Proposition (Correction de RSA).

$$d_{k_{pr}}\left(e_{k_{pub}}(x)\right) = x.$$

Preuve. On a

$$d_{k_{pr}}\left(e_{k_{pub}}(x)\right) = (x^e)^d \equiv x^{ed} \mod n \quad (1)$$

et $d \cdot e \equiv 1 \mod \phi(n) \iff d \cdot e = t \cdot \phi(n) + 1$ pour un certain $t \in \mathbb{N}$.

D'où $d_{k_{pr}}\left(\underset{y}{\underbrace{e_{k_{pub}}(x)}}\right) = x^{de} \equiv x^{1+t\cdot\phi(n)} = x \cdot \left(x^{\phi(n)}\right)^t \mod$ (2)

- Théorème d'Euler : si $pgcd(n, x) = 1$, alors $x^{\phi(n)} \equiv 1 \mod n$ (et donc $\forall$ entier l, $\left(x^{\phi(n)}\right)^l \equiv 1 \mod n$).

Donc on distingue deux cas :

$\rightarrow$ $pgcd(x, n) = 1$, $d_{k_{pr}}(y) \overset{(2)}{\equiv} \left(x^{\phi(n)}\right)^t . x$
$\equiv 1 \cdot x \equiv x \mod n$.

$\rightarrow$ $pgcd(n = pq, x) \neq 1$, donc x est de la forme

$x = r \cdot p$ ou $x = s \cdot q$ avec $r < q$ et $s < p$.

supposons que $x = rp \Rightarrow pgcd(x, q) = 1$.

$$(2) : \left(x^{\phi(n)}\right)^t = \left(x^{(q-1)(p-1)}\right)^t = \left(\left(x^{\phi(q)}\right)^t\right)^{p-1}$$
$$\equiv 1^{(p-1)} \quad \left(\text{Euler} : x^{\phi(q)} \equiv 1 \mod q\right)$$
$$\equiv 1 \quad (\bmod\ q)$$

Donc $\left(x^{\phi(n)}\right)^t = 1 + u \cdot q$