RSA kriptografija

Pavle Portić

2019-05-06

Vrste kriptografije

- Simetrična (AES, blowfish, etc.)
- Asimetrična (RSA, ECDSA, etc.)

RSA algoritam

Sastoji se iz četiri koraka:

1. Generisanje ključeva
2. Razmena ključeva
3. Enkripcija
4. Dekripcija

Generisanje ključeva

1. Izabrati dva prosta broja p i q
2. $n = p * q$ (veličina n, u bitima, je veličina ključa)
3. $l = nzs(p-1, q-1)$
4. Izabrati broj e, tako da je $1 < e < l$ i $nzd(e, l) = 1$
5. $d \equiv e^{-1} \bmod l$

Javni ključ čine brojevi n i e, a d privatni.

Razmena ključeva

A i B razmenjuju brojeve n i e, dok d drže za sebe.

Kanal slanja može biti javno dostupan, ali mora biti i pouzdan.

Enkripcija

1. Tekst se deli na segmente m, dužine jednakim dužine broja n
2. Svaki segment m se enkriptuje javnim ključem

$$c = m^e \bmod n$$

3. Segmenti se mogu spojiti sve dok je poznata duzina ključa

Dekripcija

1. Nad svakim segmentom c se primenjuje sledeca operacija privatnim ključem
$$m = c^d \bmod n$$
2. Segmenti m se zatim mogu rekonstruisati u izvornu poruku