RSA Algorithm

1) $p = 17, q = 11$

$n = p \times q = 11 \times 17 = 187$

$\phi(n) = (p-1)(q-1)$

$= 16 * 10 = 160.$

$\gcd(e, \phi(n)) = 1$

chosen $\gcd(7, 160) = 1$

So $\underline{\underline{e = 7}}$

$de = 1 \bmod \phi(n)$

$d = e^{-1} \bmod \phi(n).$

so. $d = \dfrac{((\phi(n) * i) + 1)}{e}$

when $i = 1$ $= \dfrac{((160 * 1) + 1)}{7}$

$= \dfrac{161}{7} = 23$

So $\boxed{d = 23}$

so public key $= \{7, 187\}.$

private key $= \{23, 187\}.$

CamScanner

consider plaintext = 88.

$$c = 88^7 \bmod 187$$

$88^7 \bmod 187$
can be written as

$$(88^4 \bmod 187) \times (88^2 \bmod 187) \times (88^1 \bmod 187) \bmod 187$$

by exploiting properties of modular arithemetic.

$88^1 \bmod 187 = 88$

$88^2 \bmod 187 = 77$

$88^4 \bmod 187 = 132$

so $88^7 \bmod 187 = (88 \times 77 \times 132) \bmod 187$

$= 11$

For decryption

$M = 11^{23} \bmod 187$

$11^{23} \bmod 187 = [(11^1 \bmod 187) \times (11^2 \bmod 187)$
$\times (11^4 \bmod 187)$
$\times (11^8 \bmod 187)$
$\times (11^8 \bmod 187)]$
$\bmod 187$

$11^1 \bmod 187 = 11$
$11^2 \bmod 187 = 121$
$11^4 \bmod 187 = 55$
$11^8 \bmod 187 = 33$

So $11^{23} \bmod 187 = (11 \times 121 \times 55 \times 33 \times 33)$
$\bmod 187$

$= 88$

CamScanner