

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ  
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ  
ІМЕНІ ІГОРЯ СІКОРСЬКОГО»  
Фізико-Технічний Інститут

Звіт  
із лабораторної роботи №2  
із дисципліни «Криптографія»  
на тему  
Криптоаналіз шифру Віженера

Виконав:  
студент групи ФБ-13  
Берчук В.В.

Київ – 2023

## Мета роботи

Засвоєння методів частотного криптоаналізу. Здобуття навичок роботи та аналізу поточкових шифрів гамування адитивного типу на прикладі шифру Віженера.

## Порядок виконання роботи

1. Самостійно підібрати текст для шифрування (2-3 кб) та ключі довжини  $r = 2, 3, 4, 5$ , а також довжини 10-20 знаків. Зашифрувати обраний відкритий текст шифром Віженера з цими ключами.
2. Підрахувати індекси відповідності для відкритого тексту та всіх одержаних шифртекстів і порівняти їх значення.
3. Використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст.

## Вариант 9

## Хід роботи

Підбираю ключі та пишу код (encryptor.py) який буде шифрувати текст (text.txt). Я вибрав такі ключі:

```
keys = {
    2: "шо",
    3: "бар",
    4: "лаба",
    5: "грива",
    10: "валентинка",
    11: "затрушенный",
    12: "клокочкозубый",
    13: "макродинамика",
    14: "авиаперелет",
    15: "дезинтоксикация",
    16: "высокодисперсный",
    17: "ребристотрубчатый",
    18: "катапультироваться",
    19: "абонентодержатель",
    20: "нефтегазопереработка"
}
```

У результаті маю:

Індекс для нешифрованого тексту:  
0.057198

Ключ 2: 'шо'

Шифртекст:

ВЮЭЭЖЯККЮЮ

Індекс відповідності = 0,041849

Ключ 3: 'бар'

Шифртекст:

[illegible]

Індекс відповідності = 0.037506

Ключ 4: 'л

Шифртекст:

йдсяшньмуджррваншынипониханиодж

Індекс відпов:

Ключ 5: "Грива"  
Шифртекст:

нансофдрфьамибъпыиьртгчгпак

юззпнюържеух

Індекс від

Ключ 10: 'валентинка'

Шифртекст:

мррфыгъйшрукю

лцшмчнэмуй

Індекс Відповідності = 0.036161

Ключ 11: 'затрушенный'

Шифртекст:

срѣбичиыѣ

Індекс відповідності = 0.033987

Для зручності запишу результати у таблицю:

Кількість символів ключа	Індекс відповідності
2	0.041849
3	0.037506
4	0.040354
5	0.036563
10	0.036161
11	0.033987
12	0.034017
13	0.035304
14	0.034769
15	0.034495
16	0.033389
17	0.034111
18	0.033603
19	0.034114
20	0.034258

Індекс для відкритого тексту: 0.057198



Перейдемо до завдання 3. Потрібно розшифрувати даний текст (9var.txt). Після виконання коду (index.py) маємо таблицю із значеннями індексів відповідності для цього тексту:

Кількість символів ключа	Індекс відповідності
2	0.032889
3	0.032803
4	0.032777
5	0.032811
6	0.032805
7	0.032728
8	0.032834
9	0.032699
10	0.032853
11	0.032767
12	0.032617
13	0.032877
14	0.032780
15	0.032627
16	0.033041
<b>17</b>	<b>0.055390</b>
18	0.032629
19	0.032884
20	0.032559
21	0.032814
22	0.032870
23	0.032783
24	0.032638
25	0.032717
26	0.033028
27	0.032470
28	0.032565
29	0.032944
30	0.032497

Бачимо що при  $r = 17$  значення індексу помітно відрізняється. Збільшимо кількість символів до 70:

Довжина ключа 15: Індекс відповідності = 0.032627  
 Довжина ключа 16: Індекс відповідності = 0.033041  
Довжина ключа 17: Індекс відповідності = 0.055390  
 Довжина ключа 18: Індекс відповідності = 0.032629

Довжина ключа 32: Індекс відповідності = 0.033009  
 Довжина ключа 33: Індекс відповідності = 0.032896  
Довжина ключа 34: Індекс відповідності = 0.055875  
 Довжина ключа 35: Індекс відповідності = 0.032642

Довжина ключа 50: Індекс відповідності = 0.032629  
Довжина ключа 51: Індекс відповідності = 0.055313  
 Довжина ключа 52: Індекс відповідності = 0.032799  
 Довжина ключа 53: Індекс відповідності = 0.032821

Довжина ключа 66: Індекс відповідності = 0.033001  
 Довжина ключа 67: Індекс відповідності = 0.032625  
Довжина ключа 68: Індекс відповідності = 0.055482  
 Довжина ключа 69: Індекс відповідності = 0.032730

Бачимо такий же результат для  $r$  кратних 17, тому можемо припустити, що довжина ключа = 17 символів.

Тепер розіб'ємо текст на блоки (block\_count.py) та порахуємо яка літера найчастіше зустрічається в кожному блоці.

```
Найчастіше в блоці 1: п
Найчастіше в блоці 2: ь
Найчастіше в блоці 3: о
Найчастіше в блоці 4: н
Найчастіше в блоці 5: о
Найчастіше в блоці 6: ь
Найчастіше в блоці 7: о
Найчастіше в блоці 8: г
Найчастіше в блоці 9: е
Найчастіше в блоці 10: л
Найчастіше в блоці 11: ы
Найчастіше в блоці 12: т
Найчастіше в блоці 13: ж
Найчастіше в блоці 14: э
Найчастіше в блоці 15: ц
Найчастіше в блоці 16: л
Найчастіше в блоці 17: к
```

Маємо: **пьоноъогелытжэцлк**

Припустимо, що це зашифровані літери “о” шифром Цезаря у кожному блоці.

Розшифровуємо по формулі  $x = (y - k) \bmod m$ , де  $x$  – літера відкритого тексту,  $y$  – літера шифрованого тексту,  $k$  – ключ, у моєму випадку – 14,  $m$  – кількість літер в алфавіті (32).

Після розшифровки маю ключ: **боаяамахчэндшпиъ.**

З цього моменту починаються складності. Зразу у ключі видно слово *эндшпиъ*, якщо замінити *э* на *л*. Припустимо, що так і є. Спробуємо дешифрувати (decryptor.py) таким поки перехідним ключем:

ружкстагчгозамканбкшосночькалепльвфщочнадыведомойбжзноймьпетпоказауънвечдминеизмендънадысмполыхаутпщцчудшсвмьсозвездиснветушывводитзбддьяловыиеруладьюарбб  
астуцяминичиглйханерьматривалисердалкъверхотурьбийженнууомубылозамоаитъвсгуруниконуццггьесказаливышюдещйнныеюслпжйепаяюднакосбмйякалонрогнулаишукчуткь  
ыроесловнпкфкнеродомогочувеноснашлзъпронзйвбуезъеуцтввердълахуноуцавершиепдццмальькоблканвоюнееэчднималосэбдэтоъччтооблабупудавычисчезлисоекусобюочени  
ранньюжвчяемнонцатыйидегьяыадцовойлегюнонькьронлшиилдароановилцапротивоттчнвшигсмисемандсанюогнбфауходяпоурштуноъаледруимрещякиешчгортыпроевсалияследомсе  
евеньсточгопопритигнсшалессонерытрудофмбвийословномусалкипрулращалинегььюкюсщядухолмогвцуприяуупнуукрепояъпосщевнювозвлсарехиодныйпалитанэромупуткимеддфрит  
юазльхдевятъднжйропрожонныхнергйацдемдшиподходапмчзидощныбылиисеуактолкупослезатгщоодноуокозлонодиобжебифиздесъсогсоърядьхимператоссъялсьхерзениемдлитянар  
ьлотрублеонийгольаскривойналегдорастывшейфсхушкочлоззриласэнийцмпейтораипреждоемоощийаастертифкнымэснкомотпрбвсеекбнатокподнпжсмхольиправителемощинойсьлы

У тексті вже видно деякі слова, які можна розрізнити. Візьмемо наприклад частину *созве*.

Ймовірно, що це слово *созвездие*. Спробуємо далі підібрати правильний ключ.

Розшифруємо **пьоноъогелытжэцлк** відносно інших літер, які трапляються в тексті найчастіше (їх я визначав у 1 лабораторній роботі).

Відносно *е*: кчиййхйюажцнбшсже

Відносно *а*: оынмнщнвдкъсьехкй

Відносно *и*: зфжежтжыэгукюхогв

Відносно *н*: впбабнбцшюоещрйюэ

Перебравши в нашому ключі на першій позиції літери, позитивний результат маю при літері *в*, тобто ключ: **воаяамахчэндшпиъ.**

пуыкстагчгозамканакшосночькалепльвфщочнадыведомойбжзноймьпетпоказатьнвечдминеизмендънадысмполыхаутпщцчудшсвмьсозвездиснвет  
астуцяминичиглйханерьматривалисердалкъверхотурьбийженнууомубылозамоаитъвсгуруникомуццггьесказалибышюдещйнныеюсложйепаяью  
ыроесловнпкфкнеродомогочудивонашлзъпронзйвбуезъеуцтввердъкахуноуцавершиеподццмальькоблакамвоюнееэчднималосъбдэтоъччтообл  
ранньюжвчяемнонцатыйидевьяыадцовойлегюнонькьронлшиилдароановилцапротивостчнвшигсмисемандранюогнбфауходяпотрйштуноъаледруимпе  
ебенъсточгопопртивншшалессонерытрудофмбвийословномуралкипрулращалинегььюкюсщядухолмоввцуприяуупнуукрепояъпосщевнювозвелсар  
юазльхдевятъднейропрожонныхнергйацдемдшиподходапомчзидощныбылиистеактолкупослезавтщоодноуокозлонодиобжебифиздесъсовсоърядьх  
ьлотрубленнийгольаскривойналегдорастывшейфсхушкочлоззриласэнийцмпейтораипреждоемоощийаастерсифкнымэснкомотправсеекбнатокп

Вже ближче, наступна літера о виглядає найкращим варіантом після в, залишимо її. На 3 місце є кандидати й, н, ж, б. Спробуємо й: **войяамахчэндшпиль**

путь стаю гозам канакрасночькалепльвущейнадыведомой бездноймьпетпоказатьснвечьдминеизменньнадысмпольхаютпрчудшсвье **созвездия** ветушв астуцаминичьиглаханерьматривалисьвдалкьверхотурыбашеннуоумбылозаметитьсгуруникомуничегыцесказалибыподещйныееюсложныепаяыодна ыроесловноклыкнеродомогочудищанасшлозьпронзившеезъцуютвердькамунноуцавершиеподнцмальькоблакамвеюнееэчднималосьбызототьчтооблака раннеевосемноцатыйидевятнадцатыйлег ионыоборонлишииелдарнадавилицапротивостоявшигсмисемандрадрогабфауходяпотраштуноьаледруимперяк ебедьстоцгопопротивникалесонерытрудолюбивыесловномуравкипрулращалиневысокуюсцядухолмоввнуприяуипнуякрепосаьпосщбнювозвелиарехии юазльхдевятднейзапрожонныхнергианцемдщиподходапомозидошпныбылиистечтьтолкуюпослезавтраодноуокозлогиеужебифиздесьсовсемрядьхимпе ьлотрубленнагольаскривойнавсегдорастывшейусмешкоцлоззриласьнаимпейторайпреждееемощийаастерсилкнымэснкомотправиеекбнатокподн

Підходить, залишаємо. Можна припустити, що перше слово в ключі це *война*, спробуєм його:

путь стаю гозам канакрасночькалепльвущейнадыведомой бездноймьпетпоказатьснвечьдминеизменньнадысмпольхаютпричудшсвье **созвездия** ветушв астуцаминичьиглазанерьматривалисьвдалкьверхотурыбашеннуоумбылозаметитьсгуруникомуничегыцесказалибыпродещйныееюсложныепаяыодна ыроесловноклыкнеродомогочудищанасшлозьпронзившеезъцуютвердькаменноуцавершиеподнцмальькоблакамвернееэчднималосьбызототьчтооблака раннеевосемноцатыйидевятнадцатыйлег ионыоборонлишииелдарнадавилицапротивостоявшигсмисемандрадрогабфауходяпотрактуюьаледруимперск ебедосточгопопротивникалесонерытрудолюбивыесловномуравьипрулращалиневысокуюсцядухолмоввнуприяуипнуякрепостьпосщбнювозвелитрехю разльхдевятднейзапрожонныхнергианцемдщиподходапомозидошпныбылиистечтьтолкуюпослезавтраодноуокозлогиеужебифиздесьсовсемрядьхимпе ьлотрубленнаягольаскривойнавсегдорастывшейусмешкоцлоззриласьнаимпейторайпреждееемощийаастерсилнымэснкомотправиеекбнатокподн

Маємо прогрес і ключ **война махч эндшпиль**. На цьому етапі я вирішив зауглити чи є щось в інтернеті, що містить ці слова і знаходжу книгу “Война мага. Эндшпиль”.

Спробуєм дешифрувати:

путь старогозам канакраснойскалепльвущейнадыведомой безднойможетпоказатьсявечнымининеизмеи астенаминичьиглазаневсматривалисьвдалкьверхотурыбашеннекомубылозаметитьсгуруникомуничегыцесказалибыпродещйныееюсложныепаяыодна троесловноклыкневедомогочудищанасквозьпронзившееземнуютвердькаменноенавершиеподнимало раннеевосемнадцатыйидевятнадцатыйлег ионыоборонявшииелдарнадавилинапротивостоявшихимис ебедостойногопротивникалег ионерытрудолюбивыесловномуравьипревращалиневысокуюгрядухолм разломдевятднейзапрошенныхнергианцемдляподходапомоидолжныбылиистечтьтолькопослезавтра овьотрубленнаяголоваскривойнавсегдазастывшейусмешкойвоззриласьнаимператорайпреждееемми

Текст розшифровано (decrypted\_9var.txt), отже ключ **войнамагаэндшпиль**.

## Висновок

У ході виконання лабораторної роботи я засвоїв методи частотного криптоаналізу. Я досліджував шифр Віженера, на прикладі якого я набув практичні навички аналізу та розшифрування криптографічних шифрів.