Décryptage affine

Situation du problème

Un premier travail nous a appris à chiffrer un message à l'aide d'un procédé affine. Nous allons voir ici comment retrouver le message en clair.
Dans un premier temps, nous supposerons la clé de chiffrement connue et nous chercherons à déchiffrer le message.
Dans un deuxième temps, nous verrons comment déterminer cette clé lorsqu'elle est inconnue permettant ainsi d'effectuer un décryptage.

Rappel du principe de chiffrement affine

- On choisi un couple d'entiers $(a;b)$ appelé clé de chiffrement.
- À chaque lettre on associe son rang x dans l'alphabet :

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

- On calcule y le reste de la division euclidienne de $ax+b$ par 26.
- On associe la lettre correspondant au reste y.

Partie A : En connaissant la clé de chiffrement, méthode de déchiffrement

1) Vérifier que pour $a=5$ et $b=22$, la lettre M est codée par la lettre E.
2) La clé de chiffrement est $(7;23)$ et le message codé est XYYMZKSMZ.
   a) Montrer que $7x \equiv y+3\,[26]$.
   b) Justifier l'existence de deux entiers u et v tels que $7u+26v=1$ et en donner une valeur.
   c) En déduire un inverse de 7 modulo 26.
   d) Déchiffrer alors le message XYYMZKSMZ.
3) Montrer que, si la clé est choisie de sorte que a est premier avec 26 la méthode ci-dessus assure le déchiffrement de n'importe quelle lettre.

Partie B : En recherchant la clé de chiffrement, méthode de décryptage

Voici un message codé à l'aide d'un chiffrement affine dont la clé est inconnue.

WXVXGKXVERHFPSVSFPVVXSGWPQKXVXGXTFRYXSMPTSPGXXGXSMKDPGV

Une analyse rapide du message montre que les deux lettres les plus fréquentes sont le X et le V avec respectivement 23 et 21 itérations. Or, dans un texte en français, les lettres les plus fréquentes sont le E, le S et le A.

Soit $(a;b)$ la clé de chiffrement.

1) Supposons que X et V correspondent respectivement à E et S.
   a) Montrer que l'on est ramené à résoudre le système $(\mathcal{S})\begin{cases} 4a+b \equiv 23\,[26] \\ 18a+b \equiv 21\,[26] \end{cases}$
   b) Montrer que $(\mathcal{S}) \Rightarrow 14a \equiv -2\,[26]$ et chercher deux entiers u et v tels que $14u+26v=-2$.
   c) En déduire une valeur de a puis une valeur de b.
   d) Déchiffrer les quatre premières lettres du message.
2) Supposons que X et V correspondent respectivement à S et E.
   a) Montrer que l'on est ramené à résoudre le système $(\mathcal{S}')\begin{cases} 4a+b \equiv 21\,[26] \\ 18a+b \equiv 23\,[26] \end{cases}$
   b) Montrer que $(\mathcal{S}') \Rightarrow 14a \equiv 2\,[26]$ et chercher deux entiers u et v tels que $14u+26v=2$.
   c) En déduire une valeur de a puis une valeur de b.
   d) Déchiffrer les quatre premières lettres du message.
3) Choisir l'hypothèse la plus crédible et utiliser un programme pour automatiser le déchiffrement du message.