Національний технійчний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Фізико-технічний інститут

«Криптографія»

Комп’ютерний практикум №2

Криптоаналіз шифру Віженера

Виконали:

ФБ-21 Жиговець Олександр

ФБ-21 Альгішиєв Дмитро

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

Варіант: 3

Хід роботи

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.

```
keys = [
    "да",
    "нет",
    "снег",
    "взять",
    "возможност",
    "красивыхили",
    "можноиспольз",
    "путьквыживани",
    "беглеципитомцы",
    "охотаиприбежище",
    "непокореннаяземл",
    "покорителипустоши",
    "беглецвнебезопасно",
    "выжитьвсредепустоши",
    "выжитьлюбымисредства"
]
```

```
Довжина ключа: 2
Довжина ключа: 3
Довжина ключа: 4
Довжина ключа: 5
Довжина ключа: 10
Довжина ключа: 11
Довжина ключа: 12
Довжина ключа: 13
Довжина ключа: 14
Довжина ключа: 15
Довжина ключа: 16
Довжина ключа: 17
Довжина ключа: 18
Довжина ключа: 19
Довжина ключа: 20
```

Було використано ключі на картинці вище із вказаними довжинами. Для шифрування тексту була використана наступна функція:

```
def encr(text:str, key:str) -> str:
    chars = "абвгдежзийклмнопрстуфхцчшщъыьэюя"
    result = ""

    kI = 0
    for char in text:
        char_index = chars.index(char)
        key_char_index = chars.index(key[kI % len(key)])
        new_char_index = (char_index + key_char_index) % len(chars)
        new_char = chars[new_char_index]

        result += new_char
        kI += 1

    return result
```

Пройшовшись по масиву з ключами текст було зашифровано кожним ключем.

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

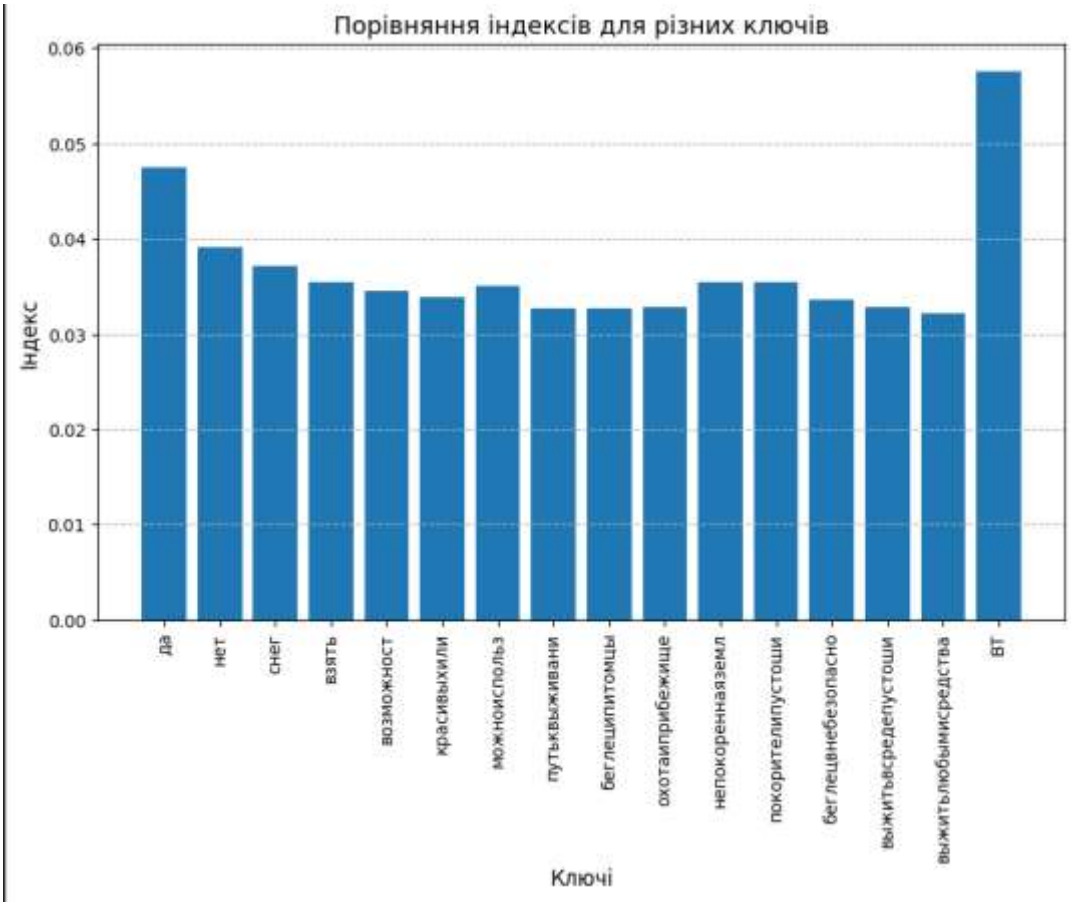
Індекси підраховані наступною функцією:

```python
def idx(text:str) -> float:
    chars = char_n(text)

    ic = 0
    for count in chars.values():
        ic += count * (count - 1)

    return ic / (len(text) * (len(text) - 1))
```

Після підрахунку індексів всіх шифротекстів, було отримано наступні результати, як бачимо, найбільший індекс має відкритий текст:



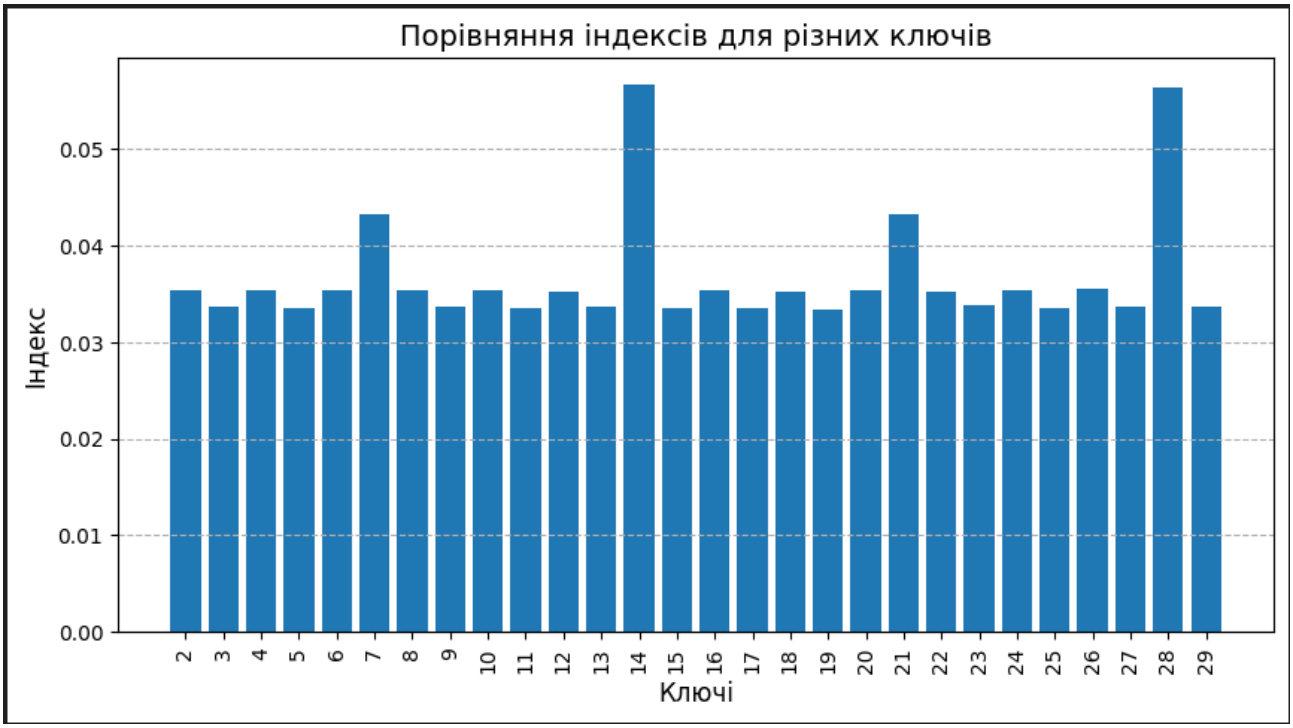
Використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст (згідно свого номеру варіанта).

```python
def make_blocks(text: str, l):
    blocks = [""] * l
    i = 0
    for char in text:
        i_block = i % l
        blocks[i_block] += char
        i += 1
    return blocks

def key_l(text:str) -> dict:
    results = {}
    for key_length in range(2, 30):
        blocks = make_blocks(text, key_length)
        i = []
        for block in blocks:
            i.append(idx(block))
        avg = sum(i) / len(i)
        results[key_length] = avg
    return results
```

Для визначення довжини ключа було використано функцію key_l, яка в свою чергу використовує функцію make_blocks.

Порівнюючи результати на діаграмі, бачимо, що наш ключ має довжину 14.



Після визначення довжини шукаємо можливі літери ключа, для порівняння було взято літеру «о».

```python
def find_key(text: str, l: int) -> list:
    chars = "абвгдежзийклмнопрстуфхцчшщьыэюя"
    block_size = 14
    blocks = make_blocks(text, block_size)
    key = []

    for block in blocks:
        freq = char_n(block)

        freq_char = max(freq, key=freq.get)
        offset = (chars.index(freq_char) - chars.index('о')) % len(chars)

        key_char = chars[offset]
        key.append([key_char])

    return key
```

Результат, після аналізу розуміємо, що ключ, це «экомаятникфуко»

Шифротекст:

еьбюятфхмпяякнпчццшявпрыумтчкктълвацхтжышэргущнныюкшяпьйтшюмвзщыэъвачьймуч ицъхцщьдерэхшълдунхтутсыэхыъибгмттэбгбптщныоасякдуццйпющоибаужеуацебаъпдвхцою бхуюкыфйнбэнощюпыльыъшдяхнцюхктнкащовачцъбтощечйщисъчятеюэюзшаърнчхшъфйть ккщиннчсуйгбощрчызхтюыкщдшощеаьшбнштщьцшчылуюмцзаънэюбыыеьучьмаюцщдтновь ьцртшъцыжыытекъстптщрхтфегоэзсссфажгьифюрньокяьхкъщяйэвъушешчъримуъольърннхы чшясыозщюътз

Частина розшифрованого тексту:

Итутяувиделмаятникшарвисящийнадолгойнитиопущеннойсвольтыхоравизохронномвеличии описывалколебанияязналноивсякийощутилбыподчарамимернойпульсациичтопериодколебан ийопределенотношениемквадратно

Висновки

Під час виконання роботи засвоїли метод криптоаналізу шифру Віженера, навчились розшифровувати текст на основі цього методу. Невеличка проблема виникла при визначенні ключа, не одразу було зрозуміло, що це «экомаятникфуко».