Date : ....

decrypted message: $L(c^{\lambda} \pmod{n^2}, n) \cdot \mu \pmod n$

here, $L(x, n) = \dfrac{x-1}{n}$, $c = g^m r^n \pmod{n^2}$

$\lambda = \phi(n)$

where $g = (n+1)$; $r \xleftarrow{\$} \mathbb{Z}_n^*$. $\left[\begin{matrix} 0 < r < n \\ \gcd(r, n) = 1 \end{matrix}\right]$

and $n = p \cdot q$; $p, q \in$ primes.

$\lambda = (p-1)(q-1)$; $\mu = \lambda^{-1} \pmod n$

Note that $\phi(n^2) = \phi(p^2q^2) = p^2q^2 \dfrac{(p-1)}{p} \dfrac{(q-1)}{q}$

$= pq(p-1)(q-1)$

$\Rightarrow \phi(n^2) = n\lambda.$

$L(c^{\lambda} \pmod{n^2}, n) \cdot \mu \pmod n = \dfrac{\left[\left((n+1)^m r^n\right)^{\lambda} \pmod{n^2}\right] - 1}{n} \mu \pmod n$

$= \dfrac{(n+1)^{\lambda m} \cdot r^{n\lambda} \pmod{n^2} - 1}{n} \cdot \mu \pmod n$

$\left[\begin{matrix} \text{since } n\lambda = \phi(n^2) \text{ and } \gcd(r, n) = 1 \Rightarrow \gcd(r, n^2) = 1 \\ \text{we have } r^{n\lambda} \equiv 1 \pmod{n^2} \end{matrix}\right]$

$= \dfrac{(n+1)^{\lambda m} \pmod{n^2} - 1}{n} \cdot \mu \pmod n.$

Signature.................................

Date : ....

now, $(n+1)^{\lambda m} = n^{\lambda m} + (\lambda m) \cdot n^{\lambda m-1} + \cdots (\lambda m) n + 1.$

$\Rightarrow (n+1)^{\lambda m} - 1 \pmod{n^2} = n^{\lambda m} + (\lambda m) n^{\lambda m-1} + \cdots \lambda m n + 1 - 1 \pmod{n^2}$

$= \lambda m n \pmod{n^2}.$

$\therefore \dfrac{(n+1)^{\lambda m} \pmod{n^2} - 1}{n} \mu \pmod{n}$

$= \dfrac{[(n+1)^{\lambda m} - 1] \pmod{n^2}}{n} \cdot \mu \pmod{n}$

$= \dfrac{\lambda m \cancel{n}}{\cancel{n}} \cdot \mu \pmod{n}$

$= m \cdot (\lambda \mu) \pmod{n} \quad [\lambda \mu \equiv 1 \pmod{n}$

$= m \pmod{n} = m = \text{message}.$

$\rightarrow$ The scheme is correct!

Signature..............................