3/10/2022

Le Challenge chiffre de Hill est :

Vous connaissez seulement 5 lettres « GPRCY» dans le message chiffré.

Vous savez que dans ce message « ARCSI» est chiffré en « GPRCY» avec la méthode du chiffre de Hill. La matrice est une matrice de 2x2.

Saurez-vous déchiffrer ceci :

```
Htqj s,p' GPRC Ypvi vqdj gfsv vigk tkxq yzut csrg tkks oskz zntk euyc ymyy ahgr
ksel sNPH zyvb cpae fywo e'uu iiko nibb sgpm aofv uxsi skzq jalo v.
```

Solution :

Le chiffre de hill a été publié en 1929 par Lester S. Hill (1891-1961). Il est un chiffre polygraphique. Son idée n'est plus de coder lettres par lettres, mais de coder simultanément des groupes de m lettres! Bien sûr, plus m est grand, plus les analyses statistiques deviennent difficiles!

Les lettres sont d'abord remplacées par leur rang dans l'alphabet.
D'après la position des lettres dans l'alphabet où la première lettre commence par 1 :

Clair	Chiffré
A=1	G=7
R=18	P=16
C=3	R=18
S=19	C=3

AR	CS
[1,18]	[3,19]
[7 ,16]	[18,3]
GP	RC

Nous utilisons la version bigraphique du chiffre de Hill, c'est-à-dire qu'on groupe les lettres deux par deux.

Pour le chiffrement, les deux premières lettres du message clair (X_1et X_2)seront chiffrées en(Y_1et Y_2) selon la formule et les deux équations suivantes:

$$\begin{bmatrix} Y_n \\ Y_{n+1} \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} X_n \\ X_{n+1} \end{bmatrix} mod 26$$

Y_1=a X_1+b X_2(mod26)
Y_2=c X_1+d X_2(mod26)

Il faut donc connaitre les valeurs de a,b,c,d pour pouvoir chiffrer le message.

Nous allons montrer comment on peut trouver $\begin{bmatrix} \mathbf{a} & \mathbf{b} \\ \mathbf{c} & \mathbf{d} \end{bmatrix}$

Nous devons résoudre ceci :

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 1 \\ 18 \end{bmatrix} = \begin{bmatrix} 7 \\ 16 \end{bmatrix}$$

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 3 \\ 19 \end{bmatrix} = \begin{bmatrix} 18 \\ 3 \end{bmatrix}$$

L'inverse de ce que nous devons résoudre est :

$$\begin{bmatrix} e & f \\ g & h \end{bmatrix} \begin{bmatrix} 7 \\ 16 \end{bmatrix} = \begin{bmatrix} 1 \\ 18 \end{bmatrix}$$

$$\begin{bmatrix} e & f \\ g & h \end{bmatrix} \begin{bmatrix} 18 \\ 3 \end{bmatrix} = \begin{bmatrix} 3 \\ 19 \end{bmatrix}$$

Nous avons ces 4 équations à résoudre :

a+18b=7 (<u>équation 1</u>)
c+18d=16 (<u>équation 2</u>)

3a+19b=18 (<u>équation 3</u>)
3c+19d=3 (<u>équation 4</u>)

<u>Calcul de **b**</u>

On fait 3*(<u>équation 1</u>)-(<u>équation 3</u>)

3a+54b-3a-19b=21-18
35b=3
La formule du modulo (ou Congruence) est N≡XmodP . On cherche X.
P=35 et P= 26.
35 mod 26 = 9
35 = 26 × 1 + 9
modulo 26 de 35 est 9 .
Donc **b=9**

a+18b=7 (<u>équation 1</u>)
3a+19b=18 (<u>équation 3</u>)

<u>Calcul de **a**</u>

On fait (<u>équation 1</u>)- (<u>équation 3</u>) en remplaçant **b** par 9

a+162-3a-171=7-18
-2a=-11+9=-2
-2a=-2
a=1

On utilise ces équations pour calculer c et d :

c+18d=16 (<u>équation 2</u>)
3c+19d=3 (<u>équation 4</u>)

<u>Calcul de **d**</u>

On fait 3*(<u>équation 2</u>)- (<u>équation 4</u>)

3c+54d-3c-19d=48-3
35d=45

35 mod 26 = 9
35 = 26 × 1 + 9

9d=45
$d=\frac{45}{9}$
d=5

<u>Calcul de **c**</u>

On fait (<u>équation 2</u>)-(<u>équation 4</u>) en remplaçant **d** par 5

c-3c+90-95=16-3
-2c-5=13
2c=8
c=4

La clef est donc $\begin{bmatrix} \mathbf{1} & \mathbf{9} \\ \mathbf{4} & \mathbf{5} \end{bmatrix}$

Pour vérifier si la clef $\begin{bmatrix}\mathbf{1} & \mathbf{9}\\ \mathbf{4} & \mathbf{5}\end{bmatrix}$est bonne on vérifie que les 3 premières lettres du message « ARCSI» sont bien chiffrées en « GPR». Cette démonstration n'est valable que pour le chiffrement.
Le déchiffrement sera fait dans la page suivante.

Vérification que la lettre A(1) est chiffrée en G(7)

$$\begin{bmatrix}1 & 9\\ 4 & 5\end{bmatrix}\begin{bmatrix}1\\ 18\end{bmatrix}=\begin{bmatrix}7\\ 16\end{bmatrix}$$

Pour A=G
(1+9*18)mod26=7
(163)mod26=7
163=26*6+**7**

Vérification que la lettre R(18) est chiffrée en P(16)

$$\begin{bmatrix}1 & 9\\ 4 & 5\end{bmatrix}\begin{bmatrix}1\\ 18\end{bmatrix}=\begin{bmatrix}7\\ 16\end{bmatrix}$$

Pour R=P
(4*1+5*18)mod26=16
(94)mod26=16
94 = 26 × 3 + **16**

Vérification que la lettre C(3) est chiffrée en R(18)

$$\begin{bmatrix}1 & 9\\ 4 & 5\end{bmatrix}\begin{bmatrix}3\\ 19\end{bmatrix}=\begin{bmatrix}18\\ 3\end{bmatrix}$$

Pour C=R
(3*1+9*19)mod26=18
174 mod 26 = 18
174 = 26 × 6 + **18**

Déchiffrement du message :

Pour déchiffrer, le principe est le même que pour le chiffrement: on prend les lettres deux par deux, puis on les multiplie par une matrice.

Cette matrice doit être l'inverse de matrice de chiffrement (modulo 26) :

$$\begin{bmatrix} Y_n \\ Y_{n+1} \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} \begin{bmatrix} X_n \\ X_{n+1} \end{bmatrix} mod 26$$

L'inverse de la matrice est: $\begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = \frac{1}{ad-bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$

Pour le déchiffrement, les deux premières lettres du message clair (X_1et X_2)seront déchiffrées en(Y_1et Y_2) selon la formule et les deux équations suivantes:

$$\begin{bmatrix} Y_n \\ Y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & 9 \\ 4 & 5 \end{bmatrix}^{-1} \begin{bmatrix} X_n \\ X_{n+1} \end{bmatrix} mod 26$$

$$\begin{bmatrix} Y_n \\ Y_{n+1} \end{bmatrix} = \frac{1}{-31} \begin{bmatrix} 5 & -9 \\ -4 & 1 \end{bmatrix} \begin{bmatrix} X_n \\ X_{n+1} \end{bmatrix} mod 26$$

$$\begin{bmatrix} Y_n \\ Y_{n+1} \end{bmatrix} = -31^{-1} \begin{bmatrix} 5 & -9 \\ -4 & 1 \end{bmatrix} \begin{bmatrix} X_n \\ X_{n+1} \end{bmatrix} mod 26$$

…

On utilise ce lien pour inverser la matrice :
https://www.apprendre-en-ligne.net/crypto/hill/compl.html#inversemod

$$\begin{bmatrix} Y_n \\ Y_{n+1} \end{bmatrix} = \begin{bmatrix} 25 & 7 \\ 6 & 5 \end{bmatrix} \begin{bmatrix} X_n \\ X_{n+1} \end{bmatrix} mod 26$$

Y_1=a X_1+b X_2(mod26)
Y_2=c X_1+d X_2(mod26)

<u>On déchiffre la 1er lettre du message chiffré : H(8) avec T(20)</u>
Y_1=25* 8+7 *20(mod26)
Y_1=200+140(mod26)
Y_1=340(mod26)
340 = 26 × 13 + 2
Y_1=2

<u>Donc la lettre H est déchiffré en B</u>

Pour déchiffrer avec dcode.fr : https://www.dcode.fr/chiffre-hill
On chiffre avec l'inverse de la matrice trouvée précédemment pour résoudre tout le challenge.

Le message en clair est :

```
Bravo, l' ARCSI vous invite pour ses quatorziemes rencontres le vingt octobre a la
BNF sur le theme de l'epopee de la carte a puce et son avenir.
```

Commentaire :

Pour refaire ce challenge, vous devez vérifier que :

- La matrice de chiffrement ait une matrice inverse dans Z_{26}.
- (ad-bc) est impair et n'est pas multiple de 13
- Que a,b,c,d sont positif et des nombres entier.