DUOMENŲ TYRYBA IR INFORMACIJOS SAUGA: KRIPTOGRAFIJA

VARDAS, PAVARDĖ: _____

KLASĖ: _____

DATA: _____

ĮVADAS

Šiame skyriuje kuri asmeninį teorijos vadovėlio skyrių apie kriptografiją. Užduotys padės pasiruošti egzaminui: apibrėši pagrindines sąvokas, palyginsi sistemas ir paaiškinsi jų taikymą realiose situacijose.

1. SKYRIAUS TEMA

Įrašyk skyriaus temą pilnu sakiniu:

_____

2. PAGRINDINĖS ŠIO SKYRIAUS SĄVOKOS

Instrukcija: Prie kiekvienos sąvokos parašyk apibrėžimą 1–2 sakiniais, vartodamas tikslius informatikos terminus.

Kriptografija –

_____

Kriptografinė sistema –

_____

Šifravimas –

_____

Simetrinis šifravimas –

_____

Asimetrinis šifravimas –

_____

Viešasis raktas –

_____

Privatusis raktas –

_____

Skaitmeninis sertifikatas –

_____

Sertifikavimo institucija (CA) –

_____

OpenPGP –

_____

Duomenų vientisumas –

_____

3. PAAIŠKINIMAS SAVO ŽODŽIAIS (RIŠLUS TEKSTAS)

Instrukcija: Parašyk 6–8 sakinius, kuriuose paaiškintum, kas yra kriptografija, kuo skiriasi simetrinis ir asimetrinis šifravimas, ir kodėl reikalingi viešieji bei privatūs raktai.

_____

_____

_____

_____

4. LYGINIMAS

Instrukcija: Palygink šiuos tris dalykus: 1) simetrinį šifravimą, 2) asimetrinį šifravimą, 3) jų naudojimo paskirtį.

_____

_____

_____

5. KRIPTOGRAFINIŲ SISTEMŲ TAIKYMAS

Instrukcija: Atsakyk pilnais sakiniais.

Kam naudojama OpenPGP sistema?

_____

Kodėl el. pašto šifravimui svarbus viešasis raktas?

_____

6. SERTIFIKATŲ PATIKIMUMAS

Instrukcija: Išvardyk ir paaiškink tris sertifikato patikimumo požymius.

1. _____

2. _____

3. _____

7. SVARBIAUSIA INFORMACIJA PRIEŠ EGZAMINĄ

Instrukcija: Užrašyk tris svarbiausius faktus, kuriuos privalai prisiminti.

1. _____

2. _____

3. _____

8. SAVĘS ĮSIVERTINIMAS

☐Suprantu, kas yra kriptografija ir kam ji naudojama

☐Moku paaiškinti simetrinio ir asimetrinio šifravimo skirtumus

☐Žinau, kas yra viešasis raktas, privatusis raktas ir sertifikatas