Message = G E N E R A L S

**Step 1: CONVERT GENERALS TO ASCII (DECIMAL)**

G = 71

E = 69

N = 78

E = 69

R = 82

A = 65

L = 76

S = 83

**Step 2: Select two random prime numbers ( p and q )**

p = 83

q = 107

**Step 3: Compute N as the product of two prime numbers of p and q**

N = p x q

N = 83 x 107

N = 8881

**Step 4: Compute for Euler’s totient** ϕ (n) = ( p - 1 ) ( q - 1 )

ϕ (n) = ( p - 1 ) ( q - 1 )

ϕ (n) = ( 83 - 1 ) ( 107 - 1 )

ϕ (n) = ( 82 ) ( 106 )

ϕ (n) = 8692

**Step 5: Select encryption key (public key) e such as, gcd (ϕ (n), e ) = 1 and 1 < e < ϕ (n)**

**gcd (8692, 971) = 1**

e = 971

Solution:

a = b q + r

**Where: a = ϕ (n)**

**b = e**

**q = quotient (divide a and b)**

**r = remainder of q**

8692 = 971(8) + 924

971 = 924(1) + 47

924 = 47(19) + 31

47 = 31(1) + 16

31 = 16(1) + 15

16 = 15(1) + 1

**Step 6: Rewrite as:**

8692 - 971(8) = 924

971 - 924(1) = 47

924 - 47(19) = 31

47 - 31(1) = 16

31 - 16(1) = 15

16 - 15(1) = 1

**Step 7: Calculate decryption key (private key) d using Extended Euclidean Algorithm (Back substitution)**

Solution:

1 = 16 - 1(15)

1 = 16 - 1(31 - 1(16))

1 = 16 - 1(31) + 1(16)

1 = -1(31) + 2(16)

1 = -1(31) + 2(47 - 1(31))

1 = -1(31) + 2(47) - 2(31)

1 = 2(47) - 3(31)

1 = 2(47) - 3(924 - 19(47))

1 = 2(47) - 3(924) + 57(47)

1 = -3(924) + 59(47)

1 = -3(924) + 59(971 - 1(924))

1 = -3(924) + 59(971) - 59(924)

1 = 59(971) - 62(924)

1 = 59(971) - 62(8692 - 8(971))

1 = 59(971) - 62(8692) + 496(971)

1 = -62(8692) + 555(971)

d = 555 mod 8692

d = 555

**Step 8: Public Key { e, n } and Private Key {d, n}**

(Public Key) e = {971, 8881}

(Private Key) d = {555, 8881}

**Step 9: Encryption Process, using M = (G = 71) , (E = 69) , (N = 78) , (E = 69) , (R = 82) , (A = 65) , (L = 76) , (S = 83)**

*Where:*

M = ASCII Value

e= encryption key

n= 8881

Encrypting G:

C = 71^971 mod 8881

C = 4832

Encrypting E:

C = 69^971 mod 8881

C = 8447

Encrypting N:

C = 78^971 mod 8881

C = 2769

Encrypting E:

C = 69^971 mod 8881

C = 8447

Encrypting R:

C = 82^971 mod 8881

C = 1991

Encrypting A:

C = 65^971 mod 8881

C = 3069

Encrypting L:

C = 76^971 mod 8881

C = 2550

Encrypting S:

C = 83^971 mod 8881

C = 332

**Step 10: Decryption Process**



*Where:*

C = Ciphertext Value

d= decryption key

n= 8881

Decrypting G:

M = 4832^555 mod 8881

M = 71

Decrypting E:

M = 8447^555 mod 8881

M = 69

Decrypting N:

M = 2769^555 mod 8881

M = 78

Decrypting E:

M = 8447^555 mod 8881

M = 69

Decrypting R:

M = 1991^555 mod 8881

M = 82

Decrypting A:

M = 3069^555 mod 8881

M = 65

Decrypting L:

M = 2550^555 mod 8881

M = 76

Decrypting S:

M = 332^555 mod 8881

M = 83