НАЦIОНАЛЬНИЙ ТЕХНIЧНИЙ УНIВЕРСИТЕТ УКРАЇНИ «КИЇВСЬКИЙ ПОЛIТЕХНIЧНИЙ IНСТИТУТ IМЕНI СIКОРСЬКОГО» ФIЗИКО-ТЕХНIЧНИЙ IНСТИТУТ

**Комп’ютерний практикум 2**

Виконали:

Толмачов Євгеній

Котович Анна

Перевiрив: Деркач О.Г.

Київ 2021

Вар 12 Вар 2

**Мета роботи:**

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

**Постановка задачі:**

1. Зашифрувати самостійно підібраний відкритий текст шифром Віженера з ключами довжини r = 2, 3, 4, 5, а також довжини 10-20 знаків.

2. Підрахувати індекси відповідності r I для відкритого тексту та всіх одержаних шифротекстів і порівняти їх значення.

3. Розшифрувати наданий шифртекст (згідно свого номеру варіанта). Визначити довжину ключа; визначити символи ключа, прирівнюючи найчастіші літери у блоці до найчастішої літери у мові; визначити символи ключа за допомогою функції M(g) i ; розшифрувати текст, використовуючи знайдений ключ.

**Хід роботи:**

Першим чином було зашифровано ключами ріжної довжини текст та пораховані індекси відповідності для відкритого та зашифрованих текстів. Виникли невиличкі непорозуміння при підрахуванні коефіцієнтів Di. Для 12 варіанту проблем ніяких в процесі розшифрування не виникло. Для інших варіантів, не залежно від розміру ключа (добре, залежно, для ключів більше наче 21 символів треба переписувати кілька строчок коду), знаходження ключа також працює, але з якоїсь причини ключ зміщен (нийдозорпослед), причому кожний варіант, навіть з ключем однакового розміру, має різне зміщення. Підозрюю що пов’язано з дуже близькими значеннями функції M(g). Треба це брати до уваги. Код, зашиврований та розшифровані файли ~~прикріплені до листа~~ ~~та~~ знаходятся за посиланням <https://github.com/ZheZheDoshka/labs_2021_5/tree/main/%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%B02>.

I0 = 0.0580902

I2 = 0.0476006

I3 = 0.0423937

I4 = 0.0388384

I5 = 0.0356905

I10 = 0.034781

I12 = 0.033585

I20 = 0.0329171

Чугунныенебеса – ключ для варіанту 12

ПоследнийДозор – ключ для варіанту 2



