Протокол лабораторної роботи №3

Криптоаналіз афінної біграмної підстановки

Варіант №7

Виконав

Студент 3 курсу

Групи ФБ-13

Короткевич Іван

**Мета роботи:** Набуття навичок частотного аналізу на прикладі розкриття моноалфавітної підстановки; опанування прийомами роботи в модулярній арифметиці.

Використовуючи код з минулих лабораторних робіт, підрахуємо частосту біграм у шифротексті:

цл:0.014362151506617854

ял:0.01379892987890735

ае:0.012109264995775838

ле:0.011827654181920586

чо:0.01098282174035483

щб:0.010701210926499578

юэ:0.010419600112644326

юе:0.010419600112644326

за:0.010419600112644326

лл:0.010137989298789073

сф:0.010137989298789073

жл:0.009856378484933821

ул:0.009856378484933821

ьй:0.009574767671078569

еб:0.009293156857223317

вл:0.009293156857223317

об:0.009293156857223317

ьт:0.009011546043368065

ьа:0.009011546043368065

фю:0.009011546043368065

эб:0.009011546043368065

щл:0.008729935229512813

шц:0.008729935229512813

оц:0.008729935229512813

фй:0.007885102787947058

вь:0.007885102787947058

Функції для знаходження НСД та оберненого елемента:

def egcd(a, b):

if a == 0:

return b, 0, 1

else:

gcd, x, y = egcd(b % a, a)

return gcd, y - (b // a) \* x, x

def inverse\_elem(a, m):

gcd, x, y = egcd(a, m)

if gcd != 1:

return None

else:

return x % m

Функція для розв’язання лінійних конгруенцій:

def congruence(a, b, n):

d, x, y = egcd(a, n)

all\_x = []

if d == 1:

x = (inverse\_elem(a, n) \* b) % n

all\_x.append(x)

else:

if b % d != 0:

return None

else:

a1 = a // d

b1 = b // d

n1 = n // d

x0 = (inverse\_elem(a1, n1) \* b1) % n1

for i in range(d):

x = x0 + i \* n1

all\_x.append(x)

return all\_x

Використовуючи вище наведені функції та формули з методичних вказівок можна знайти кандидати на ключі:

keys = []

for i in range(0, 5):

for j in range(0, 5):

for k in range(0, 5):

for l in range(0, 5):

X1\_X2 = (bigrams\_lang[i] - bigrams\_lang[k]) % m\*\*2

Y1\_Y2 = (bigrams\_text[j] - bigrams\_text[l]) % m\*\*2

inverse = inverse\_elem(X1\_X2, m\*\*2)

if inverse is not None:

a = (inverse \* Y1\_Y2) % m\*\*2

b = (bigrams\_text[j] - a\*bigrams\_lang[i]) % m\*\*2

pair = [a, b]

keys.append(pair)

Далі розшифровуємо шифротекст кожним ключем-кандидатом:

for pair in unique\_keys:

decrypted\_text = ""

a = pair[0]

b = pair[1]

for i in range(0, len(text) - 1, 2):

bigram = text[i:i + 2]

if inverse\_elem(a, m\*\*2) is not None:

#X = (inverse \* (bigram\_number(bigram[0], bigram[1]) - b)) % m\*\*2

X = congruence(a, (bigram\_number(bigram[0], bigram[1]) - b) % m\*\*2, m\*\*2)

if X[0] is None:

continue

decrypted\_text += number\_to\_bigram(X[0])

if check\_text(decrypted\_text) == True:

file\_output.write(f"Key ({a}, {b}): ")

file\_output.write(decrypted\_text)

file\_output.write("\n")

Отримаємо для ключа (200, 900):  
атызнаешьсколькоразмывэтомгодуиграливбейсболавпрошломавпозапрошломнистогониссегоспросилтомгубыегодвигалисьбыстробыстроявсезаписалтысячпятьсотшестьдесятвосемьразасколькоразячистилзубызадесятьлетжизнишестьтысячразарукимылпятнадцатьтысячразспалчетыреслишнимтысячиразиэтотольконочьюиселшестьсотперсиковивосемьсотяблокагрушвсегодвестиянеоченьтолюблюгрушичтохочешьспросиуменявсезаписаноесливспомнитьисосчитатьчтояделалзавседесятьлетпрямотысячимиллионовполучаютсявотвотдумалдугласопятьоноближепочемупотомучтотомболтаетноразведеловтомеонвсетрещититрещитсполнымртомотецсидитмолчанасторожилсякакрысьатомвсеболтаетникакнеугомонитсяшипитипенитсякаксифонссодовойкнигяпрочелчетыресташтуккиносмотрелитогобольшесорокфильмовсучастиембакаджонсатридцатьсджекомхоксисорокпятьстомоммиксомтридцатьдевятьсхутомгибсономстодевяностодвамультипликационныхпрокотафеликсадесятьсдугласомфербенксомвосемьразвиделпризраквопереслономчаничетыреразасмотрелмилтонасиллсадажеодинпролюбовьсадольфомменжутолькоятогдапросиделцелыхдевяносточасоввкиношнойуборнойвсеждалчтобэтаерундакончиласьипустиликошкуиканарейкуилилетучуюмышьаужтутвсецеплялисьдругзадружкуивизжалидвачасабезпередышкииселзаэтовремячетыресталеденцовтристатянучексемьсотстаканчиковмороженоготомболталещедолгоминутпятьпокаотецнепрервалегоасколькоягодтысего