

Sinadura

Mikel Egaña Aranguren

mikel-egana-aranguren.github.io

mikel.egana@ehu.eus



Sinadura

<https://doi.org/10.5281/zenodo.4302267>

<https://github.com/mikel-egana-aranguren/EHU-ISSKS-31>



Sinadura digitala

Mirenek Ikerreri mezua bidaltzen dio, gako publikoko sistema erabiliz

Edonork ezin du irakurri Mirenen Ikerrentzako mezua, baina edozeinek bidali ahal du

Nola daki Ikerrek Mirenek bidali diola edo inork ez duela mezua aldatu?

Soluzioa: Mirenek mezua sinatzen du

Sinadura digitala

Erabiltzaile zilegiak soilik sinatu ahal du bere dokumentua

Inork ezin du sinadura faltsutu

Edozeinek balioztatu ahal du sinadura digitala

Sinadura digitala

Ezin da sinadura bat berrerabili

Ezin da sinadura bat aldatu

Ezin da dokumentu bat sinatu izana ukatu

Ezin da dokumentu bat aldatu sinatu ostean

Kautotzea, Osotasuna eta Zapuztezintasuna

Sinadura digitala

Mirenek mezuaren laburpen kriptografikoa lortzen du: $RC = \text{hash}(m)$

Mirenek bere klabearekin zifratzen du laburpen kriptografikoa: $\text{Sinadura} = e(RC, M_{\text{pri}})$

Mirenek bere mezua (Zifratua edo zifratu gabe) eta bere sinadura bidaltzen ditu

Sinadura digitala



criptosistema clave privada

Sinadura digitala

Ikerrek sinadura deszifratzen du Mirenen gako publikoa erabiliz: $RC = (\text{Sinadura}, M_{pu})$

Ikerrek mezuaren laburpen kriptografikoa lortzen du: $RC' = \text{hash}(m)$

Ikerrek RC' eta RC alderatzen ditu ezer aldatu ez dela baieztatzeko

Sinadura digitala



criptosistema clave privada

Sinadura digitala

Sinatzeaz gain, Mirenek mezua zifratzen badu, Ikerrek bakarrik irakurriko du:

Konfidentzialtasuna, Osotasuna, Kautotzea, Zapuztezintasuna

Hurrengoak erabiltzea dauka:

- Kriptografia asimetrikoa
- Kriptografia hibridoa

Sinadura digitala

Kriptografia asimetrikoa. Ikerreri bidali:

- Mezu zifratuaren kriptograma (M_{pri} eta I_{pu} -rekin zifratua)
- Bere sinadura digitala (Laburpen kriptografikoa, M_{pri} -rekin zifratua)

Sinadura digitala

Kriptografia hibridoa. Ikerreri bidali:

- Saio gakoarekin zifratutako mezuaren kriptograma
- Saio gako zifratuaren kriptograma, I_{pu} -rekin zifratua
- Bere Sinadura digitala (Laburpen kriptografikoa, M_{pri} -rekin zifratua)