

nov 23, 03 14:22

rsa.ki

Page 1/2

```

  *-----*
  /|      /|
  *-----*
  |*--|-*
  /|      /|
  *-----*

```

MuPAD 2.5.3 -- The Open Computer Algebra System

Copyright (c) 1997 - 2003 by SciFace Software
All rights reserved.

UNREGISTERED VERSION

Please contact info@sciface.com to register.

```

>> # ----- #
>> #           Az RSA-modszer bemutatasa MuPAD 2.5.3-mal #
>> #           Megyesi Laszlo: Bevezetes a szamelmeletbe jegyzete alapjan #
>> # (C) Kovacs Zoltan <kovzol@math.u-szeged.hu>, 2001/11/24, 2003/11/23 #
>> #           Ez a program szabadon felhasznalhato, barmilyen cellal #
>> # ----- #
>>
>> # Valasztunk ket primet Aladarnak. #
>> pa:=nextprime(673276231312):
>> qa:=nextprime(6173276231312):
>> print("Aladar ket primje: ".pa, ".qa);
>>
>>           "Aladar ket primje: 673276231319, 6173276231323"
>>
>> # Valasztunk ket primet Barbaranak. #
>> pb:=nextprime(3982192389239):
>> qb:=nextprime(382192389239):
>> print("Barbara ket primje: ".pb, ".qb);
>>
>>           "Barbara ket primje: 3982192389257, 382192389277"
>>
>> # Osszeszorozzuk a primeket, igy megkapjuk n-et. #
>> na:=pa*qa:
>> nb:=pb*qb:
>> print("Aladar n-je: ".na);
>>
>>           "Aladar n-je: 4156320155916308701405037"
>> print("Barbara n-je: ".nb);
>>
>>           "Barbara n-je: 1521963623810818056797189"
>>
>> # Latjuk, hogy a primtenyezokre bontas nehezebb falat... #
>> print("Aladar n-jenek primfelbontasa lassan megy:");
>>
>>           "Aladar n-jenek primfelbontasa lassan megy:"
>> factor(na);
>>
>>           673276231319 6173276231323
>>
>> # Egy megfelelo szamot valasztunk a-nak 1 es p-1 ill. q-1 kozott. #
>> aa:=0:
>> while gcd(aa,(pa-1)*(qa-1))<>1 do
>> & veletlena:=random(min(pa-1,qa-1)): aa:=veletlena(): end_while:
>> ab:=0:
>> while gcd(ab,(pb-1)*(qb-1))<>1 do
>> & veetlenb:=random(min(pb-1,qb-1)): ab:=veetlenb(): end_while:
>> print("Aladar a-ja: ".aa, Barbara a-ja: ".ab);
>>
>>           "Aladar a-ja: 474256143563, Barbara a-ja: 32062222085"
>>
>> # Megoldjuk az ax kongruens 1 (mod (p-1)(q-1)) kongruenciát #
>> xa:=numlib::lincongruence(aa,1,(pa-1)*(qa-1)):

```

nov 23, 03 14:22

rsa.ki

Page 2/2

```

>> xa:=xa[1]:
>> xb:=numlib::lincongruence(ab,1,(pb-1)*(qb-1)):
>> xb:=xb[1]:
>> print("Aladar x-e: ".xa.", Barbara x-e: ".xb);

"Aladar x-e: 2528600242632578368427855, Barbara x-e: 233138447687177398877\
645"

>>
>> # E S T E   N Y O L C K O R   T A L A L K O Z Z U N K   A   T O N A L   #
>> # 69838469327889797667757982328465766576757990908578753265328479786576 #
>> # \_____/ \_____/ \_____/ \_____/ #
>> # Az uzenet elso része (Aladar kuldi Barbaranak) #
>> uzenet:=69838469327889797:
>> print("Az elso uzenet: ".uzenet);

        "Az elso uzenet: 69838469327889797"

>> kodolt_uzenet:=powermod(uzenet,ab,nb):
>> print("A kodolt uzenet: ".kodolt_uzenet);

        "A kodolt uzenet: 1362893423060972922329105"

>>
>> # Ezt Barbara így tudja megfejteni: #
>> dekodolt_uzenet:=powermod(kodolt_uzenet,xb,nb):
>> print("Barbara ezt megfejtette: ".dekodolt_uzenet);

        "Barbara ezt megfejtette: 69838469327889797"

>>
>> quit

```