## Example of RSA Algorithm

```
Encryption \rightarrow C = M<sup>e</sup> mod N
Decryption \rightarrow M = C<sup>d</sup> mod N
```

Given p=61, q=53, Message, M=123 and Public Key, e = 17

N=p\*q = 
$$61*53 = 3233$$
  
Totient  $\Theta(p,q) = (p-1)(q-1)$   
=  $(61-1)(53-1)$   
=  $3120$ 

The encryption  $\rightarrow$  C =  $M^e \mod N$ 

C = 
$$M^e \mod N = 123^{17} \mod N = 123^{17} \mod 3233$$
  
= 855 (from scientific calculator)

 $= M^e \mod N = 123^{17} \mod N = 123^{17} \mod 3233$ 

Simple hand written calculation;

$$17 = 1*2^{0} + 0*2^{1} + 0*2^{2} + 0*2^{3} + 1*2^{4} = 1 + 16$$

$$123^{1} = 123 \mod 3233 = 123$$

$$123^{2} = 123*123 \mod 3233 = 15129 \mod 3233 = 2197$$

$$123^{4} = 2197*2197 \mod 3233 = 4826809 \mod 3233 = 3173$$

$$123^{8} = 3173*3173 \mod 3233 = 10067929 \mod 3233 = 367$$

 $123^{16} = 367*367 \mod 3233 = 2136$ 

$$123^{17}$$
 =  $(123^1 * 123^{16}) \mod 3233 = 123*2136 \mod 3233$   
=  $262728 \mod 3233$ 

= 855

Private Key d can be calculated from ed  $\equiv 1 \pmod{\Theta(p,q)}$ 

Therefore,  $17d \equiv 1 \pmod{3120}$ , this can be wrote as

$$d \equiv 17^{-1} \pmod{3120}$$
, it is same as  $17a + 3120b = 1$ 

If we can find a and b, we can find public key d. Then, the simplest way to find a and b is using the Extended Euclid Algorithm

$$17a + 3120b = 1$$

$$\Rightarrow$$
 3120 = 183(17) + 9  
 $\Rightarrow$  9 = 3120 - 183(17)  $\Rightarrow$  (1)

also 
$$9 = 1+8$$
  
  $1 = 9-8$ 

From (1) and (2)

Compare 17(-367) + 3120(2) = 1 with 17a + 3120b = 1Then,

$$a = -367$$
 and  $b = 2$ 

Therefore,

d = 
$$17^{-1} \mod 3120$$
  
=  $-367 \mod 3120$   
=  $3120 - 367$   
=  $2753$ 

So that, private key d = 2753.

The Decryption  $\rightarrow$  M = C<sup>d</sup> mod N

Therefore 
$$M = C^d \mod N$$
  
 $M = 855^{2753} \mod 3233$ 

Same way using the scientific calculator and get back the original message, M = 123

Or using simple hand written computation:

 $M = 855^{2753} \mod 3233$ 

## $855^{2753} \mod 3233$

```
1*2^{0}+1*2^{7}+1*2^{8}+1*2^{10}+1*2^{12}=1+64+128+512+2048
2753
855^{1}
                   855 mod 3233
                                              855
855^{2}
                   855*855 \mod 3233 =
                                              731025 \mod 3233 =
                                                                        367
855^{4}
             =
                   367*367 \mod 3233 =
                                              134689 mod 3233 =
                                                                        2136
855^{8}
             =
                   2136*2136 mod 3233 =
                                              4562496 \mod 3233 =
                                                                        733
855^{16}
             =
                   733*733 \mod 3233 =
                                              537289 mod 3233 =
                                                                        611
855^{32}
             =
                   611*611 mod 3233
                                              = 1526
855^{64}
                   1526*1526 mod 3233
                                              = 916
855^{128}
             =
                   916*916 mod 3233
                                              = 1709
855^{256}
                   1709*1709 mod 3233
                                              = 1282
855^{512}
                   1282*1282 mod 3233
             =
                                              = 1160
855^{1024}
                   1160*1160 mod 3233
                                              = 672
855^{2048}
                   672*672 mod 3233
                                              = 2197
Therefore,
             = 855^{(1+64+128+512+2048)}
855^{2753}
             = 855*916*1709*1160*2197 mod 3233
855^{65}
             = 855*916 mod 3233
                                                     794
855^{640}
             = 1709*1160 mod 3233
                                              611
            = 855^{(65+640+2048)}
8552753
             = 796*611*2197 mod 3233
             = 123
```

M = 123 and get back the original messages.