28.01.20

Théorème d'Euler

Si $pgcd(a, n) = 1$, alors $a^{\varphi(n)} \equiv 1 \pmod{n}$

Exemple

$a = 28$ et $n = 15$, $pgcd(28, 15) = 1$

$\varphi(15) = \varphi(3 \cdot 5) = \varphi(3) \cdot \varphi(5) = 2 \cdot 4 = 8$

$\{1, 2, 4, 7, 8, 11, 13, 14\} = P$

$28^2 \equiv 784 \equiv 4 \pmod{15}$

$28^4 \equiv 4^2 \equiv 16 \equiv 1 \pmod{15}$

$28^8 \equiv 1^2 \equiv 1 \pmod{15}$

$28 \cdot 1 = 28 \equiv 13 \pmod{15}$

$28 \cdot 2 = 56 \equiv 11 \pmod{15}$

$28 \cdot 4 = 112 \equiv 7$

$28 \cdot 7 = 196 \equiv 1$

$28 \cdot 8 = 224 \equiv 14$

$28 \cdot 11 = 308 \equiv 8$

$28 \cdot 13 = 364 \equiv 4$

$28 \cdot 14 = 392 \equiv 2$

$= P$

$(28 \cdot 1) \cdot (28 \cdot 2) \cdot (28 \cdot 4) \cdot (28 \cdot 7) \cdot (28 \cdot 8) \cdot (28 \cdot 11) \cdot (28 \cdot 13) \cdot (28 \cdot 14) \equiv 13 \cdot 11 \cdot 7 \cdot 1 \cdot 14 \cdot 8 \cdot 4 \cdot 2 \pmod{15}$

$28^8 \cdot (1 \cdot 2 \cdot 4 \cdot 7 \cdot 8 \cdot 11 \cdot 13 \cdot 14) \equiv (1 \cdot 2 \cdot 4 \cdot 7 \cdot 8 \cdot 11 \cdot 13 \cdot 14) \pmod{15}$

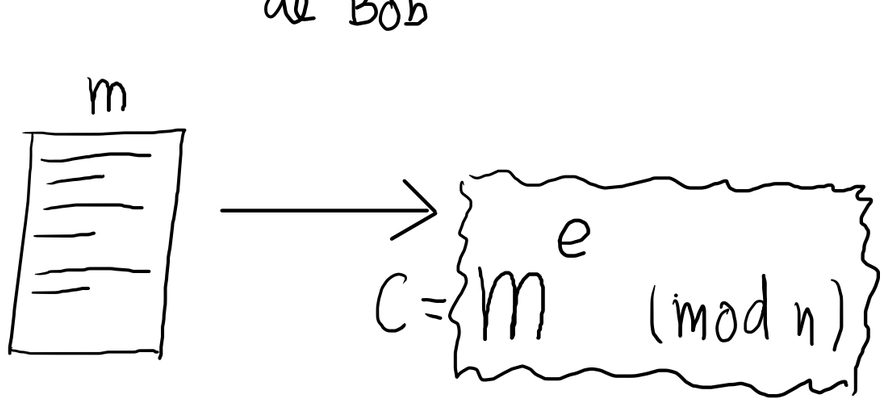
$28^8 \equiv 1 \pmod{15}$

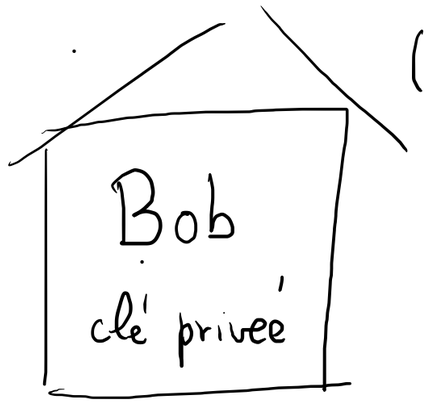
$28^{\varphi(15)} \equiv 1 \pmod{15}$

Cryptographie à clé publique

Chaque utilisateur possède deux clefs, l'une qu'il garde secrète, la clef privée, et l'autre qu'il publie, sur internet par exemple

clé pubique de Bob (e, n)





$$C^d \equiv \left(m^e\right)^d \equiv m^{ed}$$

$$\equiv m \pmod n$$

Système RSA

Théorème (Petit Théorème de Fermat)

Soit p premier et $a \in \mathbb{N}$ avec $\text{pgcd}(a, p) = 1$. On a

$$a^{p-1} \equiv 1 \pmod{p},$$

Découle du théorème d'Euler

Exemple de chiffrement avec RSA

1) Alice choisit deux nombres premiers p et q qu'elle garde secret.
Elle calcule $n = p \cdot q$

$p = 5$, $q = 17$, $n = 85$ $\quad [\varphi(85) = 4 \cdot 16 = 64]$

2) Alice détermine la clé secrète et la clé publique

clé publique $e = 5$ tel que $\text{pgcd}(e, \varphi(n)) = 1$

clé privée d, tel que $e \cdot d \equiv 1 \pmod{\varphi(n)}$

d se calcule avec l'algorithme de Bezout : $ed + K \cdot \varphi(n) = 1$

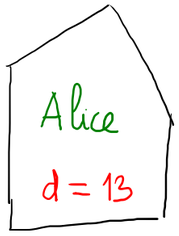
$5 \cdot d + K \cdot 64 = 1$

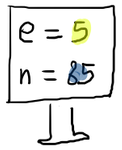
$5 \cdot 13 + (-1) \cdot 64 = 1$

$d = 13$

Algorithme d'Euclide étendu

1	64	1	0	
2	5	0	1	$64 = 12 \cdot 5 + 4$
3	4	1	-12	$5 = 1 \cdot 4 + 1$
4	1	-1	13	





J'ai le message $m = 10$ à envoyer à Alice

$$C = 10^5 \pmod{85}$$

$$m^2 = 100 \equiv 15 \pmod{85}$$

$$m^4 = 15^2 = 225 \equiv 55 \pmod{85}$$

$$C \equiv 55 \cdot 10 \equiv 550 \equiv 40 \pmod{85}$$

$c = 40$

Alice reçoit $C = 40$

$$C^{13} \equiv 40^{13} \pmod{85}$$

$$\equiv 40^{8+4+1} \equiv 40^8 \cdot 40^4 \cdot 40^1 \equiv 50 \cdot 55 \cdot 40 \equiv 10 \pmod{85}$$

$$40^2 \equiv 70 \pmod{85}$$

$$40^4 \equiv 55 \pmod{85}$$

$$40^8 \equiv 50 \pmod{85}$$