Parengė IMM Artūras Šakalys, 2025 m.

Duomenų šifravimas

Projektinė užduotis: Pažink kriptografiją per dirbtinio intelekto žvilgsnį

Tikslas:

Savarankiškai išnagrinėti kelias kriptografijos temas, naudojantis dirbtiniu intelektu ir skaitmeniniais įrankiais, pateikti kūrybiškai parengtą Word dokumentą.

✓ Užduoties eiga ir reikalavimai:

1. temos

Pasirink **vieną arba dvi** iš šių temų:

- Kriptografijos sąvoka ir istorija
- Simetrinis ir asimetrinis šifravimas
- Viešasis ir privatusis raktas, sertifikatai
- Šifravimo algoritmai ir jų pavyzdžiai (pvz., AES, RSA)
- Istoriniai šifrai (pvz., Cezario, Skytale, Perstatų)
- Hibridinė kriptografija
- Kriptografijos taikymas šiuolaikinėse technologijose
- Kriptografija finansų sektoriuje
- Praktinis šifravimas su „Kleopatra“

2. Naudok dirbtinį intelektą kūrybiškai

Pasitelk dirbtinį intelektą (pvz. ChatGPT, Copilot, Claude ir kt.), bet:

- **Nurodyk, kokį aiškinimo stilių** parinko DI (pvz., dokumentinis, istorinis, romano, pasakojimo, humoristinis ir pan.)
- **Kritiniu žvilgsniu** įvertink atsakymą: ar stilius tinkamas? Ar informacija išsami?

- **Papildyk DI atsakymą** kita informacija: terminų apibrėžimais, pavyzdžiais, istoriniais faktais ar savo komentarais.

3. Papildyk medžiagą vizualais ir šaltiniais

Įterpk bent:

- **1 lentelę** (pvz., palyginimas tarp simetrinio/asimetrinio šifravimo)
- **1 diagramą ar schemą** (pvz., kaip veikia šifravimo procesas)
- **1 paveikslėlį, žemėlapį ar istorinį šaltinį** (pvz., Skytale lazdelė, Enigma mašina)
- **1–2 nuorodas į patikimus išorinius šaltinius** (pvz., Britannica, OWASP, NIST, Europos kibernetinio saugumo portalai)

4. Sutvarkyk Word dokumentą pagal reikalavimus

Turi būti:

- Titulinis lapas su vardu, pavarde, tema, data
- Antraštės ir poraštės (su puslapių numeracija)
- Turinys (automatinis, naudojant „Heading“ stilius)
- Naudotas **stiliaus ir dizaino formatavimas**: antraštės, sąrašai, paryškinimai
- Pateikta informacija logiškai, dalimis, aiškiai
- Prieduose pateikti DI generuoti fragmentai ir tavo komentarai jiems

📤 Pateikimas:

- Failas pateikiamas MS Word formatu (.docx)
- Pavadinimas: Kriptografija_TavoVardasPavarde.docx
- Terminas: [nurodo mokytojas]
- Failas pateikiamas per TAMO, el. dienyną arba el. paštą.

Parengė IMM Artūras Šakalys, 2025 m.

🔍 Vertinimo kriterijai (iki 10 balų):

Vertinimo sritis	Taškai
Turinys atitinka temą ir tikslą	2
DI atsakymų analizė ir stiliaus įvertinimas	2
Paveikslai, lentelės, schemos, nuorodos	2
Teksto išdėstymas ir dokumento struktūra	2
Kūrybiškumas, savarankiškumas, pastabos apie DI	2

Informacija, kuria reikia aiškinti, surasti, papildyti

Kriptografija – informacijos apsaugos mokslas

Kriptografijos sąvoka

Kriptografija – tai mokslas apie informacijos šifravimą, siekiant ją apsaugoti nuo neteisėto prieigos, užtikrinant slaptumą, autentiškumą, integralumą ir neiginamumą. Ši sritis yra esminė šiuolaikinių saugumo sistemų dalis.

Atsiradimo ir vystymosi istorija

Kriptografijos ištakos siekia senovės civilizacijas: Egiptą, Graikiją, Romą. Pavyzdžiui, Cezario šifras buvo naudojamas Romos imperijoje. Viduramžiais buvo sukurta daug rankinių šifravimo sistemų. XX a. kriptografija smarkiai pažengė į priekį dėl karo poreikių (pvz., Enigma), o vėliau – dėl kompiuterių.

Kriptografinės sistemos

Kriptografinės sistemos – tai algoritmų, protokolų ir raktų rinkiniai, naudojami duomenims užšifruoti ir iššifruoti.

Viešasis ir privatusis raktas

Viešasis raktas yra skelbiamas viešai, o privatusis laikomas paslaptyje. Naudojami asimetrinėje kriptografijoje – ką užšifruoja vienas, gali iššifruoti tik kitas.

Simetrinis ir asimetrinis šifravimas

Simetrinis šifravimas naudoja tą patį raktą tiek šifravimui, tiek iššifravimui. Asimetrinis – naudoja du skirtingus raktus: viešąjį ir privatųjį.

Parengė IMM Artūras Šakalys, 2025 m.

Sertifikato sąvoka

Sertifikatas patvirtina, kad viešasis raktas priklauso konkrečiam naudotojui. Jį išduoda sertifikavimo centrai, pvz., Let's Encrypt, DigiCert.

Kriptografinių sistemų pavyzdžiai

RSA, AES, ECC, PGP – tai populiarios kriptografinės sistemos, plačiai naudojamos interneto saugumui užtikrinti.

Šifravimo algoritmas

Tai nuoseklių veiksmų rinkinys, kurio pagalba tekstas paverčiamas nesuprantama simbolių seka. Pvz., AES, Blowfish.

Iššifravimo (dešifravimo) algoritmas

Veiksmų seka, leidžianti iššifruoti užšifruotą informaciją, grąžinant ją į pradinę formą.

Hibridinė kriptografija

Tai sistemų tipas, kuriame kombinuojami simetriniai ir asimetriniai metodai – asimetrinis naudojamas raktų perdavimui, simetrinis – duomenų šifravimui.

Kriptografinės sistemos moderniose technologijose

Kriptografija naudojama HTTPS ryšiuose, el. parašuose, VPN tinkluose, duomenų bazėse, autentifikacijoje.

Šifravimas nenaudojant kompiuterių

Istoriniai metodai: Cezario šifras (raidžių paslinkimas), Skytale (pergamento apvyniojimas), Knyginis šifras (naudojant konkrečią knygą), Perstatų šifras (raidžių eiliškumo keitimas).

Šifravimas naudojant kompiuterius

Populiariausias simetrinis algoritmas – AES. Taip pat naudojami RSA (asimetrinis), SHA (maišos funkcijos), ECC (elipsinių kreivių kriptografija).

Tinklų saugumas

Duomenų šifravimas užtikrina, kad trečiosios šalys negalėtų matyti siunčiamų duomenų. Naudojamas VPN, SSL/TLS.

Finansų sektorius

Kriptografija apsaugo bankinius duomenis, internetinius mokėjimus, kriptovaliutas, autentifikavimo sistemas.

Praktika: Šifravimo įrankiai

Mokiniai gali naudotis įrankiu „Kleopatra“ (iš Gpg4win paketo) šifruoti ir dešifruoti pranešimus viešojo/privataus rakto pagalba.