구하고자 하는 값:

$a^7 = 1466092 \mod 1476221$

오일러의 정리

$N = p \cdot q \ (p, q : 소수),\ (a, N) = 1$

$\Rightarrow a^{(p-1)(q-1)} = 1 \mod N$

오일러의 정리에 따르면

$a^{(p-1)(q-1)} = 1 \mod N$ 이므로

$a^{k(p-1)(q-1)+1} = a \mod N$ 이다

$1 \cdot a$

오일러 정리를 이용한 값 구하기

$a^7 = 1466092 \mod 1476221$

$1476221 = 613 \times 1213$ 알고 있다는 가정

$a^{k(p-1)(q-1)+1} = a \mod N$

$a^{7d} = a^{k(p-1)(q-1)+1} \mod 1476221$

$7d = k(p-1)(q-1)+1 = k \cdot 1212 \cdot 1216 + 1$

$= 1473792k + 1$

If $k=4$) $d = 842167$

$(a^7)^{842167} = 1466092^{842167} \mod 1476221$

$\therefore a = 315972$