Solutions

EX:1 a) Chiffrement de BEN.

$B=3 \xrightarrow{\text{chif}} 3^e\ [22] \to 3^3 \equiv 5\ [22] \to 5=I$

$E=7 \xrightarrow{\text{chif}} 7^3 \equiv 13\ [22] \to 13=L$

$N=9 \xrightarrow{\text{chif}} 9^3 \equiv 3\ [22] \to 3=B$

donc BEN est chiffré par ILB.

b) Calcul de la clé privée d.

$e.d \equiv 1\ \varphi(22) \Rightarrow 3.d \equiv 1\ [10]$

$\Rightarrow d = 7$

Déchiffrement de IALB.

par a) on a le déchiffrement de I.LB.

$I \xrightarrow{\text{dechif}} B$, $L \xrightarrow{\text{dechif}} E$, $B \xrightarrow{\text{dechif}} N$

reste à déchiffrer $A=15$.

$A=15 \xrightarrow{\text{dechif}} 15^d \equiv 15^7 \equiv 5\ [22] \to 5=I$

donc IALB est déchiffré par BIEN.

EX:2 a) $g=3$, $g^2 \equiv 9 \equiv 2\ (7)$, $g^3 = 3^3 = 6$, $g^4 = 3^4 = 4$,

$g^5 = 3^5 = 5$, $g^6 = 3^6 = 1$ donc

$\left(\frac{\mathbb{Z}}{7\mathbb{Z}}\right)^* = \langle 3 \rangle$.

b) $a=4 \Rightarrow A = g^a = 3^4 = 4 \ (7)$.

* Déchiffrement de $m=2$ avec $k_1=5$.

$\downarrow$

$(g^{k_1} = 3^5 = 5 \ , \ m.A^{k_1} = 2.4^5 = 4)$

Déchiffrement de $(y_1=5, y_2=4)$.

$\downarrow$

$y_2 . y_1^{-a} = 4.5^{-4} = 4^{-1} = 2 = m.$

** Chiffrement de $m=2$ avec $k_2=3$.

$\downarrow$

$(3^3 = 6 \ , \ 2.4^3 = 2)$

Déchiffrement de $(y_1=6, y_2=2)$

$\downarrow$

$y_2 . y_1^{-a} = 2(-1)^4 = 2 = m$

EX: 3 La vérification :

$$y_2 . y_1^{-a} = (mA^k)(g^k)^{-a} = m\, g^{ak} . g^{-ak} = m . g^0 = m.$$

EX: 4 A calcule g^{x_A} et l'envoie à B

B calcule g^{x_B} et l'envoie à A.

A calcule $(g^{x_B})^{x_A} = (3^3)^2 = 3^6 = 1$

B calcule $(g^{x_A})^{x_B} = (3^2)^3 = 3^6 = 1$

A et B obtiennent la clé commune 1.

Exo 5 Tout triplet de 1, 2, 3, 4 obtient le même penalty S, prenons par exemple 1, 2, 3.

Par la méthode de Lagrange posons

$$\ell_1(x) = \frac{(x-2)(x-3)}{(1-2)(1-3)}$$

$$\ell_2(x) = \frac{(x-1)(x-3)}{(2-1)(2-3)}$$

$$\ell_3(x) = \frac{(x-1)(x-2)}{(3-1)(3-2)}$$

on a $S = 28\,\ell_1(0) + 34\,\ell_2(0) + 42\,\ell_3(0)$

$= 24$.

On peut calculer S par la résolution d'un système d'équations linéaires, mais la méthode de Lagrange est la plus pratique.