Un message codé, assez long, dans lequel chaque lettre a été codée par une autre toujours de la même façon, comme le codage affine, est assez facile à attaquer en s'appuyant par exemple sur la fréquence des lettres dans un texte suivant la langue.

Une amélioration, publiée en 1931 par le mathématicien américain Lester HILL, consiste à coder des blocs de lettres, le codage d'une lettre dépendant alors de sa place dans le bloc.

Comment fonctionne un tel codage sur des blocs de deux lettres ?

Le principe :

On choisit quatre entiers a, b, c et d constituant la ***clé*** du chiffrement.
Les lettres de l'alphabet sont codées de 0 à 25. A un bloc de deux lettres correspondent donc un couple $(x;y)$ d'entiers compris entre 0 et 25. On calcule les codes du message chiffré en associant au couple $(x;y)$, le couple $(x';y')$ tel que :

$$\begin{cases} x' \equiv ax + by\,(26) \\ y' \equiv cx + dy\,(26) \end{cases}$$

I Exemples de chiffrement

On souhaite chiffrer le mot ETUDIER.
On partage le mot en blocs de 2 lettres : ET - UD - IE - RA (le dernier bloc est complété au hasard)

I.1 Clé : $a = -5$, $b = 8$, $c = -2$ et $d = 3$

1. Chiffrement du premier bloc ET.
   Déterminer x et y. En déduire x' et y' puis vérifier que le bloc ET est chiffré par CX.
2. Terminer le chiffrement du mot ETUDIER à l'aide d'un tableur ou avec un algorithme.

	A	B	C	D	E	F	G	H	I
1	Clé	a=	-5	b=	8				
2		c=	-2	d=	3				
3									
4	Texte en clair	E	T	U	D	I	E	R	A
5	x , y	4	19						
6	x' , y'	2	23						
7	Texte chiffré	C							

3. Quelle remarque ce chiffrement occasionne-t-il ?

I.2 Clé : $a = 6$, $b = 7$, $c = -8$ et $d = 5$

Coder le mot ETUDIER avec cette ***clé*** ? Quel problème cela pose-t-il ?

II Chiffrement et déchiffrement : approche mathématique

Toujours suivant le même principe, posons par exemple :

$$(1)\begin{cases} x' \equiv 5x + 11y\,(26) \\ y' \equiv 8x + 3y\,(26) \end{cases}$$

1. Coder le mot REQUIN en détachant les trois blocs de deux lettres.
2. Décodage :
   Montrer que si x, y, x' et y' vérifient (1) alors :

$$\begin{cases} -3x' + 11y' \equiv 73x\,(26) \\ 8x' - 5y' \equiv 73y\,(26) \end{cases}$$

3. Résoudre dans $\mathbb{Z} \times \mathbb{Z}$, l'équation $73x + 26y = 1$, avec $0 \leqslant x \leqslant 25$.
4. Décoder alors le mot XEJQVVLDVW .

III Avec une approche matricielle

On reprend les données du paragraphe précédent : (1) $\left\{ \begin{array}{l} x' \equiv 5x + 11y\,(26) \\ y' \equiv 8x + 3y\,(26) \end{array} \right.$ $\Leftrightarrow$ (1) $\left\{ \begin{array}{l} x' = 5x + 11y \\ y' = 8x + 3y \end{array} \right.$ si l'on considère que les calculs sont faits modulo 26.

1. On écrit le système (1) précédent sous la forme $\left(\begin{array}{c} x' \\ y' \end{array} \right) = A \left(\begin{array}{c} x \\ y \end{array} \right)$ (★) où A est un tableau à 2 lignes et 2 colonnes composé de nombres que l'on note de la manière suivante :

$$A = \left(\begin{array}{cc} * & * \\ * & * \end{array} \right)$$

   (a) Quelle est la valeur du tableau A ?

   (b) Figure-t-il une opération entre A et $\left(\begin{array}{c} x \\ y \end{array} \right)$? Quel est le principe de calcul dans la relation (★) ? Quel nom pouvons-nous donner à cette opération ?

2. **Règles opératoires avec les matrices**

   (a) « MULTIPLIER » UNE MATRICE A PAR UN NOMBRE RÉEL λ.

   De manière intuitive, quelle signification donneriez-vous de la notation λA où λ est un réel non nul et A la matrice $\left(\begin{array}{cc} a & b \\ c & d \end{array} \right)$?

   (b) « MULTIPLIER » UNE MATRICE A PAR UNE MATRICE B.

   On note $A = \left(\begin{array}{cc} a_{11} & a_{12} \\ a_{21} & a_{22} \end{array} \right)$ et $B = \left(\begin{array}{cc} b_{11} & b_{12} \\ b_{21} & b_{22} \end{array} \right)$. On admet que le produit de deux matrices carrées d'ordre 2 est une matrice carrée d'ordre 2, c'est à dire en écriture matricielle :

$$A = \left(\begin{array}{cc} a_{11} & a_{12} \\ a_{21} & a_{22} \end{array} \right) \left(\begin{array}{cc} b_{11} & b_{12} \\ b_{21} & b_{22} \end{array} \right) = \left(\begin{array}{cc} a_{11}b_{11} + a_{12}b_{21} & * \\ * & * \end{array} \right)$$

   En examinant l'expression du premier coefficient, deviner le principe de calcul de AB. Que pensez-vous de la matrice obtenue en calculant BA ?

3. **Inverse d'une matrice carrée d'ordre 2.**

   (a) On note $X' = \left(\begin{array}{c} x' \\ y' \end{array} \right)$ et $X = \left(\begin{array}{c} x \\ y \end{array} \right)$. Réécrire la relation (★).
   Si l'on prolonge le principe de résolution d'équation de la forme $ax = b$ dans $\mathbb{R}$, comment écririez-vous X en fonction de A et de X' ?

   (b) Définition : ....

   Soit A une matrice carrée d'ordre 2, $A = \left(\begin{array}{cc} a & b \\ c & d \end{array} \right)$. Il est possible de calculer la matrice A^{-1} appelée matrice inverse si, et seulemnent si, $ad - bc \neq 0$. Et dans ce cas là,

$$\mathbf{A^{-1}} = \frac{\mathbf{1}}{\mathbf{ad - bc}} \left(\begin{array}{cc} \mathbf{d} & \mathbf{-b} \\ \mathbf{-c} & \mathbf{a} \end{array} \right)$$

   (c) Calculer A^{-1} pour la ***clé*** donnée en début de paragraphe. Quelle difficulté apparaît alors dans le contexte de l'exercice ?

   (d) Proposer une méthode pour décoder à nouveau le mot XEJQVVLDVW .

IV D'autres références

http://www.bibmath.net/crypto/index.php?action=affiche&quoi=poly/hill

V Un peu de culture !

Le nom du peintre auteur du tableau ci-contre a été codé avec la ***clé*** : $a = 3$, $b = 5$, $c = 4$ et $d = 7$. Il s'git de

BLPPKORKJL
(initiale du prénom et nom)

.
Quel est le nom de ce peintre ?