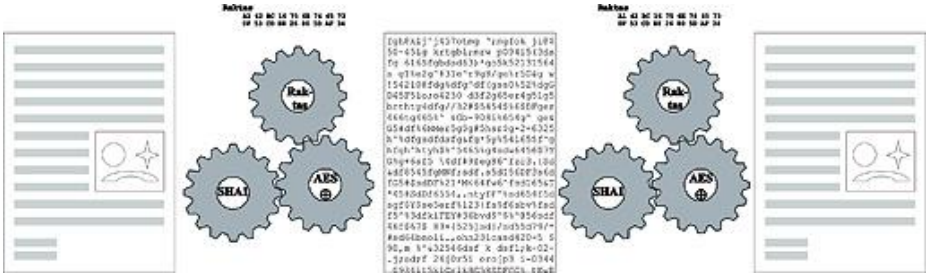
Duomenų šifravimas

Autoriai

- Doc. E. Sakalauskas,
- T. Burba,
- K. Lukšys,
- dokt. A. Katvickis,
- P. Vitkus



Duomenų šifravimo sistema leidžia šifruoti įvairius duomenis tiek su sertifikuotais, komercinės paskirties algoritmais (pvz., AES), tiek ir su įvairiais unikaliais algoritmais (pvz. pseudo atsitiktinis skaičių generatorius ir suma moduliu du (Å)), siekiant papildomai apsaugoti. Siūloma lanksti sistema, kurią galima naudoti įvairiems duomenų failams arba įvairiems duomenų bazės įrašams šifruoti. Šifravimo raktai gali būti paremti slaptažodžiais arba galima naudoti ilgus šifravimo raktus, saugomus įvairiose raktų laikmenose. Siūloma šifravimo sistema gali būti sujungta su elektroninio parašo sistema, taip būtų užtikrintas papildomas saugumas, t. y., užšifruoti duomenys papildomai pasirašomi (pvz., naudojant standartinę maišos funkciją SHA-1 ir RSA e. parašo schemą).

Paskirtis

Duomenų šifravimo sistema gali būti naudojama tiek duomenų byloms, tiek atskiriems duomenų bazės įrašams šifruoti. Ji taikoma ir asmeniniams, ir visiškai slaptiems duomenims apsaugoti nuo nesankcionuoto panaudojimo.

Baigtumo lygis

Vykdant Lietuvos Valstybinio mokslo ir studijų fondo bei LR Krašto apsaugos ministerijos finansuojamą projektą „Nacionalinės duomenų bylų šifravimo sistemos sukūrimas“, paruošta demonstracinė šifravimo programa.

Privalumai

Siūloma lanksti sistema, kurią galima naudoti tiek atskirai, tiek integruoti į jau esančius produktus. Unikalūs (slapti) šifravimo algoritmai papildomai apsaugos duomenis. Šiuos algoritmus taip pat galima naudoti kartu su sertifikuotais algoritmais.

Kontaktai

KTU Inovacijų skyrius
Tel.: (8 37) 30 06 92, 30 09 69
El. p. inis@ktu.lt