	**i**	**n**
L	a	□	v	a
l	e	u	r	□
d	‘	u	n	□
h	o	M	m	e
t	l	e	n	t
□	d	a	n	s
□	s	a	□	c
a	p	a	C	i
t	é	□	à	□
d	o	n	n	e
r	□	e	t	□
n	o	n	□	d
a	n	s	□	s
a	□	c	a	p
a	c	i	t	é
□	à	□	r	e
c	e	v	o	i
r	□	□	□	□

a	**g**	**i**	**n**	**r**
□	L	v	a	a
u	l	r	□	e
u	d	n	□	‘
m	h	m	e	o
e	t	n	t	i
a	□	n	s	d
a	□	□	c	s
a	a	c	i	p
□	t	à	□	é
n	d	n	e	o
e	r	t	□	□
n	n	□	d	o
s	a	□	s	n
c	a	a	p	□
i	a	t	é	c
□	□	r	e	à
v	c	o	i	e
□	r	□	□	□

Le message après chiffrement est alors :

Commented [DJR2]: En espérant ne pas avoir fait d'erreur lors de la transposition.
Les espaces sont remplacés par □ les miniscules restent miniscules et les majuscules majuscules.

République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université Batna-2
Faculté des Mathématiques et de l'Informatique
Dép. Informatique

« □Lvaaul□eudn□'mhmeoetntia□nsda□□csaacip□tà□éndeoert□□nn□dosa□sncaap□iatéc□reàvcoi e□r□□□»

B- L'idée est de s'exercer à l'opération inverse (le déchiffrement)

c	**o**	**p**	**r**	**t**	**y**		**c**	**r**	**y**	**p**	**t**	**o**
U	o	p	n	r	□		U	n	□	p	r	o
g	e	m	r	m	a		g	r	a	m	m	e
□	r	f	i	o	n		□	i	n	f	o	r
m	u	i	a	q	t		m	a	t	i	q	u
e	t	a	□	i	f		e	□	f	a	i	t
□	u	□	c	q	e		□	c	e	□	q	u
e	s	o	□	u	v		e	□	v	o	u	s
□	a	i	l	□	u		□	l	u	i	□	a
v	i	□	e	d	z		v	e	z	□	d	i
t	f	e	□	□	d		t	□	d	e	□	f
a	□	e	i	,	r		a	i	r	e	,	□
p	e	□	a	c	s		p	a	s	□	c	e
□	v	e	q	□	u		□	q	u	e	□	v
o	o	□	u	v	s		o	u	s	□	v	o
u	q	z	l	□	e		u	l	e	z	□	q
u	f	l	'	□	i		u	'	i	l	□	f
a	□	e	s	.	s		a	s	s	e	.	□

République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université Batna-2
Faculté des Mathématiques et de l'Informatique
Dép. Informatique

TD Nº 02

	1	2	3	4	5
1	a	b	c	d	e
2	f	g	h	i /j	k
3	l	m	n	o	p
4	q	r	s	t	u
5	v	w	x	y	z

Exercice 01 :

Soit le tableau en face.

Le chiffrement avec ce tableau se fait comme suit : Chaque lettre est codée par le numéro de sa ligne||numéro de colonne.

Alice et Bob ont utilisé ce tableau, et le résultat du chiffrement de leur conversation était le suivant :

Alice : « 41451531 154344 1315 13232421214215?»

Bob : «13'154344 3115 13232421214215 1415 353431541215»

Alice : «414524 154344 353431541215?»

Bob : «13'154344 4533 232443443442241533 22421513 »

Alice: « 1544 4324 3433 1543431154112444 453315 5111422411334415 11511513 323444 133115 "4315134542244415"»

1- Découvrez la conversation d'Alice et Bob.
2- En utilisant les résultats de la question précédente, chiffrer le message suivant.

M= « Avant de vouloir qu'un logiciel soit réutilisable, il faudrait d'abord qu'il ait été utilisable - Ralph Johnson».

Exercice 02 :

En utilisant le chiffre de Vigenère et le mot clé K= « sécurité » chiffrez le message suivant :

1- L'intégrité est une composante essentielle de la sécurité. Et pas seulement en informatique !
2- UNIX is basically a simple operating system, but you have to be a genius to understand the simplicity.

Exercice 03 :

Décidant que toutes les clés utilisées jusqu'à maintenant lors de leur communication, n'ont pas été sûres, Alice et Bob veulent générer une clé secrète. Ils utilisent pour cela le protocole Diffie-Helleman, avec les paramètres suivants : p=11, w=7. Alice utilise a=3 et Bob utilise b=6.

1- Quelle est la clé obtenue après calcul ?

Une troisième personne, Charles, rejoins Alice et Bob. Les trois décident de renouveler leur clé avec les données suivantes : p=23, w=3, a=6, b=4, et c=3

2- Calculer la nouvelle clé.

République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université Batna-2
Faculté des Mathématiques et de l'Informatique
Dép. Informatique

Mot clé	Message 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
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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	u	u	v	w	x	y	z

République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université Batna-2
Faculté des Mathématiques et de l'Informatique
Dép. Informatique

Solution TD N° 02

Exercice 01 :

Alice : « 41/45/15/31/ 15/43/44 13/15 13/23/24/21/21/42/15?»

Alice: "quel est ce chiffre?"

Bob : «13'154344 3115 13232421214215 1415 353431541215»

	1	2	3	4	5
1	a	b	c	d	e
2	f	g	h	i /j	k
3	l	m	n	o	p
4	q	r	s	t	u
5	v	w	x	y	z

Bob: "c'est le chiffre de polybe"

Alice : «414524 154344 353431541215?»

Alice:"qui est polybe"

Bob : «13'154344 4533 232443443442241533 22421513 »

Bob:"c'est un historien grec"

Alice: « 1544 4324 3433 15/43/43/11/54 /11/24/44 453315 5111422411334415 11511513 323444 133115 "43/15/13/45/42/24/44/15"»

Alice:"et si on essayait une variante avec mot cle « securite » »

Le tableau devient alors

On chiffre par la suite on appliquant le mm principe.

M= « Avant de vouloir qu'un logiciel soit réutilisable, il faudrait d'abord qu'il ait été utilisable - Ralph Johnson».

M'= « 23/51… »

	1	2	3	4	5
1	s	e	c	u	r
2	i/j	t	a	b	d
3	f	g	H	k	l
4	m	n	o	p	q
5	v	w	x	y	z

Commented [DJR3]: On écrit le mot clé dans le tableau sans répétition des caractères (exp le « e ») une fois terminé on continue à remplir le tableau avec le reste de l'alphabet dans l'ordre et sans répéter les caractères qui sont déjà apparus lors de l'écriture du mot clé.
Le i et le j prennent la mm case

Exercice 02 :

L'intégrité est une composante essentielle de la sécurité. Et pas seulement en informatique !

On répète le mot clé autant de fois qu'il faut sous le message à chiffrer, puis on cherche dans la table de Vigenère l'intersection entre la colonne du caractère du mot clé et la colonne du caractère du message en clair.

Commented [H4]: Voir la table en haut avec les couleurs.

l	'	l	n	t	e	g	r	i	t	e		e	s	t		u	n	e		
s		E	c	u	r	i	t	e	s	e		c	u	r		i	t	e		
e		N	q																	

République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université Batna-2
Faculté des Mathématiques et de l'Informatique
Dép. Informatique

Exercice 03 :

W=7, P=11	
Alice (a=3)	**Bob(b=6)**
$7^3 mod 11 = 2$ $4^3 mod\ 11 = 9$	$7^6 mod\ 11 = 4$ $2^6 mod\ 11 = 9$
La clé commune entre Alice et Bob est 9	
p=23, w=3, a=6, b=4, et c=3	

Alice	Bob	Charles
$3^6 mod 23 = 16$ $4^6 mod 23 = \mathbf{2}$ $3^6 mod 23 = 16$	$3^4 mod 23 = 12$ $16^4 mod 23 = 9$ $\mathbf{2}^4 mod 23 = 16$	$3^3 mod 23 = 4$ $12^3 mod 23 = 3$ $9^3 mod 23 = 16$

République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université Batna-2
Faculté des Mathématiques et de l'Informatique
Dép. Informatique

TD Nº 03

Rappels Mathématiques :

Soit le polynôme de degré 2 $P = aX^2 + bX + C \; avec \; a \neq 0$

Trois cas se présentent alors suivant la valeur du discriminant $\Delta = b^2 - 4ac$:

1- Soit le discriminant $\Delta < 0$ alors le polynôme n'a pas de racine dans R ;
2- Soit le discriminant $\Delta > 0$ alors le polynôme à deux racines $x_1 = \frac{-b-\sqrt{\Delta}}{2a}$ et $x_1 = \frac{-b+\sqrt{\Delta}}{2a}$;
3- Soit le discriminant $\Delta = 0$ alors le polynôme à une racine double $x = \frac{-b}{2a}$.

Propriété :

Si on pose $s = x_1 + x_2$ et $p = x_1.x_2$ alors le polynôme P s'écrit également : $P = a(X^2 - sX + p)$

RSA :

1. Choisir *p* et *q*, deux nombres premiers distincts ;
2. calculer leur produit *n* = *pq*, appelé *module de chiffrement* ;
3. calculer ϕ(*N*) = (*p* - 1)(*q* -1) (c'est la valeur de l'indicatrice d'Euler en *N*) ;
4. choisir un entier naturel *e* **premier** avec ϕ(N) et strictement inférieur à ϕ(N), appelé *exposant de chiffrement* ;
5. calculer l'entier naturel *d*, inverse de *e* modulo ϕ(*N*), et strictement inférieur à ϕ(*N*), appelé *exposant de déchiffrement* ; *d* peut se calculer efficacement par l'algorithme d'Euclide étendu.

Chiffrement : $M' = M^e \; mod \; N$

Déchiffrement : $M \quad = M'^d \; mod \; N$

Inverse modulo et Euclide étendu (*Exemple introductif*[1]***):***

Définition : *u* est un inverse de ***a*** modulo ***n*** s'il existe un entier tel que

Soit deux nombres 120, 23, alors :

Dans ce cas, le reste obtenu à l'avant-dernière ligne donne le PGCD égal à 1 ; c'est-à-dire que 120 et 23 sont premiers entre eux. Maintenant présentons autrement les divisions précédentes :

120 ÷ 23 = 5 reste 5
23 ÷ 5 = 4 reste 3
5 ÷ 3 = 1 reste 2
3 ÷ 2 = 1 reste 1
2 ÷ 1 = 2 reste 0

[1] https://fr.wikipedia.org/wiki/Algorithme_d%27Euclide_%C3%A9tendu dernière consultation 07.05.2016 à 23 : 19

République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université Batna-2
Faculté des Mathématiques et de l'Informatique
Dép. Informatique

Reste	=	Dividende	-	Quotient	×	Diviseur
5	=	120	-	5	×	23
3	=	23	-	4	×	5
2	=	5	-	1	×	3
1	=	3	-	1	×	2
0	=	2	-	2	×	1

Il est possible de possible de représenter les résultats de la manière suivante :

r													=	u	×	a	+	v	×	b
120													=	1	×	120	+	0	×	23
23													=	0	×	120	+	1	×	23
5	=	120	-	5	×	23							=	1	×	120	+	-5	×	23
3	=	23	-	4	×	5	=	1×23	-	4	×	(1×120 - 5×23)	=	-4	×	120	+	21	×	23
2	=	5	-	1	×	3	=	(1×120 - 5×23)	-	1	×	(-4×120 + 21×23)	=	5	×	120	+	-26	×	23
1	=	3	-	1	×	2	=	(-4×120 + 21×23)	-	1	×	(5×120 - 26×23)	=	-9	×	120	+	47	×	23

Suivant la définition précédente 1=(-9)*120+47*23 est de la forme 1=a*u+n*v, ceci signifie que -9 est l'inverse pour la multiplication de 120 modulo 23, parce que $1 = -9 \times 120 \pmod{23}$.

Exercice 01 :

Soit $p = 3$, $q = 11$.

Si Alice et Bob utilisent le chiffrent de RSA. Et qu'Alice choisisse e=3 alors :

1- Quelle est la clé publique d'Alice.
2- Quelle est sa clé secrète.
3- Chiffrer via la clé publique d'Alice le message M=5.
4- Alice et lui décident d'un protocole RSA dans lequel les messages sont des nombres en base 10 que l'on code par bloc de 2 chiffres en base 10. Alice veut envoyer le message 162719.
   a- Ecrire le message codé qu'elle envoie à Bob.
   b- Décoder le message qu'a reçu Bob et vérifier que c'est bien celui qu'a envoyé Alice.

Exercice 02 :

Considérons le système RSA utilisé par Alice et Bob avec p=19 et q=23

1- Calculer N et ;
2- Calculer l'exposant d associé à e=9, puis e=14 ;
3- Calculer l'exposant d associé à e=17.

République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université Batna-2
Faculté des Mathématiques et de l'Informatique
Dép. Informatique

Solution TD N° 03

Exercice 01 :

Soit p = 3, q = 11, e=3

1- La clé publique est e=3

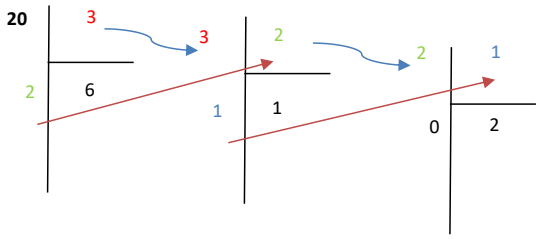
2- La clé privée est d= ?

n=p*q=3*11=33

$\varphi(n) = (p-1) * (q-1) = 2 * 10 = 20$

On cherche 'd' tel que : 1=e*d+ $\varphi(n)$ *k= 3*d+ $20 * k$

R		e	d	+	$\varphi(n)$	k
20		3	0	+	20	1
3		3	1	+	20	0
2	=20-3*6	3	-6	+	20	1
1	=3-2*1 =3-(20-3*6)*1					
	=3 *(1+6)-20	3	7	+	20	-1



Et donc on a : 1= 3*7+20*(-1) d'où **d=7**

3- **On chiffre M=5 :**

Pour chiffrer avec RSA on applique $M^e mod\ n = 5^3 mod\ 33 = 26$

4- **On chiffre M=**162719

a. Ecrire le message codé que Alice envoie à Bob :

M=$(16)_{10}||(27)_{10}||(19)_{10}$ donc :

$M' = M^e mod\ n = (16^3 mod 33)||27^3 mod 33||(19^3 mod 33) = 4||15||28$

b. Décoder le message qu'a reçu Bob et vérifier que c'est bien celui qu'a envoyé Alice :

$M'^d mod 33 = (4^7 mod 33)||(15^7 mod 33)||(28^7 mod 33) = 16||27||19 = M$

CFD