Correction du défi de Cryptographie

1.1. On sait qu'il s'agit d'un codage de César dont on ne connaît pas la clé. On peut essayer successivement toutes les clés jusqu'à ce que le mot décodé ait un sens en rapport avec l'indice donné. Comme on effectue un décodage on va décaler les lettres vers la gauche. On obtient :

lbjspkl
kairojk
jzhgnij
iygpmhi
hxfolgh
geenkfg
fvdmjef
eudide

On aurait pu remarquer que la lettre l apparaît deux fois et considérer quelle correspond à une lettre qui revient fréquemment dans la langue française. Effectivement l code e et l'on retrouve Euclide directement en faisant un décalage de 7 lettres vers la gauche.

1.2. On sait que *César* effectuait un décalage de trois vers la droite. On peut décoder immédiatement le message en opérant un décalage de 3 lettres vers la gauche pour obtenir :

jesuisvenujaivujaivaincu

II. Le décryptage repose sur la résolution de l'équation $y = ax + b \mod 26$ où $a; b$ sont les paramètres du cryptosystème et ou y est le numéro de la lettre que l'on cherche à décoder. L'idée générale est de commencer par rechercher u tel que $au = 1 \mod 26$. On s'appuie sur la relation de Bézout qui assure que si a et 26 sont premiers entre eux alors il existe deux entiers $(u ; v)$ tels que $au+26v = 1$ ce qui implique que $au = 1 \mod 26$. La relation de Bézout est donnée par l'algorithme d'Euclide. Pour $(a ; b) = (19 ; 7)$ on trouve $19\times11-26\times8=1$ donc $119\times11=1 \mod 26$. Il ne reste plus qu'à résoudre autant d'équations que nécessaire. Ainsi pour hyyduf, h étant la $7^{\text{ième}}$ lettre de l'alphabet (a est la lettre numéro 0) on résout $19\times x+7=7 \mod 26$ d'où $19\times x=0 \mod 26$.

$$11\times19\times x=11\times0=0 \mod 26$$
$$1\times x=0 \mod 26$$
$$x=0 \mod 26$$

Attention : $x\times y=0 \mod 26$ n'implique pas $x= 0 \mod 26$ ou $y= 0 \mod 26$ comme le montre le contre-exemple $x = 2$ et $y = 13$. On ne peut conclure directement que $19\times x=0 \mod 26$ implique $x = 0 \mod 26$.
Pour les autres lettres on résout les équations :

$19\times x+7=24 \mod 26$ d'où $x=11\times17=5 \mod 26$. Donc y code f.
$19\times x+7=3 \mod 26$ d'où $x=11\times(-4)=8 \mod 26$. Donc d code i.
$19\times x+7=20 \mod 26$ d'où $x=11\times13=13 \mod 26$. Donc u code n.
$19\times x+7=5 \mod 26$ d'où $x=11\times(-2)=4 \mod 26$. Donc f code e.

Finalement hyyduf est le chiffré de affine.

II.6 De même pour la clé (3 ; 17) il faut chercher u tel que $3u = 1 \mod 26$.
On trouve que $3\times9-1\times26=1$ d'où $3\times9=1 \mod 26$.

$3\times x+17=23 \mod 26$ d'où $x=9\times6=2 \mod 26$. Donc x code c.
$3\times x+17=16 \mod 26$ d'où $x=9\times(-1)=17 \mod 26$. Donc q code r.
$3\times x+17=11 \mod 26$ d'où $x=9\times(-6)=24 \mod 26$. Donc l code y.
$3\times x+17=10 \mod 26$ d'où $x=9\times(-7)=15 \mod 26$. Donc k code p.
$3\times x+17=22 \mod 26$ d'où $x=9\times5=19 \mod 26$. Donc w code t.
$3\times x+17=7 \mod 26$ d'où $x=9\times(-10)=14 \mod 26$. Donc h code o.

finalement, le message xqlkwh se décode en crypto.

III. On sait que le message a été codé par la méthode de Vigenère. On commence par chercher la longueur de la clé. On remarque l'existence d'une période de longueur 5. Toutes les 5 lettres, la lettre codée est identique à la lettre décodée. On suppose donc que la clé est de longueur 5.

Comme Q (lettre numéro 16) s'envoie sur S (lettre numéro 18) la première lettre est un C (lettre numéro 2 = 18-16). Comme la deuxième lettre du texte en clair est manquante on s'intéresse aux sixièmes lettres du chiffré et du message en clair qui sont respectivement T et H. Ainsi la deuxième lettre de la clé est O (lettre numéro 14= 7-19 mod 26).

On obtient facilement les autres lettres de la clé pour trouver COBRA.

IV.1 La calculatrice ou le calcul direct donne $5^{18} = 1 \bmod 19$. Ceci est un cas particulier du théorème de Fermat qui dit que $n^{p-1} = 1 \bmod p$ pour p premier et n premier avec p.

IV.2 Comme le nombre 19^{645} nécessite 825 chiffres décimaux; il s'avère trop grand pour une calculatrice standard, et même pour les 89 qui n'acceptent "que" un peu plus de 600 chiffres. On ne peut donc le calculer directement. Il va falloir réduire modulo 137 les calculs intermédiaires. On peut utiliser l'algorithme d'exponentiation binaire gauche - droite en remarquant que 645 = 512+128+4+1. Donc 645 s'écrit $(1010000101)_2$ en binaire.
La suite d'opérations à faire estdonc1 ; 1 ; x ; x^2 ; x^4 ; x^5 ; x^{10} ; x^{20} ; x^{40} ; x^{80} ; x^{160} ; x^{161} ; x^{322} ; x^{644} ; x^{4645}
On remplace donc x par 19 et on réduit les calculs intermédiaires modulo 137. À chaque étape on a seulement besoin d'une élévation au carre ou d'une multiplication par 19. On trouve successivement :
1 ; 1 ; 19 ; 87 ; 34 ; 98 ; 14 ; 59 ; 56 ; 122 ; 88 ; 28 ; 99 ; 74 ; 36.

Donc $19^{645} = 36 \bmod 137$. Et l'on remarque que 36 est un carré parfait.

On pouvait faire plus simple. En remarquant que la calculatrice peut effectuer correctement le calcul $19^{322} \bmod 137 = 99$ il suffit de calculer 99^2 x 19 mod 137 pour obtenir le bon résultat.

Encore plus simple… Puisque 137 est premier le théorème de Fermat assure que $19^{136} = 1 \bmod 137$. Comme 615 = 4 x 136+ 101 alors

$$\begin{aligned} 19^{645} &= 19^{136\times 4} \times 19101 \bmod 137 \\ &= (19^{136})^4 \times 19^{101} \bmod 137 \\ &= 1 \times 19^{101} \bmod 137 \\ &= 19^{101} \bmod 137 \end{aligned}$$

La calculatrice donne alors directement $19^{101} = 36 \bmod 137$.

V. La seule difficulté est le calcul de la de secrète d'Aurélia.
Tout d'abord comme $333301073927 = 389219 \times 856333$; alors
$\varphi(333301073927) = 389219 \times 856333 = 333299828376$.
Ensuite on peut utiliser l'algorithme d'Euclide ou écrire un programme de recherche exhaustive pour trouver l'entier u entre 1 et 200 tel que :
$33610066727 \times u = 1 \bmod \varphi(333301073927)$
L'algorithme d'Euclide donne $33610066727 \times 119 - 333299828376 \times 12 = 1$ d'où
$33610066727 \times 119 = 1 \bmod 333299528376$.
La clé secrète d'Aurélia est donc 119.
Pour trouver la date demandée il faut maintenant calculer $83899076890^{119} \bmod 333301073927$. Par l'algorithme binaire décrit au **IV.** on a : $83899076890^{119} \bmod 333301073927 = 12072003$.

Ainsi Bob et Aurélia ont rendez-vous le 12 juillet 2003.