TKKPFMF2026-03-17

[RSA enosmerna fja s povratnimi vrati]

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

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

$F(pk, \cdot): \mathbb{Z}_n^* \to \mathbb{Z}_n^*$
$x \mapsto x^e \pmod n$

$I(sk, \cdot): \mathbb{Z}_n^* \to \mathbb{Z}_n$
$y \to y^d \pmod n$

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

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

RSA Predpostavka: za poljuben pol. alg. A
$P(A(n, e, x^e) = x) \leq \varepsilon_A$ za $p, q \leftarrow \lambda$-bitna praštevila $n = pq$ in $x \leftarrow \mathbb{Z}_n^*$

RSA PREDPOSTAVKA $\Rightarrow$ RSA INVERZ TEŽEK $\Leftrightarrow$ RSA FAKTOR TEŽEK

- G, F, I polinomski.

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

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

izračun e^{-1} v $\mathbb{Z}^*_{\varphi(n)}$: evklidov algoritem $O(\lambda)$

izbor praštevil dolžin λ-bitov p, q:
jemljemo naključna števila dokler
ne najdemo praštevila? kako to
hitro preveriti?

izrek: Let $\pi(x)$ število praštevil manjših od x.
Tedaj $\lim_{x \to \infty} \frac{\pi(x)}{x/\ln x} = 1$. Torej za $\lambda = 1024$ je
verjetnost, da je število praštevilo 0,0014

→ fermatov verjetnostni test praštevilskosti
→ prize ... (glej slajde ajšane šteti.k)

[Kriptosistem z javnim ključem]

Def: kriptosistem je simetričen, če je šifrirni ključ k
enak dešifrirnemu k' oz da $k \to k'$ v polinomskem času

Def: kriptosist. je asimetričen sicer.

Def: kriptosist. z javnim ključem je trojica algoritmov:

- $G(1^\lambda)$: naključnostni alg, ki vrne (sk, pk)
- $E(pk, m)$: —ıı— kriptogram c
- $D(sk, c)$: —ıı— 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.

Računska ⟺ cpa
varnost.