Le TD N°2 consisterait en l’application du chiffrement par fonctions affines et chiffrement matriciel de HILL . Comme support, vous pouvez résoudre les exos suivants ou autres exercices qui vous sembleraient appropriés à cette séance.

Représentation numérique de l’alphabet :

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25

**Exercice 4**

1. Soit à chiffrer le texte en clair P= ACTION de l’alphabet Z26 selon un chiffrement à l’aide d’une fonction affine E(x)=5x +8 mod26 ou bien y=5x+8 mod26
2. Retrouver le texte en clair P à partir du chipher texte C trouvé en 1.

**Solution : a=5, b=8, PGCD(5,26) =1 donc E(x) admet une fonction inverse, elle est valide.**

**Plaintext P A C T I O N**

**Valeur numérique 0 2 19 8 14 13**

**Valeur E(x) 8 18 25 22 0 21**

**Chipher text C I S Z W A V**

**Y=5X+8 , Y-8 = 5X mod26 alors 5-1.5.X= 5-1(Y-8) d’où X=21(Y-8)mod26 ou bien X=21Y- 168 mod26 ou encore X= 21Y-12 mod26 ou encore *X=21Y+14* mod26**

**Chipher text Y I S Z W A V**

**Valeur numérique 8 18 25 22 0 21**

**X=21y-12 mod26 0 2 19 8 -12mod26=14 13**

**Plaintext A C T I 0 N**

**Exercice 5**

1. Chiffrez le texte P=ACTION de l’alphabet des 26 lettres latines Z26 à l’aide d’un chiffrement de Hill de clé K = (3 3)

(2 3)

1. Retrouvez le texte en clair P à partir du texte chiffré C obtenu en 1.

**Solution : Comme la clé est de dimension 2\*2, on forme des groupes de lettres de 2 (Digramme) à coder. AC TI ON soit x1=0 (A) x2=2 (C)**

**(K1, K2)**

**Codage : X1, X2 (K3, K4) C1=(X1K1 +X2K2)mod26 soit 0.3 + 2.2=4 correspondant à E**

**C2= 0.3 +2.3= 6 correspondant à G**

**Le digramme AC est code *EG*. De la même façon, TI devient *VD* et ON devient *QD***

**Le cipher text C est EGVDQC**

**Pour décoder EGVDQC, il faut que K-1 existe c'est-à-dire déterminant de K non nul. Donc dét(K)=9-6=3 premier avec 26. K-1 =1/det(K) (K4 -K2) = 1/3 (3 -3)**

**(-K3 k1) (-2 3)**

**Inverse 3 est 3-1 càd trouver m tel que m\*3 ≡ 1 mod26 d’où m=9.**

**K-1 = (27 -27) Finalement K-1 = (1 25)**

**(-18 27) (8 1)**

**Déchiffrement de EG : (4, 6) K-1 = (4+48, 100+6)mod26 → (0, 2) → AC**

**‘’ ‘’ VD : (21, 3)K-1 = (21+24, 21\*25+3) mod26 → (19, 8) → TI**

**‘’ ‘’ QD : (16, 3)K-1 = 16+24, 16\*25+3) =(14, 13) → ON**

**Exercice 6**

Onsuppose qu’un chiffrement affine E(x) = (ax + b) MOD26 transforme H en X and Q en Y.

1. Déterminer la fonction de chiffrement (a et b).
2. Chiffrer le message suivant « RDVJEUDI»
3. Comment chiffrer le plaint text RDV JEUDI 28 A 8H00
4. Combien de fonctions de transformations affines possibles peut-on avoir dans ce type de codage ?

**Réponse :**

1. E(x) = ax + b, H (7) → X (23), ce qui donne 7\*a+ b =23

Q (16) → Y (24) ‘’ ‘’ 16a+b =24 → 9a= 1 d’où **a=3**. 21+b=23 d’ou **b=2 ,**

donc **E(x)= 3x+2**

1. RDVJEUDI → BLNDOKLA
2. Chiffrement avec la même fonction, en considérant l’alphabet des 26 lettres, plus les 10 chiffres décimaux, plus le blanc. Donc avec un groupe multiplicatif **Z37.**  A =0 B=1 ……. Blanc =36
3. Le paramètre a d’une fonction affine valide peut prendre 36 valeurs distinctes 1≤a≤36 et le paramètre b peut en prendre 36. Donc au total, l’espace des clés est :1296