

15

$n = p \cdot q = 216773774599077 \cdot 4758131272895389067293$

$(e) d = 1 \text{ mod } (\phi) \quad \phi = (p-1)(q-1)$

USING wolfram alpha
 $\phi = 102105101047635104465904131931657592$
 $e = 2287529$

| a | b | c | d |
|---------|---------|---------|---------|
| 2287529 | 2287529 | 1955237 | 449 |
| 1955237 | 1955237 | 331642 | 856 |
| 331642 | 331642 | 297377 | 159387 |
| 297377 | 297377 | 34315 | 161450 |
| | | 2287529 | 2044572 |
| | | | 918595 |
| 2287529 | 11458 | 11394 | 1 |
| 11458 | 11394 | 54 | 1 |
| 11394 | 54 | 12 | 143 |
| 54 | 12 | 11 | 4 |
| 12 | 11 | 1 | 1 |
| 11 | 1 | 0 | 11 |
| 1 | 0 | - | 1 |

To decode

$c^d \text{ mod } n$

$= 1027795314451781441374847538625788256^d \text{ mod } n$

decoded message:

52807870857374797201687770877083

USING calculator, wolfram alpha and mod exp. java to decode $1 = sp + de$

| s | d |
|----------|--------------------------------|
| -2093674 | 941852144648755261760623254442 |
| 1740041 | -2093674 |
| -303583 | 1740041 |
| 2721762 | -303583 |
| -31467 | 272176 |
| -10487 | 20920 |
| 10433 | -10487 |
| -54 | 10433 |
| 11 | -54 |
| -10 | 11 |
| 1 | -10 |
| 1 | 1 |

$d = 941852144648755261760623254442258121$

$1 = (-54)(11394) + 4(54)$
 $1 = (11)(54) + 4(12)$
 $1 = (-10)(12) + 4(11)$
 $1 = (1)(11) + 1(-10)$
 $1 = (1)(0) + (1)(0)$