Міністерство освіти і науки України
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Фізико-технічний інститут

Симетрична Криптографія

Комп’ютерний практикум 2

Криптоаналіз шифру Віженера

Варіант 4

Виконав:
Студент гр. ФІ-03 Волинець С. А.

Київ — 2023

Мета роботи

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

Постановка задачі

1. Уважно прочитати методичні вказівки до виконання комп'ютерного прак тикуму.
2. 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.
3. Підрахувати індекси відповідності Ir для відкритого тексту та всіх одер жаних шифротекстів і порівняти їх значення.
4. Використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст (згідно свого номеру варіанта). Зокрема, необхідно:
    a. визначити довжину ключа, використовуючи або метод індексів відповідності, або статистику співпадінь Dr (на вибір);
    b. визначити символи ключа, прирівнюючи найчастіші літери у блоці до найчастішої літери у мові;
    c. визначити символи ключа за допомогою функції Mi(g);
    d. розшифрувати текст, використовуючи знайдений ключ; в разі необхідності скорегувати ключ.

Вступ

Для виконання даної лабораторної роботи я скористався засобами такої мови програмування як python.

Вцілому, як на мене, даний практикум простий, хоча й вимагає багато часу на реалізацію. Найбільша проблема у мене була пов'язана з тим, що я не дуже розумію, що означає фраза: "сукупність значень схиляється до значення" при обчислені довжини ключа. Я вирішив, що я просто знайду середнє значення у сукупності і буду його порівнювати.

Обчислення значень індексів відповідності

Для виконання завдання я вибрав декілька ключів для шифрування. А саме:
"аб", "вгд", "бвгд", "жзийк", "абвфтмглжсщлгдежзийк".

Даними ключами я зашифрував якийсь, випадково знайдений в мережі інтернет текст написаний російською мовою.

Після цього, я обчислив значення індексів відповідності:

Ключ	Розмір ключа	Значення
Початковий текст	—	0.0591
аб	2	0.0473
вгд	3	0.0434
бвгд	4	0.0425
жзийк	5	0.0411
абвфтмглжсщлгдежзийк	20	0.0340

Розшифрування шифро-тексту заданого, 4 варіанту

Для пошуку ключа використовувався метод індексів відповідності. Ось отримані значення для пошуку довжини ключа:

Теоретична довжина ключа	Індекс відповідності
2	0.032604641533356106
3	0.03257699135676468
4	0.032650882017613285
5	0.032535443566457684
6	0.03256047474074616
7	0.03271784961796955
8	0.03269169199663074
9	0.032514372292478666
10	0.03251756583831643
11	0.03271373565919388

12	0.032635472926334196
13	0.05406857059071756

Отже: виявляється, що довжина ключа рівна 13.
Тепер будемо знаходити сам ключ та розшифруємо повідомлення.

Перший метод, метод пошуку найчастішої літери в тексті зав наступні результати:
Ключ: “громыкавьдума”
Текст:
стармиысуаишколачарьдоелпифийитровцияфакультеатоощетическочишрйктическочмйгси кафедраъамолпрактикорчйсыьперваясьцсафьныйуклатбдтснравывамэищьойобщинывцкй чыовычтотоцмоеыепротиввомшищоврасприыкчршорациямивкьръоваярабоаайдоптк…

Другий метод дав значно кращі результати:

Ключ: громыковедьма
Текст:
старминскаяшколачародеевпифийитравницфакультеттеоретическойипрактическоймагиик афедрамаговпрактиковчастьперваясоциальныйукладбытинравывампирьейобщинывикачт овычтотоимеетепротиввампировраспринкорпорациямифкурсоваяработаадептквивосьмогок урсавольхиреднойнаучныйруководительмагистрпервойстепениархимагксанперловдевятьс отдевяностодевятыйгодпобелорскомулетосчислениюгородстарминведение…

Мої знання російської мови, говорять, що ключ “громыковедьма” правильний, бо текст, як на мене правильний.

Висновки

Шифр Віженера гарний, але його легко зламати якщо річ йде про живу мову. Саме тому, його не слід використовувати.