Sirli Põder ja Elisabeth Suits

Ülesanne 1

Räsimine:

1. Kirjuta selgitus räsimise (hashing) kontseptsioonist-põhiidee ja eesmärk.
   V: Räsimine on krüptograafiline protsess, kus sisendandmete töötlemisel luuakse kindla pikkusega räsiväärtus. Räsimise põhiidee on unikaalsus, kuna iga väiksema muudatuse korral sisendis muutub räsi täielikult. Räsimise rakendamine on kiire ja tõhus, sõltumata sisendi suurusest. Räsi on alati fikseeritud pikkusega ja ühesuunaline funktsioon. Räsimise eesmärgiks on andmete kaitse, paroolide turvalisus, digitaalne allkiri ja unikaalsete identifikaatorite loomine.

2. Kirjelda hea räsifunktsiooni omadusi ja selgita, miks need on olulised.
   V: Hea räsifunktsiooni omadused mitmesugustes krüptograafilistes rakendustes ja turvalisuse tagamiseks digitaalses maailmas. Hea räsifunktsioon peab olema ühesuunaline, ta peaks kiiresti arvutama ja peaks genereerima unikaalseid kombinatsioone. On kindla pikkusega ja hästi vastupidav. Need omadused on olulised, et tagada andmete turvalisus, autentimine ja terviklus paljudes krüptograafilistes ja turvalisusega seotud rakendustes.

3. Selgita kokku põrgete lahendamise tehnikaid, eriti eraldi aheldamist (separate chaining) ja avatud aadressimist (open addressing).
   V: Kokkupõrgete tekkega tegelemine on oluline osa räsifunktsioonide rakendamisel. Kokkupõrge toimub siis, kui kaks erinevat sisendit loovad sama räsi. Eraldi aheldamise põhimõte on iga räsiväärtuse jaoks, kus hoitakse eraldi andmestruktuuri, kuhu salvestatakse kõik kokkupõrget põhjustatavad sisendid. See toimib nii, et kui toimub kokkupõrge, siis uus sisend lisatakse vastavasse andmestruktuuri. Selle meetodi eeliseks on lihtsus ja efektiivne kasutus. Avatud aadressimise põhimõte on peale igat kokkupõrget leida järgmine vaba koht põhihoidlas. See toimib nii, kui tekib kokkupõrge siis algoritm jätkab ikka uute vabade kohtade otsimist. Selle meetodi eelised on mälu hea kasutamine ja see on parema jõudlusega kui eelmine meetod.