RSA kriptosistem

Dve veliki praštevili

V *Mathematici* za izračun n-tega praštevila uporabimo ukaz Prime.

```
?Prime
```

Prime[n] gives the n^{th} prime number. ≫

Radi bi poiskati dve primerljivo veliki praštevili.
Primerljivo veliki? Skoraj isto število binarnih/decimalnih mest.

```
p=Prime[10^9]
```

22 801 763 489

```
q=Prime[8*10^8]
```

18 054 236 957

Produkt praštevil p in q označimo z n.

```
n=p q
```

411 668 441 067 877 062 973

Eulerjeva funkcija

S phi oznaczimo Eulerjevo funkcijo števila n = p q.
Ker poznamo praštevilski razcep števila n je naloga otročje lahka.

```
phi=(p-1)(q-1)
```

411 668 441 027 021 062 528

Naše število je dovolj majhno, da zna njegovo Eulerjevo funkcijo izračunati tudi *Mathematica*.
To pomeni, da naši ključi v tem zgledu nikakor niso varni!!

```
EulerPhi[n]
```

411 668 441 027 021 062 528

Konstrukcija javnega in privatnega ključa

Izberimo si poljubno število d, manjše od phi, ki je TUJE phi.
Poskusimo s slučajnim številom.

```
?RandomInteger
```

RandomInteger[{i_{min}, i_{max}}] gives a pseudorandom integer in the range {i_{min}, …, i_{max}}.
RandomInteger[i_{max}] gives a pseudorandom integer in the range {0, …, i_{max}}.
RandomInteger[] pseudorandomly gives 0 or 1.
RandomInteger[*range*, n] gives a list of n pseudorandom integers.
RandomInteger[*range*, {n_1, n_2, …}] gives an $n_1 \times n_2 \times \ldots$ array of pseudorandom integers. ≫

```
d = RandomInteger[phi - 1]
```

49 549 405 303 832 841 569

```
GCD[d, phi]
```

1

Par (n,d) je Borutov privatni ključ.

Določimo naravno število e, ki reši diofansko enačbo:
e*d = 1 + k*phi

Z drugimi besedami, e*d je po modulu phi kongruenten 1.

Par (n,e) je Borutov javni ključ.

```
e=PowerMod[d,-1,phi]
```

396 702 186 635 970 141 473

```
Mod[e d, phi]
```

1

Zelo pomembno se je znebiti števila phi.

Ravno tako moramo paziti, da nihče ne more do privatnega ključa.

Prenos kriptiranih podatkov

Ančka bi rada Borutu poslala sporočilo.

```
sporocilo=12345678987654321
```

12 345 678 987 654 321

Sporočilo, ki ga Ančka počilja Borutu mora biti kratko. Manjše od n.
To ne predstavlja nobenega problema. Če je sporočilo daljše, ga lahko razseka na krajše dele.

Sporočilo Ančka zaklene z Borutovim javnim ključem.

Potencira ga na potenco e in določi ostanek pri deljenju z n.

zaklenjenoSporocilo=PowerMod[sporocilo,e,n]

373 251 538 431 623 327 490

Zaklenjeno sporočilo lahko pošlje Borutu po nezavarovanem kanalu.
Odklene ga lahko samo Borut.

Borut sporočilo odklene s svojim privatnim ključem.

Potencira ga na potenco d in določi ostanek pri deljenju z n.

odklenjenoSporocilo=PowerMod[zaklenjenoSporocilo,d,n]

12 345 678 987 654 321

sporocilo==odklenjenoSporocilo

True