CODAGE AFFINE

Pour coder et décoder avec une fonction affine on fait le calcul :

ax+b

Puis encore une fois la même fonction ce qui donne :

a(ax+b)+b

on a donc : $x \rightarrow a^2x+ab+b=x$ (mod**P**)

(→ on travail avec un modulo p tel que p est un nombre premier > à 2)

Si on veux que **$a^2x+ab+b=x$** (modP)

on a deux solutions :

$a^2=1$ (mod**P**)
a=1 ou **a=-1**

ab+b=0(modp)

avec a=1
2b=0
b=0 (mod**P**)

Quand on a=1, p un nombre premier au dessus de 2 et b un multiple de 27 : la fonction pour coder et décoder consiste à remplacer le nombre par lui même

Avec a=-1
-1b+b=0

lorsque que a= -1, b peut prendre n'importe quelle valeur

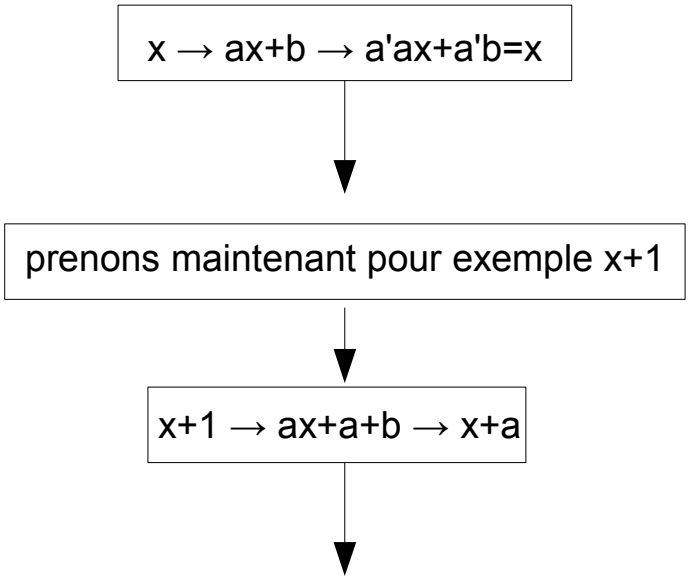
$x \rightarrow -x+b \rightarrow -(-x+b)+b=x$

prenons comme exemple b=3 en travaillant avec mod 5

0 → 3;
1 → 2;
2 → 1;
3 → 0;
4 → 4

A l'œil on voit qu'on effectue un simple décalage de -1. Ainsi en connaissant un chiffre on peux tous les trouver FACILEMENT

En codant avec une fonction affine ax+b et en décodant avec une autre fonction affine a'x+b' on a:



ceci revient a décaler de a ce qui est facilement dé-codable.

Exemple concret :
a=5 b=3 mod27

1 → 8
2 → 13
3 → 18
4 → 23

A l'œil, encore une fois, on vois qu'il y a un décalage de 5 → si on sait qu'on a ax+b
→ on sais que a=5 et que b=8-(5*1);
b=13-(5*2);
b=18-(5*3);
b=23-(5*4);

B=3

On vient de démontrer que le codage affine revient a décaler de a, c'est pourquoi il n'est pas intéressant !!