Pour transmettre un message secret, on utilise depuis longtemps des systèmes de codage (on parle de cryptographie). Un codage simple consiste à décaler les lettres de l'alphabet. Par exemple le code de César[1] fonctionne ainsi. Dans le même style, on peut remplacer chaque lettre par un symbole. Celui qui connait le nombre de lettres de décalage dans le premier cas ou la correspondance lettre-symbole dans le deuxième peut décrypter (c'est à dire décoder) le message. Mais quelqu'un qui intercepte le message (un ennemi en temps de guerre par exemple) et qui ne connait pas cette correspondance peut aussi assez facilement décrypter le message. En effet, il suffit (pour le code de César) d'essayer les différents décalages possibles. Dans le deuxième cas-plus général-on fait une étude statistique de la fréquence d'apparition des différents symboles. Or on sait qu'en français les lettres les plus fréquentes sont le E, puis le A, ... etc. Et comme dans ces codes une lettre est toujours codée par le même symbole, on peut ainsi identifier le E, le A, ... Le code de Hill[2] que je vais vous présenter n'a pas ces inconvénients. On considère le système suivant :

$$(\mathscr{C}) : \quad \begin{cases} 3x+2y &= a \\ 4x+3y &= b \end{cases}$$

I Cryptage

Pour coder un message, on commence par grouper les lettres deux par deux puis on remplace chaque lettre par son rang dans l'alphabet.

Exemple: Si on doit coder : « BATEAU » on décompose en BA-TE-AU puis on remplace par : $(2;1) - (20;5) - (1;21)$.
Ensuite chaque couple de nombres $(x;y)$ est transformé par le système $\mathscr{C}$ ci-dessus pour donner un nouveau couple $(a\,;b)$. Enfin ces deux nombres a et b sont transformés en lettre en utilisant leur rang dans l'alphabet.

Exemple: Pour coder « BA » donc $(2;1)$ on obtient : $\begin{cases} 3\times 2+2\times 1 &= 9 \\ 4\times 2+3\times 1 &= 11 \end{cases}$. Or la neuvième lettre est I et la onzième est K. Donc BA se code en IK. Attention, il peut arriver que l'on obtienne a ou b qui ne soient pas compris entre 1 et 26 ! Dans ce cas on imagine que 27 correspond à A, 28 à B... et pour les négatifs : 0 à Z, -1 à Y,..., -25 à A.

Exemple: $55 = 2\times 26+3$ donc 55 correspond au 3 donc au C. En fait 3 est le reste de la division de 55 par 26. De même avec des nombres négatifs : $-73 = -78+5 = -3\times 26+5$. Donc -73 correspond au 5, donc à la lettre E. (Attention, le reste de la division de 73 par 26 est 21)

1. Coder le mot : « CADEAU »
2. Une lettre donnée est-elle toujours cryptée par la même lettre ?
3. Dans un message codé, deux lettres identiques représentent-elles la même lettre ?

II Décryptage

Comment décoder un message ? On remplace les lettres par leur rang dans l'alphabet, on les groupe deux par deux. On obtient une liste de couples $(a\,;b)$. On doit trouver les x et y qui leur correspondent. On doit donc résoudre le système $\mathscr{C}$ pour chaque couple $(a\,;b)$.

1. Vérifier en résolvant un système que IK se décode bien en BA.
2. Résoudre un système à chaque fois serait long, donc on peut déterminer la transformation inverse du codage. Pour cela, exprimer x et y en fonction de a et b, en résolvant (avec les lettres a et b) le système $\mathscr{C}$. On obtient un système $\mathscr{D}$ pour décoder, de la forme :

$$(\mathscr{D}) : \quad \begin{cases} \ldots a+\ldots b &= x \\ \ldots a+\ldots b &= y \end{cases}$$

3. Décrypter le message : « SAGALISFPMCZYW »

[1] cf. la première référence sous Google pour « code de César ».
[2] Il a été inventé par Lester Hill en 1929.