# RSA algorithm

RSA (Rivest-Shamir-Adelman, 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.

For efficient exponentiation without calculators we use 1) binary decomposition of the power; 2) squaring; and 3) apply modulo reduction once a number is greater than N;

**Example of efficient encryption and decryption by RSA:**

Calculate 229 mod 91 to encrypt P=2.

1. : Binary decomposition of 29: 2910=111012=16+8+4+1. Hence, 2^29=2^(16+8+4+1)=2^16\*2^8\*2^4\*2
2. and 3): Squaring and modulo reduction: 2^2=4; 2^4=4^2 =16; 2^8=16^2=256 mod 91 = 74; 2^16=74\*74=74\*2\*37 = 148\*37 mod 91 = (148 mod 91)\*37 mod 91 = 57\*37 mod 91 = 19\*3\*37 mod 91 = 19\*111 mod 91 = 19\* (111 mod 91) mod 91 = 19\*20 mod 91 = 19\*5\*4 mod 91 = 95\*4 mod 91 = (95 mod 91)\*4 mod 91 = 4\*4 =16

Encryption: C=P^29 mod 91 = 2^29 mod 91=2^(16+8+4+1)=2^16\*2^8\*2^4\*2 = 16\*74\*16\*2 mod 91 = 16\*16\*74\*2 mod 91 = 74\*74\*2 mod 91 = 16\*2 mod 91 = 32

Decryption: P’=C^5 mod 91 =32^5 mod 91 = 32^(4+1) mod 91 = 32^4\*32 mod 91

Squaring: 32^2 = 32\*4\*8 mod 91 = 128\*8 mod 91 = (128 mod 91)\*8 mod 91 = 37\*8 mod 91 = 37\*4\*2 mod 91 = 148\*2 mod 91 = (148 mod 91)\*2 mod 91 = 57\*2 mod 91 = 114 mod 91 = 23

32^4 = 23^2 mod 91 = 529 mod 91 =5\*91 mod 91 = 74

32^5 mod 91 = 32^4\*32 mod 91 = 74\*32 mod 91 = 74\*2\*16 mod 91 = 148\*16 mod 91 = (148 mod 91)\*16 mod 91 = 57\*16 mod 91 = 57\*2\*8 mod 91 = 114\*8 mod 91 = (114 mod 91)\*8 mod 91 = 23\*8 mod 91 = 23\*4\*2 mod 91 = 92\*2 mod 91 = (92 mod 91)\*2 mod 91 = 1\*2 mod 91 = 2=P.

For efficient finding keys use Extended Euclid Algorithm (EAA):

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)
6. (A1,A2,A3):= (B1,B2,B3)
7. (B1,B2,B3):= (T1,T2,T3)
8. goto 2

**Example of finding keys;**

Let e=5, find its inverse d=e^(-1) mod (p-1)\*(q-1) = e^(-1) mod 6\*12 = e^(-1) mod 72 such that e\*d =1 mod 72

1. m=72, b=5
2. A=(A1, A2, A3)=(1,0, 72), B=(B1, B2, B3)=(0,1,5)
3. B3<>0, B3<>1
4. Q=floor(A3/B3)=floor(72/5)=14
5. T=(T1,T2,T3)=A-q\*B=(A1-q\*B1, A2-q\*B2, A3-q\*B3)=(1,-14,2)
6. A=(0,1,5); B=(1,-14,2)
7. B3<>0, B3<>1
8. Q=floor(A3/B3)=floor(5/2)=2
9. T=(T1,T2,T3)=A-q\*B=(A1-q\*B1, A2-q\*B2, A3-q\*B3)=(-2,29,1)
10. A=(1,-14,2), B=(-2, 29, 1)
11. B3=1=> b^(-1) mod m = 5^(-1) mod 72 = B2 =29

Check correctness of the inverse obtained: b\*b^(-1) mod m mod m = 5\*29 mod 72 = 145 mod 72 = 2\*72+1 mod 72 = 1. Result obtained is 1, hence, inverse is calculated correctly