
7.1. Let the two primes p = 41 and q = 17 be given as set-up parameters for RSA.

1. Which of the parameters e1 = 32,e2 = 49 is a valid RSA exponent? Justify your choice.
One of the conditions for exponent is that
gcd(e, phi(n)) = 1

N = p * q = 41*17 = 697
phi(n) = (p-1) * (q-1) = (41 - 1) * (17 - 1) = 40 * 16 = 640

For e1 = 32, gcd(32, 640) != 1
For e2 = 49, gcd(49, 640) = 1.

So, e2 = 49 is a valid RSA exponent.

2. Compute the corresponding private key Kpr = (p,q,d). Use the extended Eu- clidean algorithm for the inversion and point out every calculation step.

Computing gcd for 49 and 640
gcd(640, 49)
= gcd(640%49, 49)
= gcd(3, 49)
= gcd(3, 49%3)
= gcd(3, 1)
= gcd(3%1, 1)
= gcd(0, 1)
1

Writing EEA equations for above
640 = 13*49 + 3
=> 3 = 640 - 13*49

49 = 16*3 + 1
=> 1 = 49 - 16*3
Replacing 3 from above
=> 1 = 49 - 16*(640 - 13*49)
=> 1 = 209*49 - 16*640
So, multiplicative inverse of 49 is 209

So, (p, q, d) is (41, 17, 209)

7.2. Computing modular exponentiation efficiently is inevitable for the practicability of RSA.

Compute the following exponentiations xe mod m applying the square- and-multiply algorithm:

1. x = 2, e = 79, m = 101 2. x = 3, e = 197, m = 101

After every iteration step, show the exponent of the intermediate result in binary notation.

Answer:
1. x = 2, e = 79, m = 101

Writing 79 in binary
79 = 1001111_b

1a: 2

2a: 2^2 = 4

3a: 4^2 = 16

4a: 16^2 = 256
4b: 256*2 = 512 mod 101 = 7

5a: 7^2 = 49
5b: 49*2 = 98

6a: 98^2 = 9604 mod 101 = 9
6b: 9*2 = 18

7a: 18^2 = 324 mod 101 = 21
7b: 21*2 = 42

So, answer is 42

2. x = 3, e = 197, m = 101

Writing 197 in binary
197 = 11000101_b

1a: 3

2a: 3^2 = 9
2b: 9*3 = 27

3a: 27^2 = 729 mod 101 = 22
3b:

4a: 22^2 = 484 mod 101 = 80
4b:

5a: 80^2 = 6400 mod 101 = 37
5b:

6a: 37^2 = 1369 mod 101 = 56
6b: 56*3 = 168 mod 101 = 67

7a: 67^2 mod 101 = 45
7b:

8a: 45^2 mod 101 = 5
8b: 5*3 = 15

So, answer is 15

7.3. Encrypt and decrypt by means of the RSA algorithm with the following system parameters:
Only use a pocket calculator at this stage.

1. p = 3, q = 11, d = 7, x = 5

N = p*q = 3*11 = 33
Phi(N) = (p-1)(q-1) = 2*10 = 20

Because d*e = 1 mod phi(N), so e is inverse of d=7. So, e=3

So, y = x^e mod N = (5^3) mod 33 = 125 mod 33 = 26.
So, y = 26.

2. p=5, q=11, e=3, x=9

N = p*q = 5*11 = 55
Phi(N) = (p-1)(q-1) = 4*10 = 40

Because d*e = 1 mod phi(N), so d is inverse of e=3.

Writing EEA equations to calculate inverse of 3 in mod 40.
40 = 13*3 + 1
=> 1 = 40 - 13*3

So, the inverse of 3 in mod 40 is -13 ~= -13 + 40 = 27.
So, the inverse of 3 is 27. So, d is 27.

So, y = x^e mod N = (9^3) mod 55 = 729 mod 55 = 14.
So, y = 14.

7.5. In practice the short exponents e = 3, 17 and 2^16 + 1 are widely used.

1. Why can't we use these three short exponents as values for the exponent d in applications where we want to accelerate decryption?
Answer:
The public key e can be a short integer. The private key d needs to have the full length of the modulus. Hence, encryption can be significantly faster than decryption. Decryption process can be significantly slower than encryption. So that it's not easily brute forced.

2. Suggest a minimum bit length for the exponent d and explain your answer.
Answer:
Until recently, many RSA applications used a bit length of 1024 bits as default. Today it is believed that it might be possible to factor 1024-bit numbers within a period of about 10–15 years, and intelligence organizations might be capable of doing it possibly even earlier. Hence, it is recommended to choose RSA parameters in the range of 2048–4096 bits for long-term security.

7.11. In this exercise, you are asked to attack an RSA encrypted message. Imagine being the attacker: You obtain the ciphertext y = 1141 by eavesdropping on a certain connection. The public key is kpub = (n, e) = (2623, 2111).

1. Consider the encryption formula. All variables except the plaintext x are known. Why can't you simply solve the equation for x?
Answer:
In RSA, encryption equation for x is
Y = x^e mod n

Substituting y, e and n
1141 = x^2111 mod 2623

Except for brute force, there are no known algorithms to solve this equation for x.

2. In order to determine the private key d, you have to calculate d ≡ e−1 mod Φ(n). There is an efficient expression for calculating Φ(n). Can we use this formula here?
Answer:
The formula for calculating Φ(n) = (p-1)(q-1) presumes that we know the prime factorization of n, which we do not in this case. So, we cannot use this formula here.

3. Calculate the plaintext x by computing the private key d through factoring n = p · q. Does this approach remain suitable for numbers with a length of 1024 bit or more?
Answer:

Trying all prime numbers starting from 2, we get the n(=2623) can be factored into

N = 2623 = 43 * 61
So, p = 43
q = 61

So, Φ(n) = (43-1)(61-1) = 42*60 = 2520

Computing gcd of e and Φ(n)

= gcd(2111, 2520)
= gcd(2520%2111, 2111)
= gcd(409, 2111)
= gcd(2111%409, 409)
= gcd(66, 409)
= gcd(409%66, 66)
= gcd(13, 66)
= gcd(13, 66%13)
= gcd(13, 1)
= gcd(13%1, 1)
= gcd(0, 1)
= 1

So, gcd of n and e is 1. So, multiplicative inverse of e will exist

Writing equations for above

2520 = 1*2111 + 409
=> 409 = 2520 - 1*2111

2111 = 5*409 + 66
=> 66 = 2111 - 5*409
=> 66 = 2111 - 5*(2520 - 1*2111)
=> 66 = 6*2111 - 5*2520

409 = 6*66 + 13
=> 13 = 409 - 6*66
Substituting values of 409 and 66 from above
=> 13 = 2520 - 1*2111 - 6*(6*2111 - 5*2520)
=> 13 = 31*2520 - 37*2111

66 = 5*13 + 1
=> 1 = 66 - 5*13

Substituting values of 66 and 13 from above
=> 1 = 6*2111 - 5*2520 - 5*(31*2520 - 37*2111)
=> 1 = 191*2111 - 160*2520

So, multiplicative inverse of e(=2111) is 191
So, d = 191

Decryption equation for RSA is

X = y^d mod n
X = 1141^191 mod 2623
Writing 191 in binary = 10111111

Using square and multiply method

1a - 1141

2a: 1141^2 mod 2623 = 1301881 mod 2623 = 873

3a: 873^2 mod 2623 = 1459
3b: 1459*1141 mod 2623 = 1737

4a: 1737^2 mod 2623 = 719
4b: 719*1141 mod 2623 = 2003

5a: 2003^2 mod 2623 = 1442
5b: 1442*1141 mod 2623 = 701

6a: 701^2 mod 2623 = 900
6b: 900*1141 mod 2623 = 1307

7a: 1307^2 mod 2623 = 676
7b: 676*1141 mod 2623 = 154

8a: 154^2 mod 2623 = 109
8b: 109*1141 mod 2623 = 1088

So, x = 1088
