

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**  
**СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ**  
Кафедра кібербезпеки

**Дисципліна “Системи та засоби криптоаналізу”**

**Звіт до лабораторної роботи № 4**

на тему “ Дослідження криптоаналітичних атак на афінний шифр. Частина 2”

Студент	Борщ Д.О.
Варіант	№ 1
Група	КБ-01
Перевірила	Лаврик Т.В

**Суми 2022**

## ЗВІТ

Написати програмний код методу частотного аналізу для:

1. (10 б.) визначення ключа, яким зашифровано текст.

```
import sys
import math
import json
import random

alphabet = [
    'а', 'б', 'в', 'г', 'ґ', 'д', 'е', 'є', 'ж', 'з', 'и', 'і', 'ї', 'й',
    'к', 'л', 'м', 'н', 'о', 'п', 'р', 'с', 'т', 'у', 'ф', 'х', 'ц', 'ч',
    'ш', 'щ', 'ь', 'ю', 'я', ' '
]

def encrypt(string, keyA, keyB):
    output = ""
    for i in string:
        index = (keyA*alphabet.index(i) + keyB) % len(alphabet)
        output += alphabet[index]

    return output

def decrypt(string, keyA, keyB):
    output = ""
    for i in string:
        index = pow(keyA, -1, len(alphabet))*(alphabet.index(i) - keyB) %
len(alphabet)
        output += alphabet[index]

    return output

def hack(string):
    lettersFreq = {}
    for letter in string:
        try: lettersFreq[letter] += 1
        except: lettersFreq[letter] = 1

    print(f"Number of each letter: {json.dumps(lettersFreq, indent=1,
ensure_ascii=False)}")
```

```

# Finding max values
max1 = max(lettersFreq, key=lettersFreq.get)
max2 = max1
while max2 == max1: max2 = random.choice(list(lettersFreq))
for letter in lettersFreq:
    if (
        lettersFreq[letter] > lettersFreq[max2]
        and lettersFreq[letter] < lettersFreq[max1]
    ): max2 = letter

Yletters = (max1, max2)

print(f"Most frequent letters: {Yletters}")

#creating key-value pairs
XY1 = (' ', Yletters[0])
XY2 = ('o', Yletters[1])

pair1 = (
    (alphabet.index(XY1[0]) - alphabet.index(XY2[0])) % len(alphabet),
    (alphabet.index(XY1[1]) - alphabet.index(XY2[1])) % len(alphabet)
)

print(f"XY differences:\n\t-Open text: {pair1[0]}\n\t-Closed text: {pair1[1]}")

# Finding A and B
print(f"Open text  $XY^{-1} \pmod{\text{len}(\text{alphabet})}$ : {pow(pair1[0], -1, len(alphabet))}")
keyA = (pow(pair1[0], -1, len(alphabet)) * pair1[1]) % len(alphabet)
keyB = (alphabet.index(XY1[1]) - keyA * alphabet.index(XY1[0])) % len(alphabet)

print(f"Found key A: {keyA}\n Found key B: {keyB}")

print(f"Trying to decrypt...")
print(f"Decrypted text is:\n{decrypt(string, keyA, keyB)}")

def main(args=sys.argv):
    # Using file as input source
    if "--file" in args:
        try:
            fileName = args[args.index("--file")+1]
        except:
            print("ERROR, no file specified!")
            return 0
        try:
            f = open(fileName, "r")
            inputText = ''.join(f.read())
        except:
            print("ERROR, can't open file!")
            return 0

    # Using plain text as input source
    else:
        inputText = input("Enter input text: ")

```

```

# Taking key from args
try:
    keyA = int(args[args.index("--key")+1])
    keyB = int(args[args.index("--key")+2])
    if 0 > keyA > len(alphabet) or 0 > keyB > len(alphabet) or
math.gcd(keyA, len(alphabet)) != 1:
        print("ERROR, wrong key specified!")
        return 0
except:
    if "--hack" not in args:
        print("ERROR, no key specified!")
        return 0
    else: pass

print(f"Input text:\n{inputText}\n")

# Choosing an option
if "--encrypt" in args:
    print(f"Encrypted text is:\n{encrypt(inputText, keyA, keyB)}")
if "--decrypt" in args:
    print(f"Decrypted text is:\n{decrypt(inputText, keyA, keyB)}")
if "--hack" in args:
    print("Trying to hack chipher...\n")
    hack(inputText)

return 0

if __name__ == "__main__":
    main()

```

## 2. (5 б.) розшифрування шифротексту за допомогою визначеного ключа.

Перевірити отримані ключі на правильність.

Скріншоти з результатами роботи програми (мінімум 3 різні шифротексти)

```
1 2 3 4 5 6 dmytro@thonkpad: ~/Study/SZK/Lab_4 | xonsh
рили вздовж потьомкінських сходів так званий живий ланцюг амбітні плани орг
анізаторів повністю виправдалися він сягнувтаки берега моря простягаючись в
ілою ниткою від педесталу пам'ятника рішельє ланцюг із року в рік ставав усе
довшим а разом із цим зростало й усвідомлення одеси як українського міста
зростало настільки що в році незважаючи на невинну зливу для участі в акц
ії вишиванковий ланцюг вишикувалася півторатисячна черга утворивши нескінче
нне живе море вишиванок подальші два роки запам'яталися встановленням нових
рекордів адже кількість учасників збільшилася вдвічі до речі дик де рішельє
також долучається до цієї події четвертий рік поспіль святковий гардероб г
ерцога поповнюється найрізноманітнішими вишиванками ооооо блакитносиній і я
скравочервоний жовтогарячий і ніжнозелений ось палітра його вишитих візерун
ків уже вдєсате майорить приморський бульвар синьожовтими барвами і вже вко
тре ми збираємось у самому серці одеси щоб помилуватися показом автентичног
о вбрання написати диктант просто неба концентруючи нашу енергію й демонстр
уючи всім як свою єдність так і свою любов до рідного міста та своєї країни

Encrypted text is:
мшдвнткрбнегенбувбмзчб гтсеаехкрбхбзвг увпбнхкпбмчзчоуеаькбзмьжпмеууьб
юуьбуанейвіушзкчблжгеуьтбмчйчббвзъктьчкуршбчзкшгччбмтнтмеужмшсшбфзкзмт
йхбгшн шдемзьеовбкшмчбжшйтбзчоювзъкбмьмкрбйхювблгіеуьтцблбмтнтмеужтбпкш
гтйбмншшмІб шкршожчуржтцбзшшчбкбжбнмеутгбїтмгбїеуахсбеоічкучб Іеутбшгс
еучнекшгчмб шмучзхкбмт гемейтзъбмчубзъсуплкежтбївгасебошгб гшзкъсехдтзрбї
чйшхбуткжшбмчббб сьвзкейпб еоькутжебгчивірсейуахсбчнбгшлбмбгчжбзкемблзвб
бюшмитобеггеншобчнбатобнгшзкейшбгблзмчшойеууьбшовзтъбьжлбжгеуьзржшсшбчзкеб
нгшзкейшбуезкчйржтблшбмбгшгшачбуанмеїехдтбуебуви туупбнйтпбнйьблпдзкчбмбеж
чябмтнтмеужшмтгбїеуахсбмтнтжпмейзъб чмкшгектзъдубдгасебпкшгтмтбвзжчууда
ууьбїтмвбошгбмтнтмеужшб швейрчбмнебгшкбне еоькейтзъбмзкеушшйууьбшчштцб
гвжшгчмбейівбжчйрмчзкрблпдзутжчмбнічїритийезъбмжмчдчбкшбгдчбнхжбмвбгчивіре
бкежшїбюшлпдеекрзъбшбачеяб шючябдвкмвгктгбгчжб шз чїрбзмьжшмтгбсегнвгшїбс
вгашсеб ш шмукєкрзъбуеггчнушоуеучкуцитобтнтмеужеотбшшшшбїежткшзтучгбчбь
зжгемшдвгшутгбїшмкшсегдтгбчбчбчїушнвейутгбшзрб ейчкгебгшсшбмтнтткцбмчнвгпг
жмботбнїтггесшзрблбзеошпбзвгачбшовзтблшїб шотїлпментзъб шженшобемквуктдушс
шмбїеууьбуе тзектбтжжеукб гшзкшбувіебжшувукгпхдтбуйепбвуьгсчбгбнвошзукг
пхдтбмзчобъжбзмшхбєнуучзкрбкежбчзбзмхбїхїшмбюшбгчнушшбшбчзкебкебзмшєябжгеут
dmytro@thonkpad ~/Study/SZK/Lab_4 main $

"ж": 44,
"й": 37,
"ї": 12,
"я": 9,
"и": 15,
"ф": 1,
"г": 16,
"і": 14,
"ш": 5,
"е": 9,
"л": 2
Most frequent letters: ('г', 'ш')
Found key A: 5
Found key B: 6
Trying to decrypt...
Decrypted text is:
вочевидь зараз не всі пригадають що серпневу дату вісімнадцате святкування
дня незалежності України відлік десятилітньої історії вишиванкового фестива
лю розпочався саме тоді коли сімдесят дев'ять людей убраних у вишиванки утво
рили вздовж потьомкінських сходів так званий живий ланцюг амбітні плани орг
анізаторів повністю виправдалися він сягнувтаки берега моря простягаючись в
ілою ниткою від педесталу пам'ятника рішельє ланцюг із року в рік ставав усе
довшим а разом із цим зростало й усвідомлення одеси як українського міста
зростало настільки що в році незважаючи на невинну зливу для участі в акц
ії вишиванковий ланцюг вишикувалася півторатисячна черга утворивши нескінче
нне живе море вишиванок подальші два роки запам'яталися встановленням нових
рекордів адже кількість учасників збільшилася вдвічі до речі дик де рішельє
також долучається до цієї події четвертий рік поспіль святковий гардероб г
ерцога поповнюється найрізноманітнішими вишиванками ооооо блакитносиній і я
скравочервоний жовтогарячий і ніжнозелений ось палітра його вишитих візерун
ків уже вдєсате майорить приморський бульвар синьожовтими барвами і вже вко
тре ми збираємось у самому серці одеси щоб помилуватися показом автентичног
о вбрання написати диктант просто неба концентруючи нашу енергію й демонстр
уючи всім як свою єдність так і свою любов до рідного міста та своєї країни
dmytro@thonkpad ~/Study/SZK/Lab_4 main $
```

Рис. 1 — Перший приклад з ключами 5 та 6.

```
1 2 3 4 5 6 7 8 9 10 dmytro@thonkpad: ~/Study/SZK/Lab_4 | xonsh  LW (55%) 95% 27% 65% 29% (0.91) 59°C 99% 5 Dec 2022 12:15:48

"q": 40,
"p": 62,
"y": 23,
"щ": 73,
"i": 16,
"д": 55,
"й": 20,
"п": 15,
"г": 9,
"е": 27,
"н": 24,
"я": 6,
"ф": 23,
"x": 2,
"с": 7,
"r": 2
}
Most frequent letters: ('6', 'e')
XY differences:
-Open text: 15
-Closed text: 29
Open text XY^-1(mod len(alphabet)): 25
Found key A: 11
Found key B: 12
Trying to decrypt...
Decrypted text is:
шедевром козацької архітектури бо рівного за красою й урочистістю не було зпосеред храмів у всій Україні вважають собор у нинішнім новомосковську запорізькому місті самарі цей дивовижний дерев'яний витвір збудував народний майстер яким погребняк замовляючи йому будівлю козаки просили спорудити її без цяхів бо вважали що не можна вбивати цяхи в храм спасителя ісуса христа який ними був прибитий на хресті він останній який побудували козаки перед скасуванням запорізької січі основним знаряддям будівничих була всьогонавсього сокира тому дотепер залишається загадкою як їм вдалося досягти такої високої точності у виготовленні деталей храм прикрашає дев'ять куполів пізніше перед ним була побудована дзвіниця виростаючи собор усе більше вражав усіх грандіозною монументальністю вишуканою стрімкістю та легкістю форм архітектор поєднав у ньому візантійське зодчество та українське бароко у цього храму є багато незбагнених таємниць наприклад одна з них геніальне моделювання замкненого простору який охоплює людину в інтер'єрі собору світлі прикрашені витонченими малюнками площини стін які в стрімкому злеті перетинаються створюють атмосферу величного спокою та божественного відсторонення від мирської марноти
dmytro@thonkpad ~/Study/SZK/Lab_4 main $
```

Рис. 2 — Другий приклад з ключами 11 та 12

```
1 2 3 4 5 6 dmytro@thonkpad: ~/Study/SZK/Lab_4 | xonsh  LW (15%) 100% 35% 58% 16% (1.22) 56°C 94% 27 Nov 2022 16:37:52

Input text:
дрогобич друге за розмірами місто львівської області що має чимало цікавих
пам'яток воно своєрідне адже на відміну від більшості інших західноукраїнсь
ких міст є зразком старовинного індустріального центру це звичайно не за мі
рками сучасності зараз зовні це затишне охайне містечко зі старовинними буд
инками та вимощеними бруківкою вуличками великого промислового значення мі
сто набуло ще з давніхдавен тут видобували сіль біле золото другим поштово
м до індустріального розвитку дрогобича стало відкриття нафтових джерел а в
році тут запрацював нафтопереробний завод до речі перший у центральній є
вропі нафта зробила місто багатим та успішним тому центральна його частина
може похвалитися розкішним архітектурним ансамблем тут височіє готичний соб
ор святого варфоломія а поруч тягнеться до неба дзвіниця перебудована з обо
ронної вежі поблизу також стоїть пам'ятник юрію котермаку філософу астроном
у професору медицини але головними пам'ятками міста справжніми дивами дрогоб
ича є дерев'яні церкви що вражають витонченістю та оригінальністю архітектур
ице місто хвилює та заспокоює водночас тут можна вічнавіч зустрітис з істо
рією доторкнутися до ще ніким не розгаданих таємниць

Encrypted text is:
хацинцш1б6хацин1бетбачеолатошболсжбцбюельсеицбцзютсжлпцбот б1шотуцбфлтыг
битокжбцбцбсць алхд1бтхр1бдтбълхолдцбълхбзлюеяцсжлбдхгбетггхдциатвдсе
ишгболсжб баетеицбсжтацщддцнцблдхсжалтведцнцбфіджачбфібешітудцбдібетбол
айтошбсцітсдсцжлбетатебецьдлбфібетжшяд1бцгтудіболсж1іицбелбсжтацщддшобзєх
шдитошбжтбшоцпідшошбзацшильицбьшошитошб1юишицнб1яацшошцнцбедтіідкболс
жцбдтзщюцп1б6ххтдлгхт1дбжшбжбхцщцтбшбслнеббзл1беццжцбхациншоб1яцжцгц
обхцблдхсжалтведцнцбачеьшжибхацинцш1тбсжтцбълхашжжкбдтмжцьгбхр1аіотбтб
ббачфлбжшбетятфчтбдтмжц1іаіацзшубетцхб6хцбаі1лб1іаяшубсбфіджкатедлб
ьяйцлбдтмжтбеацшотболсжцбзтнтжшбжтбсйлядшобжцшбфіджкатедтбучнцб1тсжшдтб
ш1тб бх1аіцкдлбф1аишбпцбятрчжебьшжцдіідлсжбжтбцашндтведлсжбтагл1ишжца
шф1болсжцбгьшюч бжтбетсйцицч бьхцдц1тсбжшжбжцбжордтб1дт1дтл1бешсжалшжсбелсж
ал чбхццциидшжсбхцб1бдлшшоб1б1бацентхтдшгбжт одшфе
dmytro@thonkpad ~/Study/SZK/Lab_4 main $

"b": 4,
"n": 5,
" ": 10,
"ф": 13,
"г": 13,
"й": 17,
"к": 14,
"д": 68,
"р": 8,
"я": 7,
"у": 7,
"ч": 10,
"м": 7
}
Most frequent letters: ('6', 'ц')
Found key A: 21
Found key B: 22
Trying to decrypt...
Decrypted text is:
дрогобич друге за розмірами місто львівської області що має чимало цікавих
пам'яток воно своєрідне адже на відміну від більшості інших західноукраїнсь
ких міст є зразком старовинного індустріального центру це звичайно не за мі
рками сучасності зараз зовні це затишне охайне містечко зі старовинними буд
инками та вимощеними бруківкою вуличками великого промислового значення мі
сто набуло ще з давніхдавен тут видобували сіль біле золото другим поштово
м до індустріального розвитку дрогобича стало відкриття нафтових джерел а в
році тут запрацював нафтопереробний завод до речі перший у центральній є
вропі нафта зробила місто багатим та успішним тому центральна його частина
може похвалитися розкішним архітектурним ансамблем тут височіє готичний соб
ор святого варфоломія а поруч тягнеться до неба дзвіниця перебудована з обо
ронної вежі поблизу також стоїть пам'ятник юрію котермаку філософу астроном
у професору медицини але головними пам'ятками міста справжніми дивами дрогоб
ича є дерев'яні церкви що вражають витонченістю та оригінальністю архітектур
ице місто хвилює та заспокоює водночас тут можна вічнавіч зустрітис з істо
рією доторкнутися до ще ніким не розгаданих таємниць
dmytro@thonkpad ~/Study/SZK/Lab_4 main $
```

Рис.3 — Третій приклад з ключами 21 та 22.