

[RSA enosmerna fja s povratnimi vrati]

$G(1^\lambda)$: generiramo slučajni λ -bitni praštevilki p in q .
 $n := pq$. $\varphi(n) = (p-1)(q-1)$. Izberemo $e, d \in \mathbb{Z}_{\varphi(n)}^*$
 da $ed \equiv 1 \pmod{\varphi(n)}$.

$$sk := (n, d)$$

$$pk := (n, e)$$

$$F(pk, \cdot): \mathbb{Z}_n^* \rightarrow \mathbb{Z}_n^*$$

$$x \mapsto x^e \pmod{n}$$

$$I(sk, \cdot): \mathbb{Z}_n^* \rightarrow \mathbb{Z}_n$$

$$y \mapsto y^d \pmod{n}$$

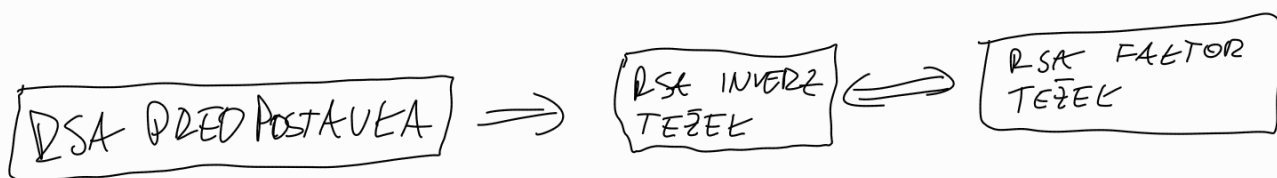
pravilnost: $I(sk, F(pk, x)) = (x^e \pmod{n})^d \pmod{n} =$
 $= x^{e \cdot d} = x^{1 + t \cdot \varphi(n)} = \underset{\parallel}{x^1},$ ker $x^{\varphi(n)} = x^{|\mathbb{Z}_n^*|} = 1$

ali je $F(pk, \cdot)$ enosmerna fja?

RSA predpostavka: za poljuben pol. alg. A

$$P(A(n, e, x^e) = x) \leq \epsilon_A \quad \text{za } p, q \leftarrow \lambda\text{-bitna}$$

praštevilka $n = pq$ in $x \leftarrow \mathbb{Z}_n^*$



• G, F, I polinomski.

$\rightarrow F$ in I : square and multiply $\Rightarrow O(\lambda^3)$

- $\rightarrow G$:
- (1) naključno izberemo p, q .
 - (2) izberemo e , da je tuje $\varphi(n)$
 - (3) $d = e^{-1} \pmod{\varphi(n)}$

izračun $e^{-1} \in \mathbb{Z}_q^*$: euclidov algoritem $O(\lambda)$

izbor prvteci dolžin λ -bitov p, q :
jeunfeno matfirna stevila do flec
ne najdemo prvtevila? kako to
bitvo preveriti?

izlet: let $\pi(x)$ stevilo prvtevil, manjših od x .

tedaj $\lim_{x \rightarrow \infty} \frac{\pi(x)}{x/\ln x} = 1$. Torej za $\lambda = 1024$ je

verjetnost, da je stevilo prvtevil 0,0014

→ ferretov verjetnostni test prvtevilosti
→ priče ... (glej slajde adfane etnik)

[Kriptosistem z javnim ključem]

Def: kriptosistem je simetričen, če je šifrirni ključ k
enak dešifrirnemu k' oz da $k \rightarrow k'$ v polinomske časne

Def: kriptosist. je asimetričen sistem.

Def: kriptosist. z javnim ključem je trojica algoritmov:

- $G(\lambda)$: naključnostni alg, ki vrne (sk, pk)

- $E(pk, m)$: -||- kriptogram c

- $D(sk, c)$: -||- m

veljati mora pravilnost: $D(sk, E(pk, m)) = m$

in varnost: semantična varnost, kot
pri simetričnih šifrah, le da napadalec pozna
tudi javni ključ.

Računski \Leftrightarrow cpa
varnost.