Informacijos kodavimo ir kriptografijos algoritmų egzamino užduotys

Informacijos teorija

1. Šaltinis perduoda simbolius su tikimybėms $P = [0.02, 0.05, 0.07, 0.08, 0.1, 0.68]$. Sudarykite šaltiniui dvejetainį Shannono kodą. Apskaičiuokite vidutinį kodo žodžių ilgį.

1.1. Šaltinis perduoda simbolius su tikimybėms P=[0.03, 0.04, 0.07, 0.09, 0.17, 0.6]. Sudarykite šaltiniui dvejetainį Huffmano kodą. Apskaičiuokite vidutinį kodo žodžių ilgį.

1.2. Lentelėje duotos atsitiktinių dydžių X, Y reikšmių tikimybės $P(X = x, Y = y)$:

P(X=x,Y=y)	a	b	c	d
a	0.02	0.03	0.04	0.05
b	0.05	0.06	0.07	0.07
c	0.08	0.09	0.09	0.35

Apskaičiuokite entropijas $H(X,Y), H(X), H(Y), H(X|Y), H(Y|X)$.

1.3. Sudarykite teksto AAADBDAACAACAAD LZ77 kodą, su m=5 ilgio žodynu. Atkurkite tekstą iš LZ77 kodo su m=5 ilgio žodynu: [[0, 0, 'B'], [1, 1, 'A'], [3, 3, 'C'], [3, 2, 'B'], [0, 0, 'D'], [4, 1, 'C'], [4, 1, 'B']].

1.4. Sudarykite teksto AACAAABCCAAAADA LZ78 kodą ir žodyną. Atkurkite tekstą ir žodyną iš LZ78 kodo: [[4, 'B'], [1, 'D'], [1, 'A'], [6, 'A'], [1, 'B'], [6, 'B'], [1, '*']].

Klaidas taisantys kodai

2.1. Dvejetainio Hammingo kodo žodžiai $x_1x_2\ldots x_{10}$; kontroliniai simboliai sudaromi iš informacinių pagal lygybes:

$$\begin{aligned} x_1 &= 1\cdot x_3 + 1\cdot x_5 + 0\cdot x_6 + 1\cdot x_7 + 1\cdot x_9 + 0\cdot x_{10}, \\ x_2 &= 1\cdot x_3 + 0\cdot x_5 + 1\cdot x_6 + 1\cdot x_7 + 0\cdot x_9 + 1\cdot x_{10}, \\ x_4 &= 0\cdot x_3 + 1\cdot x_5 + 1\cdot x_6 + 1\cdot x_7 + 0\cdot x_9 + 0\cdot x_{10}, \\ x_8 &= 0\cdot x_3 + 0\cdot x_5 + 0\cdot x_6 + 0\cdot x_7 + 1\cdot x_9 + 1\cdot x_{10}. \end{aligned}$$

Iš kanalo gautas žodis d=1101001011 Ištaisykite įvykusią vieną perdavimo klaidą.

2.2. Sudarykite žodžio 583747 IBM kodo kontrolinį simbolį.

Simetrinių raktų kriptografija

3.1. Iššifruokite perstatų šifrą, jei raktas=VANDUO,
abėcėlė=AĄBCČDEĘĖFGHIĮYJKLMNOPRSŠTUŲŪVZŽ.
Šifras:
EKEIA USSAŠ SPNNG USNRP MSALY
VDRŽL IKAIŲ ASYRŲ ULUEM ATAID
EPIAT LIŲUŠ IIAEA ŽPĖUS UVRČS
JPKAA ŲALŽT IAAIN VORUE AŠORN
KPIN.S UKKRM ŽAJLK SĖAII ĘAILU
PIĖTŲ ŲI

3.2 Iššifruokite Vigenere šifrą, jei raktas=TIKRAS,
o abėcėlė=AĄBCČDEĘĖFGHIĮYJKLMNOPRSŠTUŲŪVZŽ
Šifras:
ĮLGER SDZKP AKŽBI H

3.3 Feistelio struktūros šifras šifruoja 8 bitų ilgio blokus. Funkcija

$$f(x_1x_2x_3x_4, k_1k_2k_3k_4) = y_1y_2y_3y_4$$

apibrėžiama taip: $y_1 = x_4 \oplus k_1, y_2 = x_3 \oplus k_2, y_3 = x_2 \oplus k_3, y_4 = x_1 \oplus k_4$. Šifrą sudaro dvi iteracijos su tuo pačiu raktu k=0100 Užšifruokite bloką 10000010

Viešojo rakto kriptografija

4.1. Naudodamiesi sparčiai didėjančia svorių sistema

$$w = [27, 729, 19683, 531441, 14348907]$$

sudarykite viešą kuprinės kriptosistemą ir šifruokite žinutę 10011.

4.2. Pasirinkite pirminius skaičius, sudarykite RSA raktus, užšifruokite žinutę $m = 10982$. Sudarykite šios žinutės RSA skaitmeninį parašą.

4.3. Skaičius $p = 20000107$ yra pirminis, $g = 3$ yra generuojantis $\mathbb{Z}_p^*$ elementas. Sudarykite ElGamalio kriptosistemos raktus ir užšifruokite žinutę $m = 66637$.

4.4. Skaičius $p = 20000107$ yra pirminis, $g = 3$ yra generuojantis $\mathbb{Z}_p^*$ elementas. Sudarykite ElGamalio kriptosistemos raktus ir pasirašykite žinutę $m = 97273$.