# RSA algoritması

RSA (Rivest-Shamir-Adleman, 1978) algoritması asimetrik bir şifreleme algoritmasıdır. Bir şifreleme/şifre çözme anahtarı çifti tasarlamak için iki büyük asal sayı olan p ve q, , seçilir. Daha sonra, (p-1)(q-1) göreli olarak asal olan d seçilir, yani d ve (p-1) (q-1)'in 1'den başka ortak böleni yoktur. Son olarak, bir e tamsayısı şu şekilde hesaplanır:



Anahtarlardan biri (e,N) ve diğeri (d,N)'dir, burada N=p\*q ve modül olarak anılır.

Örneğin, p=7 ve q=13'ü seçebiliriz. O halde N=91 ve (p-1)(q-1)=72, e\*d=145 ve



O halde, bir anahtar K1 =(29,91) ve diğeri K2=(5,91) olur. Şifrelenecek mesaj, her blok M'nin 0 ile (N-1) arasında bir tamsayı olarak ele alınabileceği şekilde bloklara bölünür. M'yi şifreli metin bloğu B'ye şifrelemek için,



B'nin şifresini çözmek için



Protokol doğru çalışıyor çünkü



RSA algoritması hakkında daha fazla ayrıntı William Stallings, Cryptography and Network Security tarafından yazılan ders kitabında bulunabilir.

Örneğe dönersek, M=2 olduğunu varsayalım.

Ardından, M'yi şifrelemek için hesaplarız



Böylece, B=32. B'nin şifresini çözmek için hesaplıyoruz



düz metin mesajı olan M.

p ve q'nun elde edilmesi son derece zordur, bu nedenle, yalnızca gizli bir anahtarı bilen K2 alıcı bir mesajın şifresini doğru bir şekilde çözebilir.

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