# RSA algorithm

RSA (Rivest-Shamir-Adleman, 1978) algorithm is an asymmetric encryption algorithm. To design an encryption/decryption key pair, two large prime numbers, p and q, , are selected, and an integer, d, is chosen that is relatively prime to (p-1)(q-1) (d and (p-1)(q-1) have no common factors other than 1). Finally, an integer e is computed such that



One key is (e,N), and the other is (d,N), where N=p\*q, and is referred to as the modulus.

For example, we might select p=7, and q=13. Then N=91, and (p-1)(q-1)=72. We can choose d=5 (which is relatively prime to 72) and e=29, because e\*d=145 and



Then, one key is K1=(29,91) and the other is K2=(5,91). The message to be encrypted is broken into blocks such that each block, M, can be treated as an integer between 0 and (N-1). To encrypt M into the ciphertext block, B, we perform



To decrypt B, we perform



The protocol works correctly because



More details about RSA algorithm can be found in the textbook by William Stallings, Cryptography and Network Security.

Returning to the example, assume M=2.

Then, to encrypt M, we compute



Thus, B=32. To decrypt B, we compute



which is the plaintext message M.

Obtaining of p and q is extremely difficult, hence, only knowing a secret key K2, receiver can correctly decrypt a message.

Find multiplicative inverse of d modulo fi(N)=(p-1)\*(q-1) by

EXTENDED EUCLID(m,b)

1. (A1,A2,A3):=(1,0,m); (B1,B2,B3):=(0,1,b);
2. if B3=0 return A3=gcd(m,b); no inverse
3. if B3=1 return B3 = gcd(m,b); B2= b-1 mod m
4. Q=
5. (T1,T2,T3):=(A1-QB1, A2-QB2, A3-QB3) //T=A-Q\*B
6. (A1,A2,A3):= (B1,B2,B3)
7. (B1,B2,B3):= (T1,T2,T3)
8. goto 2

In our example, d=5, fi(N)=72

A=(1,0,72), B=(0,1,5)

Q=floor(A3/B3)=floor(72/5)=floor(14.4)=14

T=A-Q\*B=(1-14\*0,0-14\*1, 72-14\*5)=(1,-14,2)

A=B==(0,1,5);

B=T=(1,-14,2);

B3 is not 0, nor 1

Q=floor(A3/B3)=floor(5/2)=2

T=A-Q\*B=(0-2\*1, 1-2\*(-14),5-2\*2)=(-2,29,1);

A=B==(1,-14,2);

B=T=(-2,29,1);

B3=1=>B2=5-1 mod 72 = 29=e

Check it: 5\*29=145=2\*72+1=1 mod 72

Encrypt M=5

C=M^e mod N = 5^29 mod 91

Use squaring for exponentiation and a\*b mod N = ((a mod N)\*(bmod N)) mod N

5^2 mod 91 =25

5^4 mod 91 = 25^2 mod 91 = 125\*5 mod 91 = 34\*5 mod 91 = 170 mod 91 = 79

5^8 mod 91 = 79\*79 mod 91 = (-12)\*(-12) mod 91 = 144 mod 91 = 53

5^16 mod 91 = 53\*53 mod 91 = 79

5^29 mod 91 = 5^16\*5^8\*5^4\*5 mod 91 = 79\*53\*79\*5 mod 91 = 53\*53\*5 mod 91 = 79\*5 mod 91 = 395 mod 91= 4\*91+31 mod 91 = 31 = C

Decryption:

M=C^d mod N = 31^5 mod 91

31^2 mod 91 = 51

31^4 mod 91 = 51\*51 mod 91 = 53

31^5 mod 91 = 31^4\*31 mod 91 = 53\*31 mod 91 = 5