Cryptographie2
Historique
Le chiffrement de Hill (chiffrement par blocs)

On choisit une taille de blocs k. On sépare le texte en suites de k lettres. Chaque lettre est remplacée par son rang dans l'alphabet.
a$->$0,b$->$1,...,z$->$25.
La clef est constituée d'une application linéaire bijective de $(Z/26Z)^k$ vers $(Z/26Z)^k$.
Si l'application linéaire a pour matrice A, le cryptage d'un bloc M de k lettres est donné par:
$C = MA$ (produit matriciel, M et C sont des matrices lignes). Puisque l'application est bijective, il existe une application inverse de matrice A^{-1}.
Le décrytage se fait par:
$M = CA^{-1}$
Exemples

Pour $k = 1$,la transformation est $c = am \bmod 26$.
Avec la clef $a = 5$: $c = 5 \times m \bmod 26$ transforme a(0) en (5×0)soit A, b(1) en F(5), m en I($12 \times 5 = 60 = 8 \bmod 26$).
A quelle condition cette application est elle bijective ?
Pour $k = 2$, si on prend l'application de matrice
$A = \begin{pmatrix} 3 & 2 \\ 4 & 5 \end{pmatrix}$
Le bloc `bo`, soit $(1, 14)$ est chiffré en :
$(1, 14) \times \begin{pmatrix} 3 & 2 \\ 4 & 5 \end{pmatrix} = \begin{pmatrix} 3 \times 1 + 4 \times 14 \bmod 26,\ 2 \times 1 + 5 \times 14 \bmod 26 \end{pmatrix} = \begin{pmatrix} 7, 20 \end{pmatrix}$, soit HU.

Déchiffrement

Le déterminant de A doit être inversible dans $Z/26Z$.

Par exemple si $k = 2$, A est de la forme $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

Le déterminant est $ad - bc$. S'il est inversible, la matrice inverse est $(ad - bc)^{-1} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$

L'application de matrice $A = \begin{pmatrix} 1 & 3 \\ 5 & 12 \end{pmatrix}$ est elle utilisable pour un cryptage de Hill ?

Echangez des messages cryptés et décrytez les.

Cryptanalyse

Pour un cryptosystème moderne, on considère que l'algorithme est connu. La clef ne doit pas être découverte même si, *par ordre d'exigence croissant* :

1. on dispose d'un texte clair et du texte crypté correspondant
2. on peut choisir un texte clair et obtenir le texte crypté correspondant
3. on peut choisir les textes clairs et obtenir les textes chiffrés au fur et à mesure.
4. on peut choisir des textes chiffrés et obtenir les textes en clair.

A quelles attaques résiste le chiffrement de Hill ?

Déchiffrez le texte `Hill.txt`, sachant qu'il s'agit d'une lettre commençant par `monsieur`.

Annexe : Identité de Bezout

On verra dans un prochain cours comment calculer les inverses modulo m.

Si d est le pgcd de a et b, on peut trouver u et v tels que $d = au + bv$. Si $d = 1$ et $b = m$, u est l'inverse de a modulo m.

Pour $m = 26$, on peut se contenter de précalculer une table.

Méthode de détermination des entiers u et v de l'égalité de Bezout :
le pgcd étant le dernier reste non nul dans la méthode d'Euclide, la méthode consiste à écrire les restes successifs en fonctions de a et de b.
On ne fait qu'appliquer $a = bq + r \Leftrightarrow r = a - bq$ et le reporter tout au long des calculs !
On définit une suite $a_0 = a$, $a_1 = b$, $a_{i+2} = a_i \mathrm{mod} a_{i+1}$ (a_k est le dernier reste non nul (pgcd)) On définit deux suites u_i et v_i telle que pour tout i on

ait $au_i + bv_i = a_i$ L'idée est de maintenir tout au long du calcul des valeurs vérifiant la relation.
$i = 0$: $au_0 + bv_0 = a_0$ $a_1 + b_0 = a = a_0$
$i = 1$: $au_1 + bv_1 = a_1$ $a_0 + b_1 = b = a_1$
. . .
i : $au_i + bv_i = a_i$
$i + 1$: $au_{i+1} + bv_{i+1} = a_{i+1}$
$i + 2$: $a_{i+2} = a_i \mod a_{i+1}$
soit: $a_i = a_{i+1}q_i + a_{i+2}$
$a_{i+2} = a_i - a_{i+1}q$
$= au_i + bv_i - q(au_{i+1} + bv_{i+1})$
$= a(u_i - qu_{i+1}) + b(vi - qv_{i+1})$
$= au_{i+2} + v_{i+2}$

Les suites u_i et v_i sont définies par
$u_0 = 1$; $u_1 = 0$; u_{i+2}=$u_i - q_i u_{i+1}$;
$v_0 = 0$; $v_1 = 1$;$v_{i+2} = v_i - q_i v_{i+1}$;
o q_i est le i$^{\text{ème}}$ quotient dans les divisions euclidiennes du calcul du pgcd.