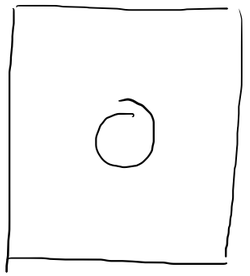
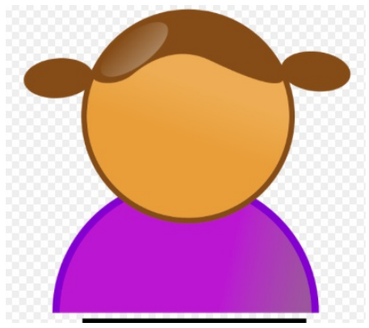
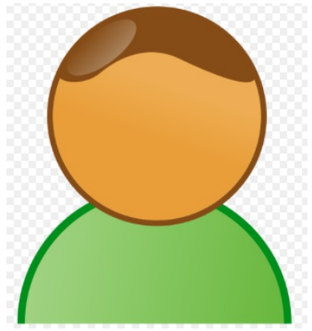
Message

coffre-fort

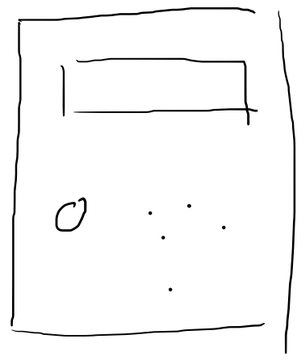




Alice

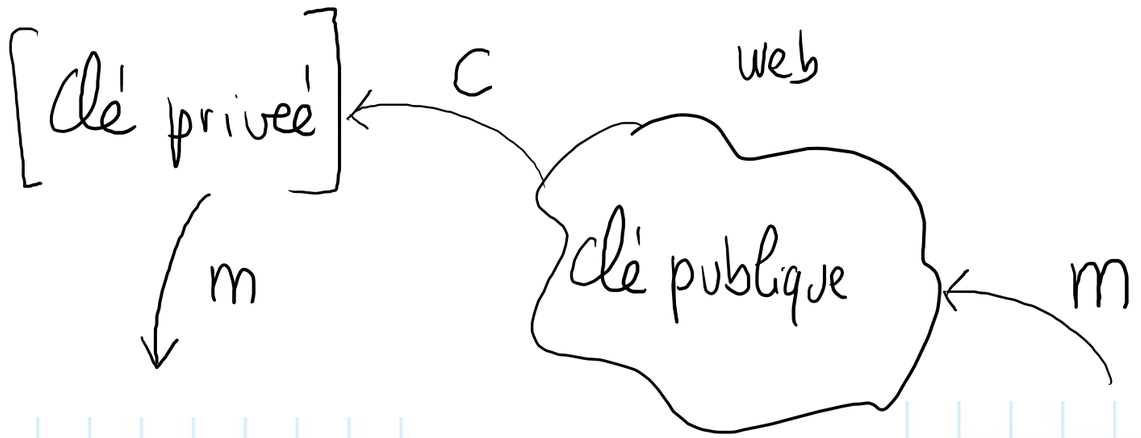


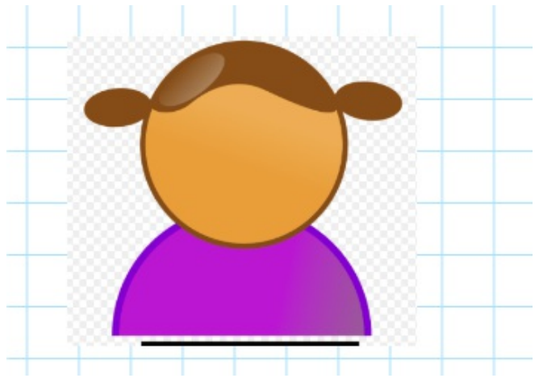
Bob

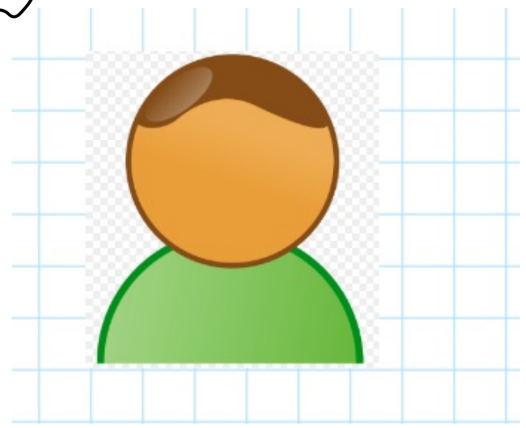


Symétrique

RSA





Alice asymétrique

$n = p \cdot q$

Bob

- pgdc
- nombre premiers
- $a^n \pmod p$

**2.5.2** Trouver tous les diviseurs communs positifs de

a) 16 et 48,

b) 30 et 45,

c) 18 et 65.

a) 16 / 48 pgcd(16,48) = 16

| | |
|---|---|
| 1 | 16 |
| 2 | 8 |
| 4 | 4 |

| | |
|---|---|
| 1 | 48 |
| 2 | 24 |
| 3 | 16 |
| 4 | 12 |
| 6 | ~~78~~ 8 |

b) $\sqrt{30} \simeq 5$

| | |
|---|---|
| 1 | 30 |
| 2 | 15 |
| 3 | 10 |
| 5 | 6 |

| | |
|---|---|
| 45 | 3 |
| 15 | 3 |
| 5 | 5 |
| 1 | |

$45 = 3^2 \cdot 5$

pgdc(45, 30) = 15

pgdc(30, 15) = 15

$3^7 \cdot 5^8 \cdot 7^2 \cdot 11^3$

**2.5.3** Trouver le plus grand diviseur commun de

a) 35 et 65,

b) 135 et 156,

c) 49 et 99.

a) $D_{35} = \{1, 5, 7, 35\}$

$D_{65} = \{1, 5, \quad , 13\ 65\}$

$D_{35} \cap D_{65} = \{1, 5\}$

$\text{pgdc}(35, 65) = 5$

b)

| Itération | a | b | a − b | Commentaire |
|---|---|---|---|---|
| 1 | 135 | 156 | | Comme a < b on échange a et b |
| 2 | 156 | 135 | 21 | |
| 3 | 135 | 21 | 114 | |
| 4 | 114 | 21 | 93 | |
| 5 | 93 | 21 | 72 | |
| 6 | 72 | 21 | 51 | |
| 7 | 51 | 21 | 30 | |
| 8 | 30 | 21 | 9 | |
| 9 | 21 | 9 | 12 | |
| 10 | 12 | 9 | 3 | |
| 11 | 9 | 3 | 6 | |
| 12 | 6 | 3 | 3 | |
| 13 | 3 | 3 | 0 | |
| 14 | 0 | 3 | | |

$a = 0 \Rightarrow \text{pgdc}(156, 135) = 3$

$156 = 135 \cdot 1 + 21$

$\text{pgdc}(156, 135) = \text{pgdc}(21, 135)$

$156 \cdot t + 135 \cdot s = 3$

## Propriétés du pgdc

1) $pgdc(a, a) = a$

2) $pgdc(a, 0) = a$

3) $pgdc(a, b) = pgdc(a - b, b) \qquad a > b$

4) $pgdc(a, b) = pgdc(a \bmod b, b)$

## Théorème du pgdc

Soit $a, b$ deux nombres entiers. Il existe deux entiers $s$ et $t$ tels que

$$a \cdot s + b \cdot t = \text{pgdc}(a, b)$$

On ne va pas faire une démonstration directe, on va créer un algorithme qui donne $s$ et $t$ à partir de $a$ et $b$.

Cet algorithme s'appelle l'algorithme d'Euclide étendu.

On commence par écrire $a > 0$

$$
\begin{aligned}
a &= 1 \cdot a + 0 \cdot b \\
b &= 0 \cdot a + 1 \cdot b \\
r &= 1 \cdot a + (-q \cdot b) \quad \Big| \quad a = q \cdot b + r
\end{aligned}
$$

On réitère les deux dernières lignes

Prenons un exemple $a = 2322$ et $b = 654$

| Ligne | r | a | b | Commentaire | q | Calcul de q |
|---|---|---|---|---|---|---|