« Le Défi » Fête de la science 2002

Fonctions utiles sur calculatrices: rappel mod(a,n) donne pour résultat le reste de la division euclidienne de a par n. char(n) donne la lettre de code ASCII n. Exemple char(97)="a". Inversement ord("a")=97.

I. Codage Caesar

1. Quel mathématicien, qui comme César aimait diviser pour régner se cache derrière ce code : "**lbjspkl**"
2. César aurait pu envoyer ce message : "**mhvxlvyhqxmdlyxmdlydlqfx**"

II. César étendu ou Cryptographie affine

Le codage César étendu ou cryptographie affine est l'utilisation d'un codage de type $x \mapsto ax+b \text{ modulo } 26$, où *a* et *b* sont deux entiers choisis par les crypteurs. *x* et son image sont les codes attribués aux lettres. Contraintes sur les deux entiers *a* et *b* : 1<*a*<25 et 0<*b*<25. Le cas *a*=1 n'étant autre que le codage César classique.

Le codage ne demande aucune difficulté… et n'est pas l'objet de cet exercice.

But du problème : décrypter le message "**hyyduf**" codé en César étendu de clés (19 ; 7).

Comme indiqué ci-dessus, le codage ne pose pas de problème par exemple pour 'a' (la lettre) nous avons *f*(a)=0 alors *y*=19.0+7=7. La lettre image de "a" par codage est donc "h".

Pour le décodage (qui pourrait se faire par les méthodes statistiques), que faut-il faire ? Contrairement au codage 'simple César', une série de décalages réalisée sur le texte ne rend pas le texte d'origine, il manque de préciser la première lettre de correspondance.

L'idée est d'essayer de déterminer quelle lettre permet d'obtenir une lettre préalablement choisie. Le code de b étant 1, le choix se porte sur celle là parce que… nous travaillons en arithmétique et que 1 fait penser que Bézout n'est peut être pas loin.

Soit *x* le code de la lettre d'image b de code 1. Si *x* est l'antécédent de 1 c'est que $19x+7 \equiv 1 \ [26]$

1. Utiliser judicieusement l'algorithme d'Euclide pour déterminer deux entiers u et v tels que 19u+26v=1.

On pose α=26 et β=19

Euclide	Calculs intermédiaires	Calculs définitifs
26=19.1+7 19=7.2+5 7=5.1+2 5=2.2+$\boxed{1}$ 2=1.2+0	α=β.1+7 β=(α-β).2+5 α-β=(3β-2α).1+2 3β-2α=(3α-4β).2+$\boxed{1}$	7=α-β 5=3β-2α 2=3α-4β $\boxed{1}$=11β-8α **u=11 et v= -8**

Sachant α=26 et β=19, $\boxed{1}$=11β-8α s'écrit 19.11-26.8=1. On trouve u=11 et v= -8 tels que 19u+26v=1.

2. Justifier alors que $19u \equiv 1 \ [26]$.

3. *x* vérifie $19x+7 \equiv 1 \ [26]$ soit $19x \equiv -6 \ [26]$. En déduire que $x \equiv -6u \ [26]$.

Comme $19xu = -6u \ [26]$ et que $19u \equiv 1 \ [26]$… OR u=11 d'où $x \equiv -6.11 \equiv 12 \ [26]$. Ce qui se traduit par « l'antécédent de 'a' c'est 'm' ».

4. Faire de même pour 'c' et 'a' :

On cherche *x* le code de la lettre d'image c de code 2. Si *x* est l'antécédent de 2 c'est que $19x+7 \equiv 2 \ [26]$, i.e. $19x \equiv -5 \ [26]$. D'après ce qui précède, multiplier chaque membre par 11.
Alors $11 \times 9x \equiv -5.11 \equiv 23 \ [26]$. Donc *f*('x')='c', soit « 'x' est l'antécédent de 'c' ».
On cherche *x* le code de la lettre d'image a de code 0. Si *x* est l'antécédent de 0 c'est que $19x+7 \equiv 0 \ [26]$, i.e. $19x \equiv -7 \ [26]$. Alors $11 \times 9x \equiv -7.11 \equiv 1 \ [26]$. Donc *f*('b')='a', « 'b' est l'antécédent de 'a' ».
Remarque : pour passer d'une lettre à sa suivante, il suffit d'ajouter 11 (modulo 26).

Sur ce principe il est possible de construire une liste de correspondance : (ce qui peut se faire par programmation sur calculatrice).

Lettre codée :	a	b	c	etc.
Son code :	0	1	2	
Code de la lettre d'origine :	1	12	23	
Lettre d'origine :	b	m	x	

5. Il ne reste plus qu'à décoder le message donné.
6. Décoder "**xqlkwh**" codé avec les clés (3; 17).

III. Codage Vigenère

Exemple de codage de Vigenère : codage avec la clé 'BAC' Les lettres étant numérotées de 0 à 25, les lettres du message 1 ; 4 ; 7 ; 10 etc. seront décalées d'une unité les lettres 2 ; 5 ; 8 ; 11 etc. seront inchangées, lettres 3 ; 6 ; 9 ; 12 ; etc. seront décalées de deux unités.

Message	V	I	G	E	N	E	R	E
Clé	B	A	C	B	A	C	B	A
Résultat	W	I	I	F	N	G	S	E

On a retrouvé un fragment de parchemin contenant un texte en clair ainsi que sa version cryptée à l'aide de la méthode de Vigenère. Malheureusement le texte chiffré est incomplet.

Q	U	I	S	O	N	T	C	E	S	S	E	R	P	E	N	T	S
S		J	J	O	P	H		V	S	U	S		G	E	P	H	T

Saurez-vous retrouver la clé ?

IV. Arithmétique modulaire

1. Calculer $5^{18} \text{ modulo } 19$.
2. L'entier appartenant à [0,136] et congru à $19^{645} \text{ modulo } 137$ est-il un carré parfait ?

V. RSA

Principe du RSA : Aurélia choisit deux nombres premiers p et q très grands. Elle calcule n=pq et z=(p-1)(q-1) (n étant difficile à factoriser donc le calcul de z l'est aussi). Elle choisit c un nombre premier avec z tel que 0<c<n Les nombres n et c sont les clés publiques de codage. D'après Bézout, il existe u et v tels que $c \times u + z \times v = 1$ ce qui s'écrit aussi $u \times c \equiv 1 [z]$. Alors d=u, est la clé (privée) de décodage d'Aurélia.

Dans ce cas, pour a un entier tel que a<n, $a^c \equiv \alpha [n]$ et $\alpha^d \equiv a [n]$.

Exemple p=5, q=11 deux nombres premiers. n=p.q=55 et z=(p-1)(q-1)=4.10=40. Aurélia choisit c=23 premier avec 40. Par l'algorithme d'Euclide décrit à l'exercice II, elle détermine d tel que $d \times c + v \times z = 1$.

Elle trouve 7.23-4.40=1 d'où $7 \times 23 \equiv 1 [40]$.

Pour le message '2' elle constate $2^{23} \equiv 8 [55]$ et $8^7 \equiv 2 [55]$. Codage… Décodage.

On suppose que la clef RSA d'Aurélia est (333301073927, 33610066727). Celle de Bob est (5397501569, 458897897).
Bob désire faire parvenir à Aurélia la date de sa prochaine visite. Il lui envoie sous la forme d'un entier D (exemple 15021990 pour le 15 février 1990) qu'il a au préalable crypté à l'aide de RSA. Il a envoyé D_1=83899076890.
Sachant que 333301073927 se factorise sous la forme 389219×856333 et que l'exposant secret d'Aurélia est inférieur à 200, pouvez-vous en déduire quand Bob verra de nouveau Aurélia ?

Le jury est souverain dans ses décisions.