Example 1

Watch presentation: [here]. https://www.youtube.com/watch?v=pHES8eNor6k

Let's select:

P =11 Q=3 [Link] http://asecuritysite.com/encryption/rsa?val=11%2C3%2C3%2C4

The calculation of n and PHI is:

n=P × Q = 11 × 3 =33

PHI = (p-1) × (q-1) = 20

The factors of *PHI* are 1, 2, 4, 5, 10 and 20. Next the public exponent e is generated so that the greatest common divisor of *e* and *PHI* is 1 (e is relatively prime with *PHI*). Thus, the smallest value for e is:

e = 3

Next we can calculate d from:

(3 x d) mod (20) = 1 [Link]

Thus the smallest value of d will be:

d = 7

Encryption key [33,3]

Decryption key [33,7]

Then, with a message of 4, we get:

Cipher = $(m)^e$ mod n

Cipher = $(4)^3$ mod 33 = 31

Decoded = $(\text{cipher})^d$ mod n

Decoded = 31^7 mod 33 = 4

Example 2

Let's select (using the same P and Q, but we'll pick a different e value):

P =11 Q=3 [Link] http://asecuritysite.com/encryption/rsa?val=11,3,7,2

The calculation of n and PHI is:

n=P × Q = 11 × 3 =33

PHI = (p-1)(q-1) = 20

We can select e as:

e = 7

Next we can calculate d from:

$7 \times d \bmod (20) = 1$ [Link]

$d = 3$

Encryption key [33,7]

Decryption key [33,3]

Then, with a message of 2, we get:

Cipher = $(2)^7 \bmod 33 = 29$

Decoded = $29^3 \bmod 33 = 2$

Example 3

Let's select:

P =13 Q=11 [Link] http://asecuritysite.com/encryption/rsa?val=13%2C11%2C7%2C7

The calculation of n and PHI is:

$n = P \times Q = 13 \times 11 = 143$

$PHI = (p-1)(q-1) = 120$

We can select e as:

$e = 7$

Next we can calculate d from:

$(7 \times d) \bmod (120) = 1$ [Link]

$d = 103$

Encryption key [143,7]

Decryption key [143,103]

Then, with a message of 7, we get:

Cipher = $(7)^7 \bmod 143 = 6$

Decoded = $(6)^{103} \bmod 143 = 7$

Example 4

Let's select:

P =47 Q=71 [Link] http://asecuritysite.com/encryption/rsa?val=47%2C71%2C79%2C688

The calculation of n and PHI is:

$n = P \times Q = 13 \times 11 = 3337$

PHI = (p-1)(q-1) = 3220

We can select e as:

e = 79

Next we can calculate d from:

(79 × d) mod 3220 = 1 [Link]

d = 1019

Encryption key [3337,79]

Decryption key [3337,1019]

Then, with a message of 688, we get:

Cipher = $(688)^{79}$ mod 3337 = 1570

Decoded = $(1570)^{1019}$ mod 3337 = 688

Example 5

Let's select:

P=23 Q=41 [Link] http://asecuritysite.com/encryption/rsa?val=23%2C41%2C7%2C35

The calculation of n and PHI is:

n=P×Q = 24×41 =943

PHI = (p-1)(q-1) = 880

We can select e as:

e = 7

Next we can calculate d from:

(7 x d) mod 880 = 1 [Link]

d = 503

Encryption key [943,7]

Decryption key [943,503]

Then, with a message of 35, we get:

Cipher = $(35)^{7}$ mod 943 = 545

Decoded = 545^{503} mod 943 = 35

Example 6

Let's select:

P=61, Q=53 [Link] http://asecuritysite.com/encryption/rsa?val=61,53,17,65

The calculation of n and PHI is:

N = 61 x 53 = 3233

PHI = (P-1)(Q-1) = 3120

We can select e as:

e = 17

Next we can calculate d from:

(d x 17) mod (3120) = 1

d= 2753

Encryption key [3233,17]

Decryption key [3323,2753]

Then with a message of 65, we get:

Cipher = $(65)^{17}$ mod 3233 = 2790

Decoded = 2790^{2753} mod 3233 = 65

Example 7

Let's select:

P=7, Q=13 [Link] http://asecuritysite.com/encryption/rsa?val=7,13,5,10

The calculation of n and PHI is:

N = 7 x 13 = 91

PHI = (P-1)(Q-1) = 72

We can select e as:

e = 5

Next we can calculate d from:

(d x 5) mod (72) = 1

d= 29

Encryption key [91,5]

Decryption key [91,29]

Then with a message of 10, we get:

Cipher = $(10)^{5}$ mod 91 = 82

Decoded = $82^{29} \bmod 91 = 10$

- Prof Bill Buchanan, 2015