НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ

«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО»

Навчально-науковий фізико-технічний інститут

КАФЕДРА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

«Криптографія»

Комп’ютерний практикум №2

Студенти: Маврикін Едуард

Слобода Ірина

Група: ФБ-25

Варіант 2

**Київ – 2025**

**Мета роботи:**

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

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.

Підібрано текст розміром 3132 символи (після очищення від пробілів та пунктуації)

Текст на російській мові, алфавіт m=32 символи

Ключі для шифрування:

Короткі ключі (r=2-5):

* - r=2: "ау"
* - r=3: "дно"
* - r=4: "куда"
* - r=5: "можно"

Довгі ключі (r=10-20):

* - r=10: "достижение"
* - r=11: "воображение"
* - r=12: "многообразие"
* - r=13: "автоматизация"
* - r=14: "взаимодействие"
* - r=15: "непосредственно"
* - r=16: "экспериментально"
* - r=17: "предусмотрительно"
* - r=18: "производительность"
* - r=19: "электрооборудование"
* - r=20: "антирадиолокационный"

Изображение выглядит как текст, снимок экрана, программное обеспечение, Шрифт

Содержимое, созданное искусственным интеллектом, может быть неверным.

Изображение выглядит как текст, программное обеспечение, снимок экрана

Содержимое, созданное искусственным интеллектом, может быть неверным.

Изображение выглядит как текст, снимок экрана

Содержимое, созданное искусственным интеллектом, может быть неверным.

Алгоритм шифрування:

y[i] = (x[i] + k[i mod r]) mod 32

Створено 15 файлів шифртекстів (cipher-2.txt ... cipher-20.txt)

Изображение выглядит как текст, снимок экрана

Содержимое, созданное искусственным интеллектом, может быть неверным.

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

Індекс відповідності (IC) обчислюється за формулою:

IC = (1/(n(n-1))) \* Σ N\_t(N\_t - 1)

де N\_t - кількість появ символу t у тексті.

Изображение выглядит как текст, снимок экрана, программное обеспечение, Мультимедийное программное обеспечение

Содержимое, созданное искусственным интеллектом, может быть неверным.

Результати:

Изображение выглядит как текст, снимок экрана, График, линия

Содержимое, созданное искусственным интеллектом, может быть неверным.

Изображение выглядит как текст, снимок экрана, программное обеспечение, Мультимедийное программное обеспечение

Содержимое, созданное искусственным интеллектом, может быть неверным.

1. IC відкритого тексту (0.0558) значно вище за теоретичне значення рівноімовірного алфавіту I₀=1/32≈0.0313

2. Зі збільшенням довжини ключа IC падає і наближається до I₀

3. При r≥10 IC стабілізується на рівні ~0.033-0.034

4. Це підтверджує, що шифр Віженера з довгим ключем добре маскує статистичні властивості мови

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

Крок 1. Визначення періоду ключа (Method 1)

Розбиття тексту на блоки для різних r і обчислення середнього IC:

Изображение выглядит как текст, линия, График, диаграмма

Содержимое, созданное искусственным интеллектом, может быть неверным.

Изображение выглядит как текст, снимок экрана

Содержимое, созданное искусственным интеллектом, может быть неверным.

Висновок: Виразні піки на r=7, 14, 21, 28. Це кратні 7 і 14. Ймовірний період: r=7 або r=14

Крок 2. Перевірка методом D(r) (Method 2)

Изображение выглядит как текст, График, линия, диаграмма

Содержимое, созданное искусственным интеллектом, может быть неверным.

Підрахунок кількості співпадінь символів на відстані r:

- D(r) показує кількість однакових символів на відстані r

- Для істинного періоду D(r) буде максимальним

Результат: Максимуми D(r) також на r=7, 14, 21, 28

Період найімовірніше r=14 (найбільший пік IC=0.0553)

Крок 3. Пошук ключа

Метод: Для кожного блоку Y₀, Y₁, ..., Y₁₃ знайти найчастішу букву і припустити що вона відповідає "о" (найчастіша буква російської мови).

Автоматично знайдений ключ: жосвеыдиадозор

Розшифрування: "уакисхчгжтосдефатес..." (не читається)

Крок 4. Коригування ключа

Аналізуючи структуру ключа "ос\_е\_ыдиадозо", можна припустити:

- "ос\_е" схоже на початок слова

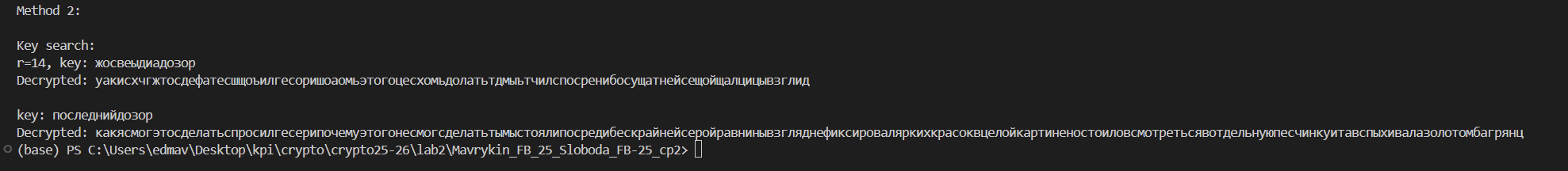
- "дозор" в кінці виглядає логічно

- Можливо слово: "последний" + "дозор"

Перевірка ключа: последнийдозор

Изображение выглядит как текст, снимок экрана, программное обеспечение

Содержимое, созданное искусственным интеллектом, может быть неверным.



Розшифрування:

какясмогэтосделатьспросилгесерипочемуэтогонесмогсделатьтымыстоялипосредибескрайнейсеройравнинывзгляднефиксироваляркихкрасоквцелойкартиненостоиловсмотретьсявотдельнуюпесчинкуитавспыхивалазолотомбагрянцем...

Це відрвок з книги Сергія Лук'яненка "Дозори: Останній Дозор"

1. Ефективність шифру Віженера: При довжині ключа r≥10 IC наближається до рівноімовірного розподілу, що ускладнює криптоаналіз

2. Метод визначення періоду: Обидва методи (середній IC блоків та D(r)) ефективно виявляють період ключа при достатньому обсязі шифртексту

3. Обмеження автоматичного пошуку: Припущення "найчастіша буква = о" не завжди справджується для окремих блоків. Потрібна ручна корекція або перебір варіантів

4. Практичне значення: Шифр Віженера з коротким ключем вразливий до частотного аналізу. Для надійності потрібен ключ довжиною близькою до довжини повідомлення