RSA

In RSA, if P = 3 & q = 11, M = 31
Compute Encryption & Decryption.

Step 1:-

Calculate $n = p * q$

$n = 3 \times 11$

$\boxed{n = 33}$

Step 2:-

Calculate $\phi(n) = (P-1) * (q-1)$

$= (3-1) * (11-1)$

$= 2 \times 10$

$\boxed{\phi(n) = 20}$

Step 3:-

Choose "e" such that $1 < e < \phi(n)$

e is co-prime to $\phi(n)$. $\gcd(e, \phi(n)) = 1$

$1 < e < \phi(n)$

$1 < e < 20$

$\boxed{e = 3}$

Step 4:-

Calculate d, such that

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

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

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

$\because d = \frac{1 + K\phi(n)}{e}$

$d = \frac{1+1(20)}{3} \Rightarrow \frac{21}{3} = 7$

$d = \frac{1+2(20)}{3} \Rightarrow \frac{41}{9} = 4.5$

$d = \frac{1+4(20)}{3} = .$

$d = 7$

Public Key = $\{e, n\} = \{3, 33\}$

Private Key = $\{d, n\} = \{7, 33\}$

▶ Given $M = 31$

For Encryption:-

$C = M^e \bmod n$

$C = 31^3 \bmod 33$

$31 \bmod 33 = 31$

$31^2 \bmod 33 = 4$

$124 \bmod 33 = 25.$

$\boxed{C = 25}$

For Decryption:-

$M = C^d \bmod 33$

$= 25^7 \bmod 33$

$25 \bmod 33 = 25 \qquad 25^2 \bmod 33 = 31$

$25^4 \bmod 33 = 4$

$25 \times 31 \times 4 = 3100$

$3100 \bmod 33 =$

$\boxed{D = 31}$

In RSA, if e = 13 & n = 100, Encryp the message "HAPPY" using 0-25 for A to Z

Step 1:-

Choose two large prime numbers

$P = 7$, $q = 11$

Step 2:-

Given $\boxed{n = 100}$

Step 3:-

Calculate $\phi(n) = (P-1) * (q-1)$

$= (7-1) * (11-1)$

$= 6 * 10$

$\boxed{\phi(n) = 60}$

Step 4:-

Given $\boxed{e = 13}$

▶ H A P P Y

7 + 0 + 15 + 15 + 24

$\boxed{M = 61}$

For Encryption:-

$C = M^e \bmod n$

$= 61^{13} \bmod n$

$61 \mod 100 = 61$

$61^2 \mod 100 = 21$

$61^4 \mod 100 = 41$

$61^8 \mod 100 = 1.9170$

$61 \times 41 \times 21 \times 1.9170 = 1.006865$

$$C = 1.006865$$