Sinadura DSA erabiliz

Egileak: Oier Barrutiabengoa eta Gaizka Cerezo
Data: 10/11/2024

Praktika hau 2 zatietan banatzen da, lehenengo zatian hainbat fitxategi ditugu karpeta batean, eta fitxategi horiek sinatuta daude DSA sistema erabiliz, beraz gure lehen eginkizuna sinadura hauek baliozkoak diren ala ez egiaztatzea da. Baita ere “public” fitxategian praktikan zehar erabiliko ditugun **p**, **q**, **alfa(α)** eta **beta(β)** aldagaiak aurkituko ditugu.

Hasteko, sinadurak dauden fitxategitik **r** eta **s** lortuko ditugu eta mezua hasheatuko dugu **h(x)** lortzeko, ondoren $\mathbf{s^{-1}}$ kalkulatu eta horrekin u_1 eta u_2 kalkulatu dezakegu $\mathbf{u_1=s^{-1} * h(x) \bmod q}$ eta $\mathbf{u_2=s^{-1} * r \bmod q}$ eginez. Bukatzeko, $\mathbf{v=(\alpha^{u1} * \beta^{u2} \bmod p) \bmod q}$ kalkulatuta, **v** eta **r** berdinak badira sinadura baliozkoa dela egiaztatuko dugu. Gure kasuan, lorem.png eta lorem.jpg fitxategien sinadurak ez ziren baliozkoak.

Praktikaren bigarrengo zatian sinaduraren gako pribatua lortu behar dugu, hori lortzeko, ikusi dugu txt fitxategien sinaduren lehenengo erdia berdina dela, zati hori **r** da. Hori jakinda **k** gako efimeroa kalkulatu dezakegu 2 sinadurak eta fitxategiak erabiliz, $\mathbf{k=(h(x_1) - h(x_2)) * (s_1 - s_2)^{-1} \bmod q}$ eginez. Bukatzeko, **k** jakinda eta $\mathbf{k=s^{-1}*(h(x) + d*r) \bmod q}$ dela jakinik, **d** kalkulatu dezakegu nun **d=6536 3352 7604 2500 3152 0881 0105 3177 6565 5483 7446 0673** gako pribatua den. Hau frogatzeko fitxategi bat sinatu dugu gako honekin gero gako publikoa erabiliz, praktikaren lehenengo zatian bezela, sinadura baliozkoa den frogatuz.