Parengė ITMM Artūras Šakalys

Konspektas

Simetrinis kodavimas yra kriptografinis metodas, kuriame vienas raktas naudojamas tiek žinomajai, tiek ir koduojamai informacijai užšifruoti bei atšifruoti. Tai reiškia, kad tie patys raktai yra naudojami tiek kodavimui, tiek atkodavimui. Naudojamas raktas turi būti saugus, kad nebūtų galima dekoduoti informacijos neautorizuotiems asmenims.

Asimetrinis kodavimas (arba viešųjų raktų kriptografija) yra kriptografinis metodas, kuriame naudojami atskiri raktai kodavimui ir atkodavimui. Viešas raktas naudojamas informacijai užšifruoti, o privatus raktas naudojamas užšifruotos informacijos atkoduoti. Šis metodas yra saugesnis nei simetrinis kodavimas, nes privatus raktas nėra dalijamas su kitais asmenimis.

Kriptografinės sistemos yra išorės atgarsinimo priemonės, leidžiančios užšifruoti ir atkoduoti duomenis. Jos naudojamos užtikrinti, kad informacija būtų saugiai perduodama ir kad tik autorizuoti asmenys galėtų ją skaityti. Kriptografinės sistemos yra naudojamos tiek viešose, tiek privačiose komunikacijose, taip pat verslo aplinkoje ir kitose srityse, kur reikalinga duomenų saugumas.

Duomenų kodavimas yra procesas, kuriuo duomenys arba informacija konvertuojami iš vienos formos į kitą, kad būtų galima jų naudotis arba saugoti. Tai yra būdas, kaip informacija yra pateikta kompiuteriui arba kitaip tvarkoma.

Skaičiavimo sistemos yra būdas, kaip skaičiai yra pateikti ir naudojami skaičiuoti arba atlikti matematinius veiksmus. Dažniausiai naudojamos skaičiavimo sistemos yra dvejetainė (2 pagrindu), aštuonainė (8 pagrindu), dešimtainė (10 pagrindu) ir šešioliktainė (16 pagrindu). Kiekviena skaičiavimo sistema turi savo taisykles ir naudojimo metodus, tačiau dvejetainė sistema yra daugiausiai naudojama kompiuterijos srityje.