→ • Attaques mathématiques

O connaît le module n, $k_{pub} = e$. et y chiffre.

Son but est de trouver $k_{pr} = d$ tq $e \cdot d \equiv 1 \bmod \phi(n)$,

O peut appliquer l'algo d'Euclide Etendu pour trouver d,

mais il ne connaît pas $\phi(n)$.

Si par contre il factorise $\phi(n) = (p-1)(q-1)$, il peut

écrire $\begin{cases} d^{-1} \equiv e \bmod \phi(n) \\ x \equiv y^d \bmod n. \end{cases}$

⇒ revient à factoriser n. qui doit être assez grand.

($n \geq 1024$.)

Vu la rapidité des attaques., il est recommandé d'avoir

$n \geq 2048$.

→ • Attaques canneaux cachés.

Exploite la consommation d'énergie et les calculs faits

par l'algo RSA.