Виконав ст. ФБ-12 Слєпий Роман Варіант №11

# КРИПТОГРАФІЯ
## КОМП'ЮТЕРНИЙ ПРАКТИКУМ №2
### Криптоаналіз шифру Віженера

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

## Порядок виконання роботи
0. Уважно прочитати методичні вказівки до виконання комп'ютерного практикуму.
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.**Ознайомився з методичними вказівками до виконання комп'ютерного практикуму та рекомендаціями стосовно виконання(лайфхаками)

**2.** Підібрав файл для шифрування 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.

Як текст використав цитату з книги «О криптографии всерьез» Жан-Філіпп Омассон в файл формату .txt. Файл в папці під назвою "vig.input.txt"

Як ключі використовував

r=2: «ты»
r=3: «дуб»
r=4: «роща»
r=5: «атлет»
r=10: «фотосинтез»
r=15: «виброуплотнение»
r=20: «фотосинтезврощебудет»

Зашифрував текст шифром Віженера "encoding.py"

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

Написав код для підрахування індексу відповідності в кожному файлі

«#counter.py»

Для цього використовував формулу :

$$I(Y) = \frac{1}{n(n-1)} \sum_{t \in Z_m} N_t\,(Y)(N_t(Y) - 1)$$

Де n=довжина тексту, а $Nt\ (Y)$ – кількість появ букви $t$ у шифртексті $Y$.

| **Тип тексту** | **Індекс відповідності** |
|---|---|
| Незашифрований | 0.05419028 |
| r=2 | 0.04293673 |
| r=3 | 0.03955044 |
| r=4 | 0.03615929 |
| r=5 | 0.03554788 |
| r=10 | 0.03410449 |
| r=15 | 0.03405097 |
| r=20 | 0.03271624 |

Як бачимо зі збільшенням довжини ключа зменшується математичне сподівання

4. Використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст (згідно свого номеру варіанта)(Варіант №18)
Створив програму, яка використовуючи наведені нижче положення

Для знаходження істинного значення $r$ за допомогою індексу відповідності пропонується два можливих алгоритми. Перший алгоритм виглядає так:

1) Для кожного кандидата $r = 2,3,...$ розбити шифртекст $Y$ на блоки $Y_1, Y_2, ..., Y_r$.
2) Обчислити значення індексу відповідності для кожного блоку.
3) Якщо сукупність одержаних значень схиляється до теоретичного значення $I$ для даної мови, то значення $r$ вгадане вірне. Якщо сукупність значень схиляється до значення $I_0 = \frac{1}{m}$, що відповідає мові із рівноімовірним алфавітом, то значення $r$ вгадане неправильно.

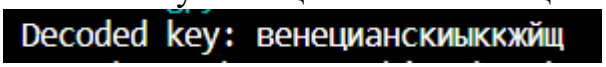
Знайшов довжину ключа
I(теор)=0,0467558
“find_key_len.py” і визначив що довжина ключа для мого варіанту 17 символів

Далі я створив програму яка за принципом

Після встановлення значення періоду шифру подальше його розшифрування зводиться до серії розшифрувань шифрів Цезаря. Дійсно, кожен фрагмент $Y_i$ зашифрований шифром Цезаря з ключем $k_i$, $i = \overline{1,r}$; знайти цей ключ можна, поклавши $k = (y^* - x^*) \bmod m$, де $y^*$ – буква, що частіше за всіх зустрічається у фрагменті $Y_i$, а $x^*$ – найімовірніша буква у мові, якою написано відкритий текст (для російської мови це буква «о», для англійської – буква «е» тощо). Якщо ключ вгадано невірно, замість $x^*$ треба брати другу, третю і т.д. за імовірністю літеру, або коригувати значення ключа відповідно до реконструкції тексту за правильно розшифрованими фрагментами.

При розшифруванні деякі фрагменти будуть встановлені неправильно, але можливі помилки легко виправляються при аналізі розшифрованого тексту в цілому.

Знайшов ключ за допомогою програми “key_find.py”
Decoded key: венецианскиыккжйщ




- логічно можна здогадатися, що малося на увазі. Ключ= «венецианскийкупец»

Далі, за допомогою програми “decoding.py” – розшифрував ШТ

5.Висновки
Висновки*: в ході виконання комп. Практикуму №2 я засвоїв методи частотного криптоаналізу. Здобув навички обробки та аналізу потокових шифрів гамування адитивного типу на прикладі шифру Віженера. Навчився шукати та знаходити довжину та значення ключа яким було зашифровано ШТ, та використовуючи його розшифровувати ШТ.*