RSA:

- Generar primos P y Q
- $N = P \cdot Q$
- $\phi(N) = (P-1)(Q-1)$

$\frac{1}{2^{100}}$

- Generar un número d tal que $MCD(d, \phi(N)) = 1$
- Construir e tal que e es inverso de d en módulo $\phi(N)$: $e \cdot d \equiv 1 \mod \phi(N)$
- Clave pública: (e, N)
  Clave privada: (d, N)

$Enc((e,N), m) = m^e \mod N$

$m \in \{0, \dots, N-1\}$

$Dec((d,N),m) = m^d \bmod N$

M $\quad e \in \{0, \ldots, M-1\}$

$MCD(e,M) = 1$

~~$\{p_1, \ldots, p_{1.000.000}\}$~~

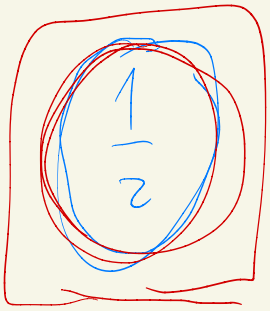
$N_{ij} = p_i * p_j$

$\{(e_1,N_1), \ldots, (e_{1000},N_{1000})\}$

$MCD(N_1,N_2)$

M $\quad a \in \{0, \dots, M-1\}$

$MCD(a, M) = 1$ $\quad n$



$\Omega\left(\frac{n}{\log(\log n)}\right)$

$a \in \{0, \dots, M-1\}$

$MCD(a, M) > 1$

$100 \rightarrow \frac{1}{2^{100}}$

$1 - \frac{1}{2^{100}}$

m^e $\qquad$ $e \bmod N = e$

m^{10} $\qquad$ $m^{10} = m^5 \cdot m^5$

$t = m^5$

$m^{10} = t \cdot t$

$ER(a, b, n) \rightarrow a^b \bmod n$

```
if b==0 return 1
else if b%2==0
    t = ER(a, b/2, n)
    return (t*t)%n
else
    t = ER(a, (b-1)/2, n)
    return (t*t*a)%n
```

$m \in \{0, \ldots, N-1\}$

$$\mathrm{DEC}((d,N), \underbrace{\mathrm{Enc}((e,N), m)}_{c}) = m$$

$$(m^e \bmod N)^d \bmod N$$

$$= \boxed{m^{e \cdot d} \bmod N} = m$$

$$\underbrace{((m^e \bmod N) \cdot \ldots \cdot (m^e \bmod N))}_{d} \bmod N$$

$$= (\underbrace{m^e \cdot \ldots \cdot m^e}_{d}) \bmod N = m^{e \cdot d} \bmod N$$

$$(m^e \bmod N \equiv m^e) \bmod N$$

$m \in \{0, \ldots, N-1\}$

$m^{d \cdot e} \bmod N = m$

$$m^{d \cdot e} \equiv m \bmod N$$

$d \cdot e \equiv 1 \bmod \phi(N)$

$\phi(N) \mid (d \cdot e - 1)$

$\alpha \cdot \phi(N) = d \cdot e - 1$

$\therefore \; d \cdot e = \alpha \cdot \phi(N) + 1$

$m^{\alpha \phi(N) + 1} \equiv m \bmod N$

$(m^{\phi(N)})^{\alpha} \cdot m \equiv m \bmod N$

$$m^{\phi(N)} \equiv 1 \bmod N$$

$N = P \cdot Q \qquad \phi(N) = (P-1)(Q-1)$

$m \in \{1, \dots, P-1\}$

$m^{P-1} \bmod P = 1$

$P = 7 \qquad \{1, \dots, 6\}$

$1^6 \bmod 7 = 1$

$2^6 \bmod 7 = 1$

$5^6 \bmod 7$

$((5 \cdot 5) \bmod 7)^3 \bmod 7$

$4^3 \bmod 7$

$((4 \cdot 4) \bmod 7 \cdot 4) \bmod 7$

$(2 \cdot 4) \bmod 7 = 1$ //

$$m^{\phi(N)} \bmod P = 1$$

$m \in \{1, \dots, P-1\}$
$m \neq 0$

$$\phi(N) = (P-1)\cdot(Q-1)$$

$$m^{(P-1)\cdot(Q-1)} \bmod P$$

$$\left(m^{(P-1)}\right)^{(Q-1)} \bmod P$$

$$= \left(\underbrace{m^{(P-1)} \bmod P}_{1}\right)^{(Q-1)} \bmod P$$

$m \in \{0, \dots, N-1\}$ es multiplo de P

$$m^{P-1} \bmod P = 1$$