Šifravimo būdai

Šifravimo būdai

Šifravimo metodai yra būdai, kaip užkoduoti informaciją taip, kad tik tie, kurie turi teisingą raktą arba slaptąjį algoritmą, gali ją atšifruoti ir perskaityti. Šifravimas yra naudojamas užtikrinti duomenų konfidencialumą ir apsaugoti juos nuo nepageidaujamų asmenų

Šifravimo būdai

Simetrinis šifravimas. Simetrinis šifravimas yra būdas, kai tiek šifravimui, tiek atšifravimui naudojamas tas pats raktas. Tai reiškia, kad abiem pusėms, norinčioms saugoti slaptumą, turi būti žinomas tas pats raktas. Populiariausias simetrinio šifravimo algoritmas yra AES (Advanced Encryption Standard).

Šifravimo būdai

Asimetrinis šifravimas. Asimetrinis šifravimas naudoja du raktus: viešąjį ir privačiąjį. Viešas raktas naudojamas užšifruoti duomenis, o privatus raktas reikalingas atšifruoti juos. Viešas raktas gali būti dalinamas su bet kuo, bet tik turėtojas žino privataus rakto. Tai naudojama daugelyje interneto komunikacijos formų. Populiarus asimetrinio šifravimo algoritmas yra RSA.

Šifravimo būdai

Hachingo funkcijos. Hachingo funkcijos yra naudojamos ne duomenims šifruoti, bet vietoje to generuoti fiksuoto ilgio hachų reikšmę pagal pradinius duomenis. Šios hachai dažnai naudojami slaptažodžių saugumui, duomenų tikrinimui integritetui, ir kitoms užduotims, kuriose svarbu unikalumas. Pvz., SHA-256 yra populiari hachingo funkcija.

Šifravimo būdai

Simboliniai šifrai: Simboliniai šifrai keičia simbolius (raides, skaičius ar kitus simbolius) pagal tam tikrą taisyklių rinkinį. Pavyzdžiui, Cezario šifras keičia raides nurodytu kiekiu pozicijų šone abėcėlėje.

Šifravimo būdai

Kvantiniai šifrai: Kvantiniai šifrai yra pažangi šifravimo forma, paremta kvantinio kompiuterio teorija. Šie šifrai naudoja kvantines mechanikos principus duomenų apsaugai. Jie gali būti atsparūs tradicinių kompiuterių bandymams atšifruoti informaciją.

Šifravimo būdai

Kiekvienas šifravimo metodas turi savo privalumų ir trūkumų, ir tinkamiausią pasirinkimą lemia kontekstas ir saugumo reikalavimai. Šifruoti duomenys gali būti atšifruoti tik tada, jei turite tinkamą raktą arba žinote atitinkamą algoritmą, todėl raktų valdymas yra esminis šifravimo proceso aspektas.

Šifravimo būdai

Symmetric vs Asymmetric Encryption – What is the Difference?

https://www.youtube.com/watch?v=nRou-J4YN4Y

Asymmetric Encryption - Simply explained

https://www.youtube.com/watch?v=AQDCe585Lnc

Symmetric Encryption VS Asymmetric Encryption

https://www.youtube.com/watch?v=ydKgb0IOMhQ