and the Control of th		Date :
deoxypted r	nessage: L(c')	modn2), n)u(modn)
here, L(x	m= x-1, r=	gm m (mod n2)
$\lambda = O(n)$	n'	0
where g	$m = \frac{\chi - 1}{n}, x = $	- Z* OZ8212
and n= ?	o.q.; piq. Eprin	nes.
$\lambda = (p)$	-D(9-D; u= 2	(mod n)
Note that	$\phi(n^2) = \phi(p^2q^2) = -pq(p^2)$ => $\phi(n^2) = n\lambda$.	= P ² q ² (p-1)(q-1)
	-po/p-	-D(9-1) P 9
	$\Rightarrow \phi(n^2) = n \lambda$.	
L(c) (mod n2)),n).ll (mod n)= (n-	+1) mgn2) (ned n2)-1]
		YL
$=(n+1)^{2}$	in hys (mod no) -1	(modis)
yana and	n	M (modn)
Since na=p	(n²) and gcd(r, n) =1 (mod n²)	1=1=7 gcd (r, 12)=1]
we have y	ina =1 (mod n2)	
= (n+1)2m	(mod n2)-1	(mod n)
	N	troois.

Signature.....

TO.

Date :
now , $(n+1)^{2m} = n^{2m} + (2m) \cdot n^{2m-1} \cdot (2m)n+1$.
=> $(n+1)^{2m}-1$ $(mod n^2)=N^2+(2m)n^2m^2+2mn+1-1$ $(mod n^2)$
$= nmn \pmod{n^2}$.
(n+1) 2m (mod n²)-1 u (mod n)
$= \frac{(n+1)^{2m}-1}{n} \frac{(mod n^2)}{n} \frac{(mod n^2)}{n}$
= 2mx (modn)
= m-(au) (mod n) [au=1(mod n)]
= m (mod n) = m = message.
-> the scheme is correct!

Signature