Міністерство освіти і науки України

Національний технічний університет України

"Київський політехнічний інститут імені Ігоря Сікорського"

Фізико-технічний інститут

Криптографія

Комп’ютерний практикум №2

Криптоаналіз шифру Віженера

Варіант 3

Виконали:

Студенти 3 курсу

Загородній Я.М, Венгер П.Ю.

Перевірив:

Київ – 2024

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

Постановка задачі:

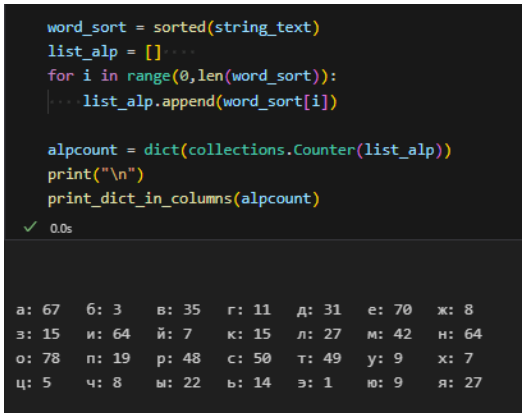
1. Самостійно підібрати текст для шифрування (2-3 кб) та ключі довжини r = 2, 3, 4, 5, а також довжини 10-20 знаків. Зашифрувати обраний відкритий текст шифром Віженера з цими ключами.

2. Підрахувати індекси відповідності для відкритого тексту та всіх одержаних шифртекстів і порівняти їх значення.

3. Використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст (згідно свого номеру варіанта).

Хід роботи

1. Для шифрування був вибраний текст з сайту (https://lingua.com/ru/russkiy/chteniye/vremena-goda/) «Времена года», який був записаний в text_lab2.txt а потім за допомогою коду був редагований в текст написаний російською мовою без знаків пунктуації, великих літерів та пробілу, а буква «ё» була заміненна «е». І даний текст був збережений в text_lab2_clean.txt .



2. Було створено ключи різної розмірності (2, 3, 4, 5, 10-20)

```
text_open = open("D:\\Web-devoloped\\Krpt\\cp2\\text_lab2_clean.txt", encoding='utf-8').read()
keys = ['он',
        'она',
        'шифр',
        'слово',
        'информация',
        'кодовеслово',
        'закодировать',
        'розкодировать',
        'сотрудничество',
        'двузначноечисло',
        'трехзначноечисло',
        'шифраторивиженера',
        'операциинадчислами',
        'моногаммахудожника',
        'автоматыдлякодировкы', ]
for key in keys:
    print(f"Ключ: '{key}', Кількість символів: {len(key)}")
```

0.0s

```
Ключ: 'он', Кількість символів: 2
Ключ: 'она', Кількість символів: 3
Ключ: 'шифр', Кількість символів: 4
Ключ: 'слово', Кількість символів: 5
Ключ: 'информация', Кількість символів: 10
Ключ: 'кодовеслово', Кількість символів: 11
Ключ: 'закодировать', Кількість символів: 12
Ключ: 'розкодировать', Кількість символів: 13
Ключ: 'сотрудничество', Кількість символів: 14
Ключ: 'двузначноечисло', Кількість символів: 15
Ключ: 'трехзначноечисло', Кількість символів: 16
Ключ: 'шифраторивиженера', Кількість символів: 17
Ключ: 'операциинадчислами', Кількість символів: 18
Ключ: 'моногаммахудожника', Кількість символів: 19
Ключ: 'автоматыдлякодировкы', Кількість символів: 20
```

Потім був зашифрований відкритий текст за допомогою «Шифр Віженера», всі зашифровані тексти були записані в файли в папці **vigenere_encrypt**

```
def vigenere_encrypt(plaintext, key):
    ciphertext = []
    key_length = len(key)
    key_as_int = [ord(i) - ord('а') for i in key]
    plaintext_int = [ord(i) - ord('а') for i in plaintext if 'а' <= i <= 'я']

    for i in range(len(plaintext_int)):
        value = (plaintext_int[i] + key_as_int[i % key_length]) % 32
        ciphertext.append(chr(value + ord('а')))

    return ''.join(ciphertext)

ciphertexts = {}
for key in keys:
    encrypted_text = vigenere_encrypt(text_open, key)
    ciphertexts[key] = encrypted_text
    print(f"Ключ: '{key}', Зашифрований текст: {encrypted_text}\n")

    with open(f"vigenere_encrypt\\iphertext_{len(key)}.txt", "w", encoding='utf-8') as file:
        file.write(encrypted_text)
print("Всі зашифровані тексти записані у файли.")
```

3. Визначаємо індекс відповідальності для відкритого тексту та для шифрованіх текстів (дані збережені в табличку **index_of_coincidence_results**)

Key	Length key	Index_of_coincidence
Відкритий текст	ВТ	0,057952474
он	2	0,04900652
она	3	0,04167671
шифр	4	0,036417292
слово	5	0,040252155
информация	10	0,03303668
кодовеслово	11	0,03657798
закодировать	12	0,033963722
розкодировать	13	0,034532307
сотрудничество	14	0,034995828
двузначноечисло	15	0,033571274
трехзначноечисло	16	0,034930935
шифраторивиженера	17	0,034108958
операциинадчислами	18	0,033982263
монограммахудожника	19	0,034034795
автоматыдлякодировкы	20	0,032931615

```python
import pandas as pd

def index_of_coincidence(text):
    frequency = [0] * 32  # Для російських літер
    for char in text:
        if 'а' <= char <= 'я':
            frequency[ord(char) - ord('а')] += 1
    total_letters = sum(frequency)

    if total_letters == 0:
        return 0

    ic = sum(f * (f - 1) for f in frequency) / (total_letters * (total_letters - 1))
    return ic

# Створюємо словник для збереження результатів
indexes = {
    "Key": [],
    "Length key" : [],
    "Index_of_coincidence": []
}

# Обчислення індексу відповідності для відкритого тексту
plaintext_ic = index_of_coincidence(text_open)
print(f"Індекс відповідності відкритого тексту: {plaintext_ic}")

# Додаємо відкритий текст в результати
indexes["Key"].append("Відкритий текст")
indexes["Length key"].append("ВТ")
indexes["Index_of_coincidence"].append(plaintext_ic)

# Обчислення індексу відповідності для кожного шифротексту
for key, ciphertext in ciphertexts.items():
    ciphertext_ic = index_of_coincidence(ciphertext)
    print(f"Індекс відповідності для ключа '{key}': {ciphertext_ic}")

    # Додаємо результати в словник
    indexes["Key"].append(key)
    indexes["Length key"].append(len(key))
    indexes["Index_of_coincidence"].append(ciphertext_ic)

df = pd.DataFrame(indexes)
indexes_file = "index_of_coincidence_results.xlsx"
df.to_excel(indexes_file, index=False)

print(f"Результати записано в {indexes_file}")
```

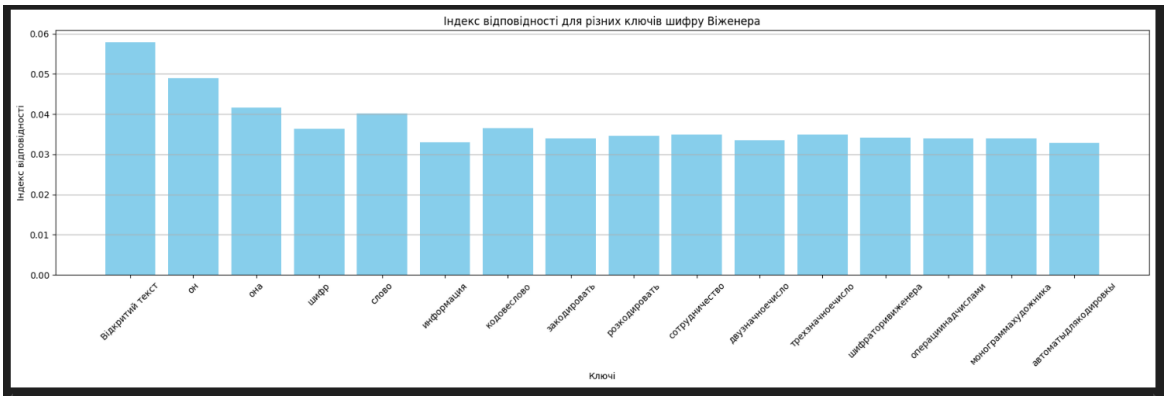
```
Індекс відповідності відкритого тексту: 0.05795247365656191
Індекс відповідності для ключа 'он': 0.04900652019406075
Індекс відповідності для ключа 'она': 0.04167670961960385
Індекс відповідності для ключа 'шифр': 0.036417292419888135
Індекс відповідності для ключа 'слово': 0.040252155372207284
Індекс відповідності для ключа 'информация': 0.033036679954265936
Індекс відповідності для ключа 'кодовеслово': 0.036577979666882976
Індекс відповідності для ключа 'закодировать': 0.03396372176385155
Індекс відповідності для ключа 'розкодировать': 0.03453230740706406
Індекс відповідності для ключа 'сотрудничество': 0.034995828311856866
Індекс відповідності для ключа 'двузначноечисло': 0.03357127406446031
Індекс відповідності для ключа 'трехзначноечисло': 0.03493093538518587
Індекс відповідності для ключа 'шифраторивиженера': 0.034108958314019965
Індекс відповідності для ключа 'операциинадчислами': 0.033982262600043264
Індекс відповідності для ключа 'монограммахудожника': 0.034034794969253115
Індекс відповідності для ключа 'автоматыдлякодировки': 0.032931615215846234
Результати записано в index_of_coincidence_results.xlsx
```

Побудую гістограму для демонстрації індексів відповідальності

```python
import matplotlib.pyplot as plt

plt.figure(figsize=(18, 6))
plt.bar(df["Key"], df["Index_of_coincidence"], color='skyblue')
plt.xlabel('Ключі')
plt.ylabel('Індекс відповідності')
plt.title('Індекс відповідності для різних ключів шифру Віженера')
plt.xticks(rotation=45)  # Повертаємо підписи по осі X для кращого вигляду
plt.grid(axis='y')

# Відображення гістограми
plt.tight_layout()
plt.show()
```



Для дешифрування тексту використаємо перший метод з методичних вказівок.

1. Читаємо файл з текстом

```python
encryption_text = open('encrypted_text(3).txt', encoding='utf8').read().replace('\n', '')
print(encryption_text)
```

✓ [80] < 10 ms

2. Обчислюємо частоту літер у тексті

```python
# Функція для обчислення частоти
def calc_letters_frequency(text: str):
    letters_frequency = {c: text.count(c) for c in set(text)}
    letter_frequency_dict = {c: round(count / len(text), 5) for c, count in
                             letters_frequency.items()}
    return letters_frequency, letter_frequency_dict
```

3. Обчислюємо індекс відповідності

```
def calc_index_of_coincidence(text):
    letter_counts, _ = calc_letters_frequency(text)
    total = sum(letter_counts[char] * (letter_counts[char] - 1) for char in letter_counts)
    index = total / (len(text) * (len(text) - 1)) if len(text) > 1 else 0
    return index
```

4. Розбиваємо текст на блоки

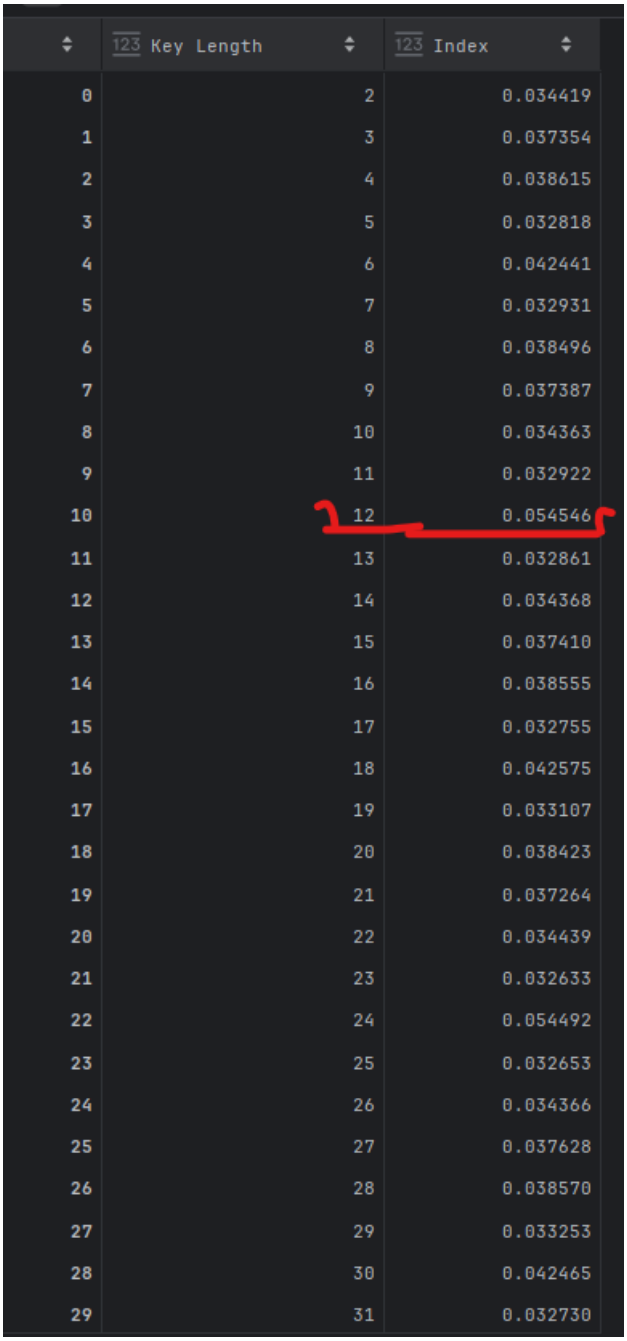
```
def create_blocks(text, key_length):
    blocks = []
    for i in range(key_length):
        block = ""
        for j in range(0, len(text), key_length):
            if i + j < len(text):
                block += text[i + j]
        blocks.append(block)
    return blocks
```

5. Знаходимо індекс відповідності для всіх можливих довжин ключа

```
def find_key_length_index(text):
    key_results = pd.DataFrame(columns=['Key Length', "Index"])
    for key_length in range(2, 32):
        blocks = create_blocks(text, key_length)
        indices = [calc_index_of_coincidence(block) for block in blocks]
        avg_index = np.mean(indices)
        key_results.loc[len(key_results)] = {'Key Length': key_length, 'Index': avg_index}

    return key_results
```

6. Отримуємо таблицю з індексами. Шукаємо той, що найближче до індексу відповідності російської мови – 0,055



	Key Length	Index
0	2	0.034419
1	3	0.037354
2	4	0.038615
3	5	0.032818
4	6	0.042441
5	7	0.032931
6	8	0.038496
7	9	0.037387
8	10	0.034363
9	11	0.032922
10	12	0.054546
11	13	0.032861
12	14	0.034368
13	15	0.037410
14	16	0.038555
15	17	0.032755
16	18	0.042575
17	19	0.033107
18	20	0.038423
19	21	0.037264
20	22	0.034439
21	23	0.032633
22	24	0.054492
23	25	0.032653
24	26	0.034366
25	27	0.037628
26	28	0.038570
27	29	0.033253
28	30	0.042465
29	31	0.032730

Найближче – довжина ключа 12, тому обираємо її

7. Знаходимо можливий ключ на основі частотного аналізу

```python
def find_key(text):
    blocks = create_blocks(text, 12)
    key_options = []

    for block in blocks:
        _, frequency_dict = calc_letters_frequency(block)
        most_frequent_letter = max(frequency_dict, key=frequency_dict.get)
        possible_letters = [
            alphabet[(alphabet.index(most_frequent_letter) - alphabet.index(reference_letter)) % 32]
            for reference_letter in ['о', 'е', 'и', 'а']
        ]
        key_options.append(possible_letters)

    return key_options
```

8. Отримуємо зсуви найбільш частотних літер відносно найбільш популярних символів у російській мові о, е, и, а

```
[['в', 'л', 'и', 'р'],
 ['ш', 'б', 'ю', 'ж'],
 ['е', 'о', 'л', 'у'],
 ['б', 'к', 'з', 'п'],
 ['с', 'ъ', 'ч', 'я'],
 ['п', 'ш', 'х', 'э'],
 ['и', 'с', 'о', 'ц'],
 ['р', 'щ', 'ц', 'ю'],
 ['б', 'к', 'з', 'п'],
 ['у', 'ь', 'щ', 'б'],
 ['р', 'щ', 'ц', 'ю'],
 ['я', 'и', 'е', 'н']]
```

9. Підбираємо ключ. «вшекспирбуря»
10. Дешифруємо текст

```
def decode(text, key):
    decrypted_text = []
    key_length = len(key)
    for i, c in enumerate(text):
        decrypted_char = alphabet[(alphabet.index(c) - alphabet.index(key[i % key_length])) % 32]
        decrypted_text.append(decrypted_char)

    return ''.join(decrypted_text)

decrypted_text = decode(encryption_text, 'вшекспирбуря')
print(decrypted_text)
```

11.Отримуємо відкритий текст

действующиелицаалонзокорольнеаполитанскийсебастьянегобратпросперозаконныйгерцогмиланскийантониоег
обратнезаконнозахвативший властьвмиланскомгерцогствефердинандсынкоролянеаполитанскогогонзалостарыйч
естныйсоветниккоролянеаполитанскогоадрианфрансископридворныекалибанрабуродливыйдикарьтринкулошут
стефанодворецкийпьяницакапитанкораблябоцманматросымирандадочьпросперо ариэльдухвоздухаиридацерера
юнонанимфыжнецыдухидругиедухипокорныепросперо местодействиякораблькорабльвморебурягро
мимолниявходяткапитанкорабляибоцманкапитанбоцманбоцманслушаюкапитанкапитанзовикомандуна верхжив
ейзаделонетомыналетимнарифыскорейскорейкапитануходитпоявляютсяматросыбоцманэймолодцыве селейребя
тавеселейживоубратьмарсельслушайкапитанскийсвистокнутеперьветертебепросторнодуйпоканелопнешьвходят
алонзосебастьянантониофердинандгонзалоидругиеалонзодобрыйбоцманмыполагаемсянатебяагдекапитанмужай
тесьдрузьябоцмананукаотправляйтесьвнизантониобоцмангдекапитанбоцманавамегонеслышночтоливынаммеша
етеотправляйтесьвкаютывидитештормразыгралсяатутещевыгонзалополегчелюбезныйусмирисьбоцманкогдаусм
иритсяморе убирайтесьэтимревущимваламнетделадокоролеймаршпокаютаммолчатьнемешайтегонзаловсетакип
омнилюбезныйктоутебянабортубоцманаяпомнючтонетникогочьяшкурабылабымнедорожемоейсобственнойвотв
ысоветникможетпосоветуетестихиямутихомиритьсятогдамыинедотронемсядоснастейнукаупотребитевашувласт
ьаколинеберетесьтоскажитеспасибочтодолгопожилинасветепроваливайтевкаютудаприготовьтесьнеровенчасслу
читсябедаэйребятапошевеливайсяпрочьсдорогиговорятвамвсекромегонзалоуходятгонзалооднакоэтотмалыймен
яутешилонотъявленныйвисельникакомусужденобытьповешеннымтотнеутонетофортунадайемувозможностьдож
итьдовиселицысделайпредназначеннуюдлянеговеревкунашимякорнымканатомведьоткорабельногосейчаспольз

ымалоеслиемунесужденобытьповешеннымымыпропалигонзалоуходитбоцманвозвращаетсябоцманопуститьстень
гуживонижениженепопробуемидтинаодномгротеслышенкрикчумазадавиэтихгорлодеровонизаглушаютибурюикап
итанскийсвистоквозвращаютсясебастьянантониоигонзалоопятьвытутчеговамнадочтожеброситьвсеиззавасиидти
надновамохотаутонутьчтолисебастьянязватебевглоткупроклятыйгорланнечестивыйбезжалостныйпесвоттыктоб
оцманахтакнуиработайтетогдасамиантониоподлыйтрусмыменьшебоимсяутонутьчемтыгрязныйублюдокнаглаят
ыскотинагонзалоонтоужнепотонетеслибдаженашкорабльбылнепрочнейореховойскорлупыатечьвнембылобытак
жетруднозаткнутькакглоткуболтливойбабыбоцмандержикручекветрукручеставьгротифокдерживоткрытоеморе
прочьотберегавбегаютпромокшиематросыматросымыпогиблимолитесьпогиблиуходятбоцманнеужтонампридет
сярыбкормитьгонзалокорольипринцмольбывозносяткбогунашдолгбытьрядомснимисебастьянявзбешенантонион
аспогубилаэташайкапьяницгорластыйпесоеслибутонултыдесятьразподрядизбитыйморемгонзалонетпоручусьон
виселицейкончитхотябывсеморяиокеаныуговорилисьпотопитьегоголосавнутрикорабляспаситетонемтонемпрощ
айтеженаидетибратпрощайтонемтонемтонемантониопогибнемрядомскоролемвсекромегонзалоуходятгонзалояб
ыпроменялсейчасвсеморяиокеанынаодинакрбесплоднойземлисамойнегоднойпустошизаросшейверескомилидро
комдасвершитсяволягосподняновсетакиябыпредпочелумеретьсухойсмертьюуходитостровпередпещеройпроспе
ровходятпроспероимирандамирандаоеслиэтовыотецмоймилыйсвоеювластьювзбунтовалиморетоямолювасусмир
итьегоказалосьчтогорящаясмолапотокамиструитсяснебосводановолныдостигавшиенебессбивалипламяокакястр
адаластраданьяпогибавшихразделяякорабльотважныйгдеконечнобылиичестныеиправедныелюдиразбилсявщеп
ывсердцеуменязвучитихвоплювыонипогиблибылабыявсесильнымбожествомяморевверглабывземныенедраскор
ейчемпоглотитьемудалабыкорабльснесчастнымилюдьмипросперо утешься япустьдоброетвоенестонетсердценикто
непострадалмирандаужасныйденьпросперониктонепострадалявсеустроилзаботясьотебемоедитяодочериединств
еннойлюбимойведьтынезнаешьктомыиоткудачтоведомотебечтотвойотецзоветсяпросперо ичтоемупринадлежиту
богаяпещерамирандарасспрашиватьмневмысльнеприходилопросперонасталовремявсетебеоткрытьнопомогимне
снятьмойплащволшебныйснимаетплащлежимогуществомоемирандеутешьсяотримирандаслезысостраданьястол
ьбедственноекораблекрушеньекотороеоплакиваешьтыясилоюискусствасвоегоустроилтакчтовсеосталисьживыда
целывсектоплылнаэтомсуднектопогибалвволнахзовянапомощьсихголовыиволоснеупалсадисьислушайвсесейча
сузнаешьмирандавычастособиралисьмнеоткрытьктомыипрерывалисвойрассказсловаминетпостойещеневремяпр
осперонопробилчасвнимаймоимречамкогдавпещерепоселилисьмытебеедваисполнилосьтригодаитынаверноене
можешьвспомнитьотомчтобылопреждемиранданетяпомнюпросперотыпомнишьчтожедомилилюдейповедайобо
всемчтосохранилатывпамятисвоейпоявляетсяневидимыйариэльонпоетвсопровождениимузыкизанимследуетфер
динандариэльпоетдухигорлесовиводвсевхороводутихломоревлегкойпляскесплескомруксомкнитекругмнедружн
овторявнимайтедухисовсехсторонгаугауариэльпсысторожевыелайтедухигаугауариэльвнимайтеморесмолклодал
ьтихаслышнопеньепетухакукарекуфердинандоткудаэтамузыкаснебесилисземлитеперьонаумолклатоверногимн
ыздешнимбожествамясмертьотцаоплакиваягорькосиделнаберегувдругповолнамкомнеподкралисьсладостныезву
киумеривяростьволнискорбьмоюяследуюзамузыкойвернееонаменявлечетонаумолкланетвотопятьариэльпоетоте
цтвойспитнаднеморскомонтиноюзатянутистанетплотьегопескомкоралломкостистанутоннеисчезнетбудетонлиш
ьвдивнойформевоплощенчуслышенпохоронныйзвондухидиндондиндонариэльморскиенимфыдиндиндонхранят
егопоследнийсонфердинандпоетсявпеснеомоемотценемогутбытьземнымиэтизвукионисюданисходятсвысотыпр
осперомирандеприподнимижезанавесресницвзглянитудамирандачтоэтодухобожекаконпрекрасенправдаведьоте
цпрекрасенонноэтолишьвиденьепроспероонетдитяоннамвовсемподобениспитиестичувствуеткакмыонспассявпл
авьпрокораблекрушеньездесьищетонтоварищейпропавшихкогдабытолькоскорбьврагкрасотынеискажалачертего
лицатыназвалабыюношукрасивыммирандабожественнымегобяназваланетназемлесуществтакихпрекрасныхпрос
перовсторонуслучилосьвсекакяпредначерталмойариэльискусныйязаэточередздаднятебяосвобожуфердинандтак
вотонабогинявчестькоторойзвучалтотгимнответомудостойтыздесьнаэтомостровеживешьчтоделатьмневелишьво
проспоследнийноглавныйдляменяскажимнечудотыфеяилисмертнаямирандасиньорядевушкапростаяянечудофер
динандкакмойроднойязыкноеслибябылтамгдеговорятнанемябылбыизвсехтоговоритнанемпервейшимпросперо
первейшимнуаеслибуслыхалтебякорольнеаполяфердинандонслышитдивясьчтовдругт

Висновок

Засвоїли методи частотного криптоаналізу. Здобули навички роботи та аналізу потокових шифрів гамування адитивного типу на прикладі шифру Віженера.