## Part 1:

p =1049

q = 1543

n = p \* q = 1,049 \* 1,543 = 1,618,607

z = (p – 1) \* (q – 1) = (1049 – 1) \* (1543 – 1) = 1,616,016

public exponent e = gcd (e, euler function (n) ) = 1

gcd (e, fi (n)) = 1

gcd (e, (p-1) (q-1)) = 1

gcd (e, p-1) = 1, gcd (e, q-1) = 1

1511 checks both these fields and will now be our public exponent, e.

Now to find our d, private exponent.

e \* d 1 mod (n)

d = e ^ -1 mod fi(n)

d = 537959 = 1,511 ^ -1 mod 1616016

s = 194249 - my student number

Encryption:

Each letter separately:

y = s ^ e mod n – where y is the cryptogram

s1 = 1, y = 1 ^ 1511 mod 1618607, y1 = 1

s2 = 9, y = 9 ^ 1511 mod 1618607, y2 = 1414345

s3 = 4, y = 4 ^ 1511 mod 1618607, y3 = 318384

s4 = 4, y = 2 ^ 1511 mod 1618607, y4 = 1543467

s5 = 4, y = 4 ^ 1511 mod 1618607, y5 = 318384

s6 = 4, y = 9 ^ 1511 mod 1618607, y6 = 1414345

Wholly:

s = 194249, 194249 ^ 1511 mod 1618607 = 1310087

Decryption:

Each Letter Separately:

s = y ^ d mod n - decryption process, s is plain text

y1 = 1, s = 1 ^ 537959 mod 1618607, s1 = 1

y2 = 1,414,345, s = 1414345 ^ 537959 mod 1618607, s2 = 9

y3 = 318,384, s = 318384 ^ 537959 mod 1618607, s3 = 4

y4 = 1,543,467, s = 1543467 ^ 537959 mod 1618607, s4 = 2

y5 = 318,384, s = 318384 ^ 537959 mod 1618607, s5 = 4

y6 = 1,414,345, s = 1414345 ^ 537959 mod 1618607, s6 = 9

Wholly:

y = 1310087, 1310087 ^ 537959 mod 1618607, s = 194249

After that, compute s ^ d mod n and x ^ e mod n:

1. s ^ d mod n = x

194249 ^ 537959 mod 1618607 = 109374

1. x ^ e mod n = s

109374 ^ 1511 mod 1618607 = 194249

## Part 2:

p =1049

q = 1543

In p we have 2 roots: 1 and 1049-1 = (1, 1048)

In q we have 2 roots: 1 an 1543-1 = (1, 1542)

Possible combinations:

(1,1) maps to 1

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(1, 1048) maps to

a= 1

b = 1048

n = 1618607

p = 1049

q = 1543

alfa = 253

beta = -172

We need to map two elements from the direct product (Zp X Zq) to the composite product by:

1. x = a mod p = 1 mod 1049

x= b mod q = 1048 mod 1543

1. Bezeout Identity of 1049 and 1543:

1049 \* 253 + 1543 \* (-172) = 1

1. Mapping

(a,b) (a\*beta\*q + b \* alfa \* p) mod n= x

1. (1 \* (-172) \* 1543 + 1048 \* 253 \* 1049) mod 1618607 = -(265396 + 278136056) mod 1618607 = 1088863

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(1, 1542)

a= 1

b = 1542

n = 1618607

p = 1049

q = 1543

alfa = 253

beta = -172

We need to map two elements from the direct product (Zp X Zq) to the composite product by:

1. x = a mod p = 1 mod 1049

x= b mod q = 1542 mod 1543

1. Bezeout Identity of 1049 and 1543:

1049 \* 253 + 1543 \* (-172) = 1

1. Mapping

(a,b) (a\*beta\*q + b \* alfa \* p) mod n= x

1. (1 \* (-172) \* 1543 + 1542\* 253 \* 1049) mod 1618607 = (-265396 + 409242174) mod 1618607 = 1087814‬

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(1048, 1542) = n-1 = 1618607 -1 = 1618606