Kako GPG funkcioniše

Cryptoparty Serbia

August 3, 2016

Contents

1 Šifrovanje i Dešifrovanje

Figure 1: Svako za sebe generiše svoje ključeve na svom računaru.
Tajni ključ čuva u tajnosti na sigurnom mestu, a Javni ključ pošalje na server javnih ključeva.

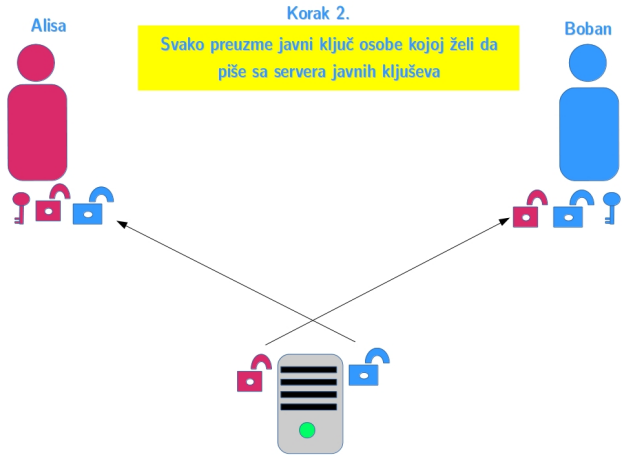

Figure 2: Svako sa servera javnih ključeva preuzme javni ključ osobe sa kojom želi razmenjivati šifrovane poruke.

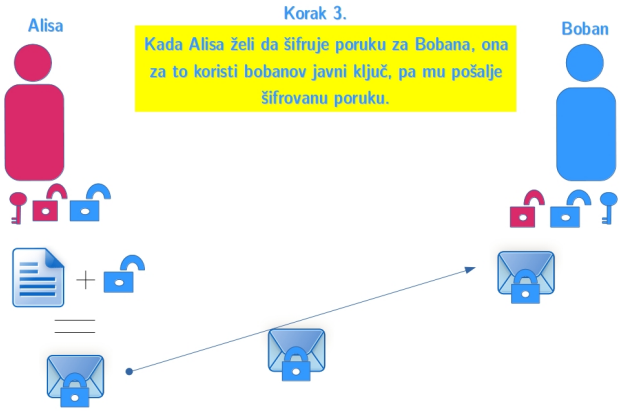

Figure 3: Kada Alisa napiše poruku, ona je šifruje Bobanovim javnim ključem, i pošalje je Bobanu.

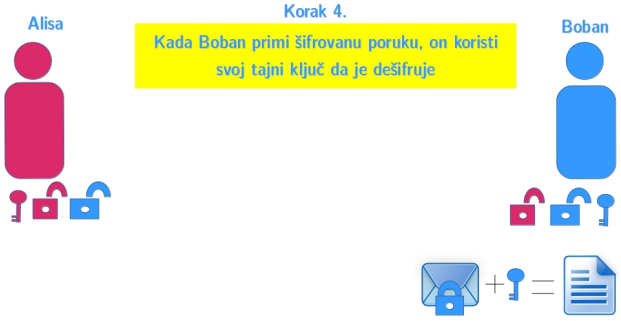

Figure 4: Boban primljenu poruku dešifrije svojim tajnim ključem.

1.1 Digitalno potpisivanje i provera autentičnosti

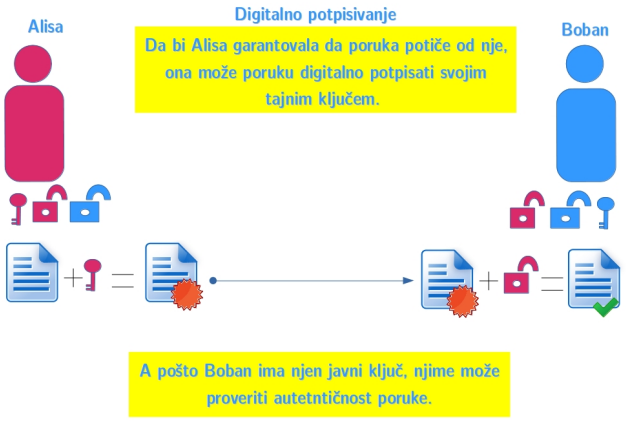

Figure 5: Digitalno potpisivanje je suprotan proces od šifrovanja. Alisa koristi svoj tajni ključ i njime širuje-potpisuje poruku. Svako ko ima njen javni ključ onda može proveriti da je poruku zaista ona napisala dešifrujući njenu poruku njenim javnim ključem.

1.2 Šifrovanje i digitalno potpisivanje

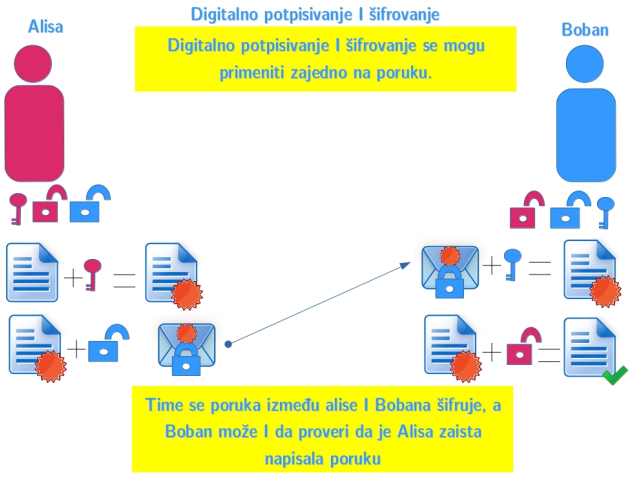

Figure 6: Šifrovanje i digitalno potpisivanje se može kombinovati kako bi se tajna poruka sigurno prenela primaocu, i kako bi primaoc mogao kad je dešifruje da se uveri da je pošiljalac zaista onaj koji to i tvrdi da jeste.

2 Kako GPG funkcioniše

Da bi na slikovit način bolje objasnili kako funkcioniše **GPG** koristićemo dva načina (jednostavnu matematiku i boje).

2.1 Boje

Prvi način je pomoću boja. Zamislite da se Alisa i Boban dogovore oko jedne boje, recimo žute. Zatim i Alisa i Boban izaberu svako za sebe svoju tajnu boju, Alisa izabere recimo crvenu, a Boban plavu. Potom i Alisa i Boban pomešaju žutu sa svojom tajnom bojom, Alisa žutu meša sa crvenom, a Boban žutu meša sa plavom. Tako Alisa dobija NARANDŽASTU (od crvene i žute), a Boban ZELENU (od plave i žute). Zatim i Alisa i Boban pošalju jedno drugom svoje nove mešavine boja, Alisa Bobanu pošalje narandžastu, a Boban Alisi zelenu.

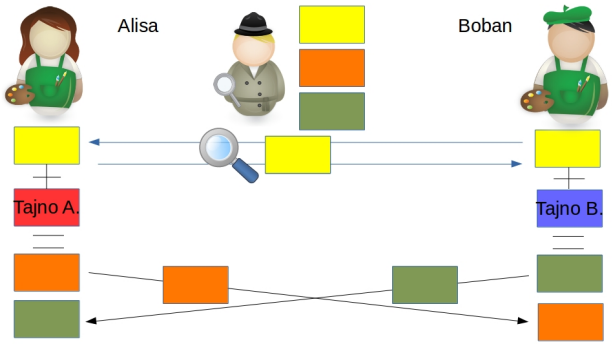

Figure 7: Alisa i boban mešaju javnu žutu sa svojim tajnim bojama, a potom razmenjuju novodobijene boje.

Kada Alisa i Boban razmene svoje mešavine boja svako na dobijenu tuđu mešavinu dodaje svoju tajnu boju i kombinuje je (meša) u novu boju. Na taj način Alisa dodaje svoju tajnu crvenu boju na zelenom, koju je dobila od Bobana, i dobija **braon** boju. Boban dodaje svoju tajnu plavu na narandžastu, koju je dobio od Alise, i dobija **braon** boju. Na taj način i Alisa i Boban su došli do tajne boje (textbfbraon), ne razmenjujući nikakve tajne preko javne mreže.

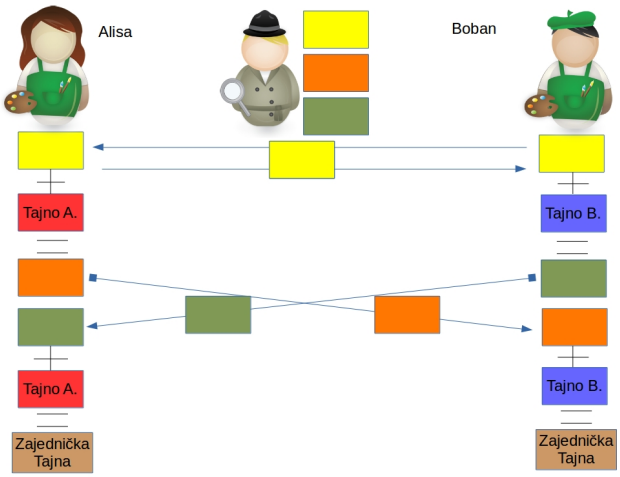

Figure 8: Alisa i boban mešaju svoje tajne boje sa razmenjenim mešavinama, i dobijaju istu tajnu **braon** boju.

2.2 Matematika

Ovde čemo opisati kako radi **RSA** algoritam izmišljen 1977. godine. Situacija je ista kao i do sada, imamo Alisu, Bobana, kao i treće lice Evu, koje prisluškuje sve informacije koje Alisa i Boban razmenjuju.
Prvi korak je da Alisa pronađe dva velika prosta broja p i q (prosti brojevi su deljivi samo sa samim sobom i sa jedinicom). U stvarnosti p i q su dužine stotinu cifara svaki, ali za potrebe ovog objašnjenja neka budu dosta manji. Na primer: $p = 17, q = 29$.
Zatim Alisa pomnoži ova dva broja da dobije novi broj N:
$N = p * q, N = 17 * 29 = 493$.
Broj N je jedan od dva broja koji čine javni ključ Alise. Drugi broj je e. Da bi dobila e, Alisa mora da uradi dve stvari, prva je da oduzme jedinicu i od p i od q i zatim da ih pomnoži i dobije novi broj Q
$(p-1) * (q-1) = 16 * 28 = 448$.
Zatim faktoriše Q=448 na činioce:
$448 = 2 * 2 * 2 * 2 * 2 * 2 * 7$
Sada e može biti bilo koji broj koji nije deljiv sa faktorima od 448, tj. nije deljiv ni sa 2 ni sa 7 u našem slučaju. Pa Alisa bira recimo broj 5. $e = 5$.
Sada alisa ima N i e koji čine njen javni ključ, dok su brojevi p i q njen tajni ključ. Sada Alisa može da objavi svoj javni ključ (pošalje ga na server javnih ključeva ili ga direkto pošalje Bobanu).
Kada Boban dobije Alisin javni ključ (N = 493 i e = 5), onda može da šifuje poruku za alisu koristeći brojeve iz javnog ključa. Prvo, ako je Bobanova poruka 42 koju obeležimo sa m, onda Boban mora da uradi dve stvari da bi svoju poruku šifrovao i poslao Alisi.
Prvo stepenuje svoju poruku sa brojem e: $m^e = 42^5 = 130691232$
Zatim treba da nadje ostatak pri deljenju dobijenog broja 130691232 sa N:
$130691232 \bmod 493 = 383$.
Sada je broj 383 šifrovana poruka koju Boban šalje Alisi.
Kada alisa dobije 383 od Bobana, da bi dešifrovala poruku mora da nadje novi broj d koji će joj pomoći u dešifrovanju. Prvo, Alisa traži umnožke brojeva e i Q, tako da je umnožak broja e tačno za jedan veći od umnožka broja Q:
Umnošci broja e=5 su: $5, 10, 15, 20, 25, 30, 35, 40, ..., 1345, ...$
a umnošci broja Q=448 su: $448, 896, 1344, 1792, 2240, 2688, ...$
Primetimo da je 269-i umnožak broja e 1345, tačno za jedan veći od trećeg umnožka broja Q 1344. Broj 269 je broj d koji smo tražili.
Sada Alaisa može da dešifruje poruku koristeći broj d i broj N, tako što Bobanovu šifrovanu poruku 383 stepenuje na d i traži ostatak pri deljenu tako dobijenog broja sa N:
$383^d \bmod N = 383^{269} \bmod 493 = 42$
Sigurnost RSA algoritma zasniva se na težini razbijanja velokog broja na dva prosta (problem diskretnog logaritma). Izvor: link