Міністерство освіти і науки України

Національний технічний університет України

«Київський політехнічний інститут імені Ігоря Сікорського»

Фізико-технічний інститут

**КРИПТОГРАФІЯ**

**КОМП ’ЮТЕРНИЙ ПРАКТИКУМ №4**

Виконали:

студент 3 курсу ФТІ

Група ФБ-74

Брікс Олексій

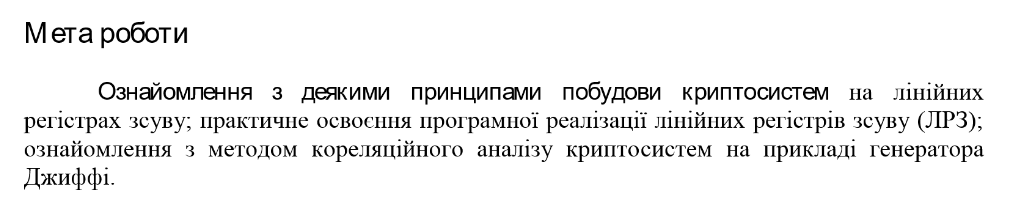
Сорбот Володимир

Перевiрили::

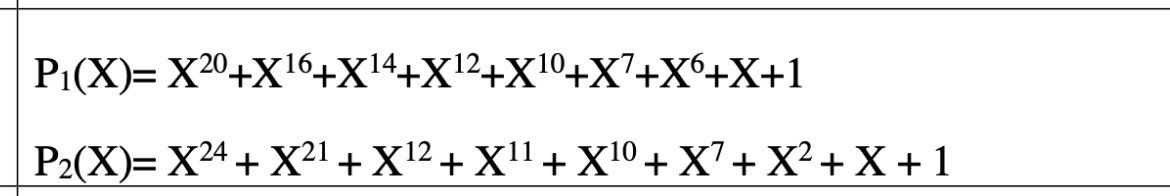
Завадська Л. О.

Савчук М. М.

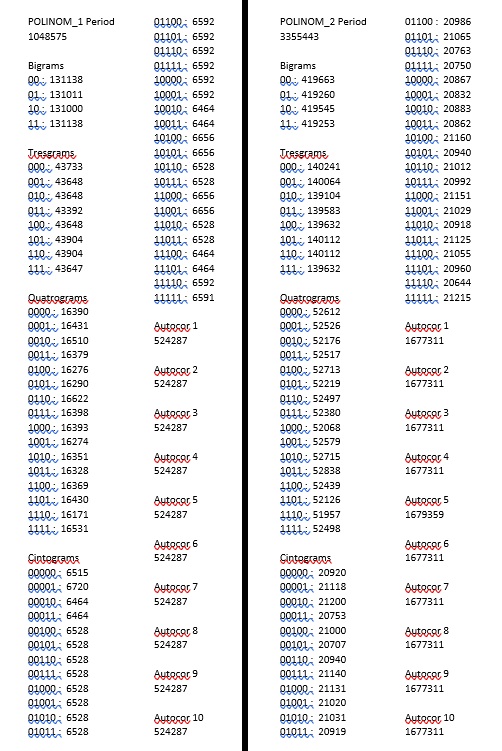
Чорний О. М.



Поліном з варіанту



Результати



Код програми

bigram = {"00":0, "01":0, "10":0, "11":0}

tresgram = {"000":0, "001":0, "010":0, "011":0, "100":0, "101":0, "110":0, "111":0}

quatrogram = {"0000":0, "0001":0, "0010":0, "0011":0, "0100":0, "0101":0, "0110":0, "0111":0, "1000":0, "1001":0, "1010":0, "1011":0, "1100":0, "1101":0, "1110":0, "1111":0}

cintogram = {"00000":0, "00001":0, "00010":0, "00011":0, "00100":0, "00101":0, "00110":0, "00111":0, "01000":0, "01001":0, "01010":0, "01011":0, "01100":0, "01101":0, "01110":0, "01111":0, "10000":0, "10001":0, "10010":0, "10011":0, "10100":0, "10101":0, "10110":0, "10111":0, "11000":0, "11001":0, "11010":0, "11011":0, "11100":0, "11101":0, "11110":0, "11111":0}

period = '0'

p1 = [1,1,0,0,0,0,1,1,0,0,1,0,1,0,1,0,1,0,0,0] #polinom 1

imp1 = [0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1] #impulse polinom 1

imp1\_1 = [0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,0] #1 step for cicle

p2 = (1,1,1,0,0,0,0,1,0,0,1,1,1,0,0,0,0,0,0,0,0,1,0,0) #polinom 2

imp2 = (0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1) #impulse polinom 2

imp2\_1 = (0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,0) #1 step for cicle

l = len(imp1\_1)

l1 = l-1

temp = []

for counter in range(0, l):

a = imp1\_1[counter]

temp.append(a)

while( temp != imp1 ):

sum\_array = []

for counter in range(0, l1):

a = p1[counter] \* temp[counter]

sum\_array.append(a)

b = (sum(sum\_array)) % 2

temp.append(b)

period = period + str(temp[0])

del temp[0]

#if (len(period) < 10):

# print(imp1)

# print(temp)

print('\nPOLINOM 1 \n \n')

print('\nPeriod \n')

print(len(period))

################### bigram

print('\nBigrams \n')

temp\_bigram = ""

for counter in range(0, (len(period)-1)):

temp\_bigram = temp\_bigram + period[counter]

if (len(temp\_bigram) == 2):

bigram[temp\_bigram]+=1

temp\_bigram = ''

for key in bigram:

print(key, ': ', bigram[key])

################## tresgram

print('\nTresgrams \n')

temp\_tresgram = ""

for counter in range(0, (len(period)-1)):

temp\_tresgram = temp\_tresgram + period[counter]

if (len(temp\_tresgram) == 3):

tresgram[temp\_tresgram]+=1

temp\_tresgram = ''

for key in tresgram:

print(key, ': ', tresgram[key])

################### quatrogram

print('\nQuatrograms \n')

temp\_quatrogram = ""

for counter in range(0, (len(period)-1)):

temp\_quatrogram = temp\_quatrogram + period[counter]

if (len(temp\_quatrogram) == 4):

quatrogram[temp\_quatrogram]+=1

temp\_quatrogram = ''

for key in quatrogram:

print(key, ': ', quatrogram[key])

################### cintogram

print('\nCintograms \n')

temp\_cintogram = ""

for counter in range(0, (len(period)-1)):

temp\_cintogram = temp\_cintogram + period[counter]

if (len(temp\_cintogram) == 5):

cintogram[temp\_cintogram]+=1

temp\_cintogram = ''

for key in cintogram:

print(key, ': ', cintogram[key])

###############################

print('\nAutocor 1 \n')

autocor1arr = []

tempPeriod = period

for counter in range(0, 0):

tempPeriod = tempPeriod + period[counter]

for counter in range(0, (len(period) - 1)):

a = (int(tempPeriod[counter]) + int(tempPeriod[counter + 1])) % 2

counter += 1

autocor1arr.append(a)

print(sum(autocor1arr))

###############################

print('\nAutocor 2 \n')

autocor2arr = []

temp2Period = period

for counter in range(0, 1):

temp2Period = temp2Period + period[counter]

for counter in range(0, (len(period) - 1)):

a = (int(temp2Period[counter]) + int(temp2Period[counter + 2])) % 2

counter += 1

autocor2arr.append(a)

print(sum(autocor2arr))

###############################

print('\nAutocor 3 \n')

autocor3arr = []

temp3Period = period

for counter in range(0, 2):

temp3Period = temp3Period + period[counter]

for counter in range(0, (len(period) - 1)):

a = (int(temp3Period[counter]) + int(temp3Period[counter + 3])) % 2

counter += 1

autocor3arr.append(a)

print(sum(autocor3arr))

###############################

print('\nAutocor 4 \n')

autocor4arr = []

tempPeriod = period

for counter in range(0, 3):

tempPeriod = tempPeriod + period[counter]

for counter in range(0, (len(period) - 1)):

a = (int(tempPeriod[counter]) + int(tempPeriod[counter + 4])) % 2

counter += 1

autocor4arr.append(a)

print(sum(autocor4arr))

###############################

print('\nAutocor 5 \n')

autocor5arr = []

tempPeriod = period

for counter in range(0, 4):

tempPeriod = tempPeriod + period[counter]

for counter in range(0, (len(period) - 1)):

a = (int(tempPeriod[counter]) + int(tempPeriod[counter + 5])) % 2

counter += 1

autocor5arr.append(a)

print(sum(autocor5arr))

###############################

print('\nAutocor 6 \n')

autocor6arr = []

tempPeriod = period

for counter in range(0, 5):

tempPeriod = tempPeriod + period[counter]

for counter in range(0, (len(period) - 1)):

a = (int(tempPeriod[counter]) + int(tempPeriod[counter + 6])) % 2

counter += 1

autocor6arr.append(a)

print(sum(autocor6arr))

###############################

print('\nAutocor 7 \n')

autocor7arr = []

tempPeriod = period

for counter in range(0, 6):

tempPeriod = tempPeriod + period[counter]

for counter in range(0, (len(period) - 1)):

a = (int(tempPeriod[counter]) + int(tempPeriod[counter + 7])) % 2

counter += 1

autocor7arr.append(a)

print(sum(autocor7arr))

###############################

print('\nAutocor 8 \n')

autocor8arr = []

tempPeriod = period

for counter in range(0, 7):

tempPeriod = tempPeriod + period[counter]

for counter in range(0, (len(period) - 1)):

a = (int(tempPeriod[counter]) + int(tempPeriod[counter + 8])) % 2

counter += 1

autocor8arr.append(a)

print(sum(autocor8arr))

###############################

print('\nAutocor 9 \n')

autocor9arr = []

tempPeriod = period

for counter in range(0, 8):

tempPeriod = tempPeriod + period[counter]

for counter in range(0, (len(period) - 1)):

a = (int(tempPeriod[counter]) + int(tempPeriod[counter + 9])) % 2

counter += 1

autocor9arr.append(a)

print(sum(autocor9arr))

###############################

print('\nAutocor 10 \n')

autocor10arr = []

tempPeriod = period

for counter in range(0, 9):

tempPeriod = tempPeriod + period[counter]

for counter in range(0, (len(period) - 1)):

a = (int(tempPeriod[counter]) + int(tempPeriod[counter + 10])) % 2

counter += 1

autocor10arr.append(a)

print(sum(autocor10arr))