**TD2 : Cryptanalyse du chiffrement affine**

Exercice1 :

1. (a ;b) = (7 ;3) ;

On a 7 ^ 26 = 1, donc (7 ;3) est une clef valide. De plus, on a 7\*15 = 105 = 1 mod (26).

Ainsi a-1 = 15 dans Z26.

1. On a :

E(a;b)(x) := ax + b mod 26 et D(a;b)(y) := a-1(y - b) mod 26

E(a;b)(x) = 7x + 3

D(a;b)(E(a;b)(x)) = D(a;b)(7x + 3)

= 15(7x + 3 – 3) mod (26)

= 15(7x + 0) mod (26)

= x .

1. Chiffrement du mot : « hot »

Dans Z26: On a h -> 7, o -> 14 et t -> 19.

on applique le chiffrement.

7 \* 7 + 3 mod 26 = 52 mod 26 = 0 ;

7 \* 14 + 3 mod 26 = 101 mod 26 = 23 ;

7 \* 19 + 3 mod 26 = 136 mod 26 = 6 :

On obtient donc le texte chiffre 0 23 6 qui correspond à « axg ».

1. Les éléments de Z26 qui sont premiers avec 26 sont 1; 3; 5; 7; 9; 11; 15; 17; 19; 21; 23 et 25.

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| a | 1 | 3 | 5 | 7 | 9 | 11 | 15 | 17 | 19 | 21 | 23 | 25 |
| a-1 | 1 | 9 | 21 | 15 | 3 | 19 | 7 | 23 | 11 | 5 | 17 | 25 |

1. Le nombre de clef possible est le nombre de « a » dans Z26 (12) combiné avec 26 valeurs de b possibles => 12 \* 26 = 312. Le nombre de clefs reste insuffisant pour assurer un cryptage solide vue la performance des calculateurs actuels.

Exercice2 :

lettre fréquence lettre fréquence

A 2 N 1

B 1 O 1

C 0 P 2

D 6 Q 0

E 5 R 8

F 4 S 3

G 0 T 0

H 5 U 2

I 0 V 4

J 0 W 0

K 5 X 2

L 2 Y 1

M 2 Z 0

1. Le caractère le plus fréquent est R (8 occurrences). Comme en anglais la lettre la plus courante est E, il est fort probable que R se déchiffre en E.
2. T -> D et E -> R :

E(a;b)(4) = 17 (R = 17, E = 4) ; E(a;b)(19) = 3 (D = 3, T = 19).

Ainsi on obtient :

- 4a + b = 17

- 19a + b = 3

Il faut résoudre ce système dans Z26.

-« 19a+b = 3 »

(x = a-1(y - b) mod 26 est l'unique solution de l'équation ax + b = y mod 26 dans Z26)

soit a = 11(3 - b) (car 19-1 = 11).

On a donc :

a = 33 - 11b = 7 - 11b mod (26).

On injecte cela dans la première équation :

4(7 - 11b) + b = 17 mod (26)

28 - 43b = 17 mod (26)

2 - 17b = 17 mod (26) (car 28 = 2 mod 26 et 43 = 17 mod 26)

ce qui est équivalent à -17b = 15 mod (26) ,

et on a donc -17b mod(26) = ((-17 mod 26)b) mod (26) = 9b mod (26) = 15 mod (26). On résout cela pour trouver b = 19 (9-1 = 3, donc b = 3\*15 mod(26) = 45 mod(26) = 19

mod 26). On trouve alors a = 7 - 11 \* 19 mod (26) = 6. Cette clef n'est pas valide

car 6 et 26 ne sont pas premiers entre eux.

1. Il s'agit de résoudre dans Z26 le système de deux équations à deux inconnues a et b :

4a + b = 17

19a + b = 10

puisque T -> K et E -> R ,donc 19a + b = 10,

on déduit que a = 19-1(10 - b) = 11(10 - b)

= 110 - 11b = 6 - 11b (puisque 110 = 6 mod 26)

= 6 + 15b

On injecte cela dans l'équation 4a + b = 17 :

4(6 + 15b) + b = 17

24 + 61b = 17

24 + 9b = 17 (puisque 61 = 9 mod 26)

9b = 17 - 24

9b = 17 + 26 - 24

9b = 19

b = 9-1 \* 19

b = 3 \* 19

b = 57 mod (26)

b = 5

Ainsi a = 6 + 15 \* 5 = 6 + 75 = 81 = 3 mod 26. 3 est premier avec 26.

Donc (3; 5) est une clef valide.

1. a = 3 donc 3-1 = 9.

Le déchiffrement se fait avec l’équation D(a;b)(y) = 9y – 19 = 9y + 7 :

num lettre D(a;b)(num) lettre

0 A 7 H

1 B 16 Q

2 C 25 Z

3 D 8 I

4 E 17 R

5 F 0 A

6 G 9 J

7 H 18 S

8 I 1 B

9 J 10 K

10 K 19 T

11 L 2 C

12 M 11 L

13 N 20 U

14 O 3 D

15 P 12 M

16 Q 21 V

17 R 4 E

18 S 13 N

19 T 22 W

20 U 5 F

21 V 14 O

22 W 23 X

23 X 6 G

24 Y 15 P

25 Z 24 Y

Message initial :

FMXVEDKAPHFERBNDKRXRSREFMORUDSDKDVSHVUFEDKAPRKDLYEVLRHHRH

Message déchiffré :

algorihmsarequitegeneraldefinitionsofarithmeticprocesses