

UN CHIFFREMENT ASYMÉTRIQUE : LE PROTOCOLE RSA (1976)

ÉLÉMENTS DE CORRECTION

EXERCICE PRÉLIMINAIRE

On note $n=pq$ où p et q sont deux nombres premiers distincts.
On pose $m=(p-1)(q-1)$ et on note c un nombre premier avec m .

On note x un entier naturel.

1. c et m sont premiers entre eux, donc d'après le théorème de Bézout : il existe deux entiers relatifs d' et k tels que $cd'+mk=1$.

• Si $d'>0$, il suffit de poser $d=d'$ et on a $cd \equiv 1 [m]$.

• Si $d'<0$, alors on trouve le premier entier λ tel que $d'-m\lambda>0$ (ie $\lambda<\frac{d'}{m}$) et on pose $d=d'-m\lambda$:

$$cd+m(c\lambda+k)=c(d'-m\lambda)+m(c\lambda+k)=cd'+mk=1.$$

Donc il existe un entier naturel d tel que $cd \equiv 1 [m]$.

2. a) Supposons x divisible par p .

$$x=pk \text{ donc } x^{cd}=(pk)^{cd}=p^{cd}k^{cd}\equiv 0 [p]$$

b) Supposons x non divisible par p .

D'après le théorème de Fermat : $x^{p-1}\equiv 1 [p]$

donc $x^{(p-1)(q-1)}\equiv 1 [p]$ ie $x^m\equiv 1 [p]$ donc $(x^m)^k\equiv 1 [p]$ donc $x^{mk}\equiv 1 [p]$

donc $x^{mk+1}\equiv x [p]$ ie $x^{cd}\equiv x [p]$.

3. $q \mid x^{cd}-x$ et $p \mid x^{cd}-x$. Or q et p sont premiers donc ils sont premiers entre eux, donc d'après le corollaire du théorème de Gauss : $pq \mid x^{cd}-x$ ie $n \mid x^{cd}-x$ ie $x^{cd}\equiv x [n]$.

LE PROTOCOLE RSA

UN EXEMPLE DE CODAGE

On choisit $p=42139$ et $q=47837$, que l'on admet premiers.

1. a) $n=pq=2015803343$; $m=(p-1)(q-1)=42138\times 47836=2015713368$.

On peut prendre $c=12111985$ car c est premier avec m d'après l'algorithme d'Euclide :

2015713368=12111985×166+5123858	3658=553×6+340
12111985=5123858×2+1864269	553=340×1+213
5123858=1864269×2+1395320	340=213×1+127
1864269=1395320×1+468949	213=127×1+86
1395320=468949×2+457422	127=86×1+41
468949=457422×1+11527	86=41×2+4
457422=11527×39+7869	41=4×10+1
11527=7869×1+3658	4=1×4+0
7869=3658×2+553	

Les clés **publiques** sont donc $n=2015803343$ et $c=12111985$.

b) Pour trouver d , on utilise les coefficients de Bézout (à faire) :

$$1=2015713368\times(-2956808)+12111985\times 492080977 \text{ donc } d=492080977 \text{ convient.}$$

2. Correction disponible sur demande (mail).

SÉCURITÉ : ATTAQUE PAR FORCE BRUTE POSSIBLE ?

1. Une clé de 256 bits comprend env. 77 chiffres décimaux car :

$$2^{256} = 2^{10 \times 25 + 6} = (2^{10})^{25} \times 2^6 = 1024^{25} \times 64 \approx 10^{75} \times 64 \approx 10^{77}$$

autre méthode : $2^{256} = 10^k \Leftrightarrow k = 256 \log(2)$ soit $k \approx 77,06$.

2. a) $0,1 \% = 10^{-3}$ et $10^{-3} \times 10^{39} = 10^{36}$ donc nous devrions procéder à 10^{36} divisions.

b) $10^{36} \div 10^{20} = 10^{16}$ donc 10^{16} secondes, soit ≈ 300 millions d'années, soit un million de fois l'âge estimé de l'univers... !