

# RSA

Diapo 14  
(cours 2)

- 1)  $d$  est l'inverse de  $e$  modulo  $\phi(n)$ , on utilise l'algo d'Euclide étendu pour déterminer  $5^{-1} \bmod 64$ :

$k$	$r_k$	$u_k$	$v_k$	$q_k$	div. eucl.
0	64		0		
1	5		1	12	$64 = 5 \times 12 + 4$
2	4		-12	1	$5 = 4 \times 1 + 1$
3	1		13		

On vérifie:

$$13 \times 5 \equiv 65 \equiv 1 \bmod 64.$$

Donc  $d = 13$

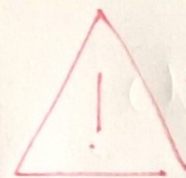
2)  $c \equiv m^e \equiv 10^5 \equiv 10^{2^2+1} \bmod 85$

or,  $10^2 \equiv 100 \equiv 15 \bmod 85$

$$10^{2^2} \equiv 15^2 \equiv 225 \equiv 55 \bmod 85$$

Donc  $c \equiv 10^{2^2} \times 10 \equiv 55 \times 10 \equiv 40 \bmod 85$

$c = 40$



modulo  $\phi(n)$

modulo  $n$

par exponentiation rapide.



$$3) m \equiv c^d \equiv 40^{13} \equiv 40^{2^3 + 2^2 + 1} \pmod{85}$$

↑  
par exponentiation  
rapide

$$\text{or } 40^2 \equiv 1600 \equiv 70 \pmod{85}$$

$$40^{2^2} \equiv 70^2 \equiv (-15)^2 \equiv 55 \pmod{85}$$

$$40^{2^3} \equiv 55^2 \equiv (-30)^2 \equiv 900 \equiv 50 \pmod{85}$$

$$\text{Dnc } m \equiv 40^{2^3} \times 40^{2^2} \times 40 \equiv 50 \times 55 \times 40 \equiv 10 \pmod{85}$$

$$\boxed{m = 10}$$

On retrouve bien le message envoyé par Alice !