2024 metų informacijos kodavimo ir kriptografijos kurso egzamino užduotys

Egzamino užduotį sudarys 4 užduotys iš šio sąrašo: po vieną iš keturių skyrių. Vienos užduoties vertė – 1 balas. Sėkmės!

Šaltinio informacijos kodavimas

1. Pagal duotas tikimybes sudaryti Shannono kodą.

2. Pagal duotas tikimybes sudaryti Huffmano kodą.

3. Turint tikimybių lentelę apskaičiuoti dydžių besąlygines ir sąlygines entropijas.

4. Koduoti simbolių eilutę LZ77 kodu.

5. Koduoti simbolių eilutę LZ78 kodu.

Klaidas taisantys kodai

1. Ištaisyti klaidą stačiakampio kodo žodyje.

2. Ištaisyti klaidą trikampio kodo žodyje.

3. Ištaisyti klaidą Hammingo kodo žodyje.

4. Sudaryti IBM kodo žodį, kai duoti informaciniai simboliai.

Klasikinė kriptografija

1. Iššifruoti perstatų šifrą.

2. Iššifruoti Cezario, Vigenere šifrų pavyzdžius.

3. Iššifruoti Enigma šifrą, kai duota abėcėlė, rotorių keitiniai, raktas.

4. Iššifruoti šifrą, sudarytą naudojant Feistelio schemą.

Šiuolaikinė kriptografija

1. Sudaryti kuprinės kriptosistemą.

2. Iššifruoti kuprinės šifrą.

3. Sudaryti RSA kriptosistemą, užšifruoti žinutę arba sukurti skaitmeninį parašą.

4. Sudaryti ElGamalio kriptosistemą (skaitmeninio parašo schemą), užšifruoti žinutę arba sudaryti skaitmeninį parašą.

5. Padalyti paslaptį pagal schemą su slenksčiu arba atkurti paslaptį.