



**For RSA algorithm, we need to generate a public and a private key.**

1. Choosing two distinct prime numbers:  $p = 6733$ ,  $q = 6073$
2. Computing  $n = p \times q = 6733 \times 6073 = 40889509$
3. Computing least common multiple of  $(p-1)$  and  $(q-1)$ :  $\text{lcm}(6732, 6072) = 309672$
4. Selecting any number that ensure  $1 < e < 123200$  and coprime to  $309672$ . Then let  $e = 7$ .
5. Computing  $d$ , the modular multiplicative inverse of  $e \pmod{\text{lcm}(p-1, q-1)}$ . Then  $d = 44239$ .
6. Now, public key =  $\{e, n\} = \{7, 40889509\}$  and private key =  $\{d, n\} = \{44239, 40889509\}$
7. For encrypting the message, we can pick the public key. " $message^e \pmod{n}$ " will return us the cipher text.
8. For decrypting the message, we should pick the private key. " $message^d \pmod{n}$ " will return us the plain text.
9. Our hash function returns a hexadecimal value. We need to convert it into decimals so we can do the calculations. Decimal value of "b9a2" is "47522".
10.  $47522^7 \pmod{40889509} = 15279871$
11.  $434054^{136889} \pmod{2469981} = 47522$
12. This is how RSA algorithm works.

### **SAMPLE RUN 1)**

**ID:** 29438745367

**Prime numbers for source keys:** (5501, 4481)

**Source public key:** {9;24649981}

**Source private key:** {136889;24649981}

**Prime numbers for destination keys:** (6733, 6073)

**Destination public key:** {7;40889509}

**Destination private key:** {44239;40889509}

```
-----  
Original ID: 29438745367  
-----
```

```
Source Public Key: {9;24649981}
```

```
Source Private Key: {136889;24649981}
```

```
Destination Public Key: {7;40889509}
```

```
Destination Private Key: {44239;40889509}  
-----
```

```
Session Key: 4480919969
```

```
Returned Session Key: 4480919969  
-----
```

```
Original Hashed ID (CRC-16/MODBUS): 0xb9a2
```

```
Computed Hash: 0xb9a2  
-----
```

```
Verified  
-----
```

### **SAMPLE RUN 2)**

**ID:** 74543222905

**Prime numbers for source keys:** (5501, 4481)

**Source public key:** {9;24649981}

**Source private key:** {136889;24649981}

**Prime numbers for destination keys:** (6733, 6073)

**Destination public key:** {7;40889509}

**Destination private key:** {44239;40889509}

```
-----  
Original ID: 74543222905  
-----
```

```
Source Public Key: {9;24649981}
```

```
Source Private Key: {136889;24649981}
```

```
Destination Public Key: {7;40889509}
```

```
Destination Private Key: {44239;40889509}  
-----
```

```
Session Key: 2376444027
```

```
Returned Session Key: 2376444027  
-----
```

```
Original Hashed ID (CRC-16/MODBUS): 0x7bff
```

```
Computed Hash: 0x7bff  
-----
```

```
Verified  
-----
```

# For the first 2 samples, e value in RSA algorithm is set to 7.

# For the next 2 run samples, we decreased the value of e in RSA algorithm to 3, for making it run faster.

#### SAMPLE RUN 3)

ID: 29438745367

Prime numbers for source keys: (4507, 3491)

Source public key: {7;15733937}

Source private key: {2246563;15733937}

Prime numbers for destination keys: (5737, 5077)

Destination public key: {5;29126749}

Destination private key: {1455797;29126749}

```
-----
Original ID: 29438745367
-----
Source Public Key: {7;15733937}
Source Private Key: {2246563;15733937}
Destination Public Key: {5;29126749}
Destination Private Key: {1455797;29126749}
-----
Session Key: 3126343501
Returned Session Key: 3126343501
-----
Original Hashed ID (CRC-16/MODBUS): 0xb9a2
Computed Hash: 0xb9a2
-----
Verified
-----
```

#### SAMPLE RUN 4)

ID: 74543222905

Prime numbers for source keys: (4507, 3491)

Source public key: {7;15733937}

Source private key: {2246563;15733937}

Prime numbers for destination keys: (5737, 5077)

Destination public key: {5;29126749}

Destination private key: {1455797;29126749}

```
-----
Original ID: 74543222905
-----
Source Public Key: {7;15733937}
Source Private Key: {2246563;15733937}
Destination Public Key: {5;29126749}
Destination Private Key: {1455797;29126749}
-----
Session Key: 2408629342
Returned Session Key: 2408629342
-----
Original Hashed ID (CRC-16/MODBUS): 0x7bff
Computed Hash: 0x7bff
-----
Verified
-----
```