Криптографія

Комп’ютерний практикум №2
Криптоаналіз шифру Віженера

Варіант 10

Виконав: студент групи ФБ-91
Кузавка Артем

Київ – 2021

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. 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.

Відкритий текст для шифрування: "plaintext.txt".

Зашифруємо відкритий текст за допомогою створеної програми для шифрування шифром Віженера: "VigenereCryptor.py". Приклад використання для шифрування файлу "plaintext.txt" ключем "ab":

```
# python3 VigenereCryptor.py plaintext.txt ab
```

Розшифруємо закритий текст за допомогою створеної програми для розшифрування шифром Віженера: "VigenereCryptor.py". Приклад використання для шифрування файлу "plaintext.txt" ключем "ab":

```
# python3 VigenereDecryptor.py ciphertext.txt ab
```

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

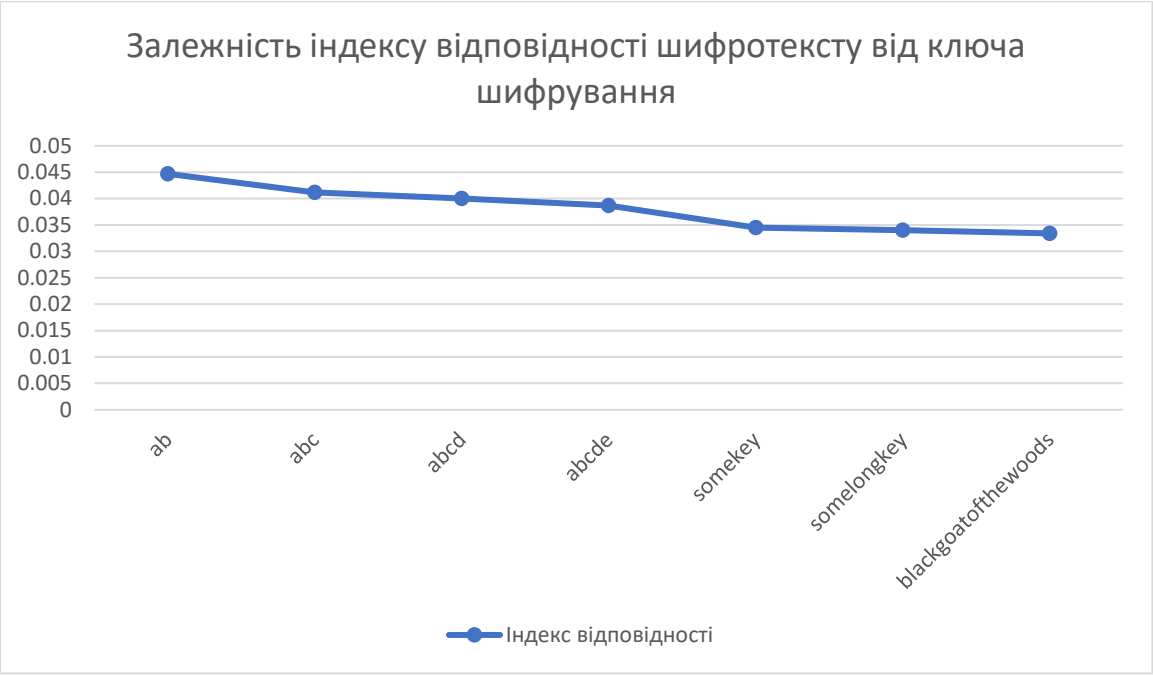
Розрахунок індексу відповідності для шифротексту відбувався за добпомогою спеціально створеної програми "indexCalculator.py". Демонстрація її роботи:

```
# python3 indexCalculator.py ciphertext_ab.txt
Index =  0.04467638777822765
```

Індекси відповідності отриманих шифротекстів:

Ключ	Індекс відповідності шифротексту
ab	0.04467638777822765
abc	0.04117265132748057

abcd	0.039997307183736085
abcde	0.03867929759588785
somekey	0.034501780458976214
somelongkey	0.03399555598823426
blackgoatofthewoods	0.03340255017965083



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

Для визначення довжини ключа була створена програма “VigenereCracker2000.py”, що використовує метод пошуку досить довгих (у даному випадку – 3 літери) послідовностей у шифротексті які повторюються та розрахунку довжини тексту, через яку вони повторюються.

Вивід програми включає можливий варіант ключа, що був розрахований методом частотного аналізу, кількості повторень послідовностей з трьох літер та відстані між ними. Щодо додаткового функціоналу визначення ключа, він розраховується з використанням довжини ключа, яку потрібно вносити в код програми вручну.

Робота з програмою “VigenereCracker2000.py”:

```
# python3 VigenereCracker2000.py ciphertest_var_10.txt
Possible key: крадущяйгявтени

{'гчт': 6, 'кус': 5, 'здк': 4, 'сою': 3, 'зиш': 2, 'к\n': 1}
Search for the common divisor for:
гчт
120
90
690
2371
```

```
689
кус
60
390
1560
300
здк
960
210
31
сою
150
255
зиш
87
```

Після цього, методом визначення читабельності розшифрованого тексту, в ключі, що був розрахований програмою “VigenereCracker2000.py”, змінювалися деякі літери, щоб покращити читабельність тексту. Після декількох змін було отримано ключ:

крадущийсявтени

Розшифрування шифротексту за допомогою програми “VigenereDecryptor.py”:

```
# python3 VigenereDecryptor.py ciphertest_var_10.txt крадущийсявтени
# cat plaintext.txt
Тихотактихочтослышнокакмотылькицепляютсяхрупкимикрылышкамизаночнуюпрохлад
упораужеотправлятьсяпосвоимделамстражадавнопрошланоясегоднячтотослишкомос
торожничаюнекоенеобъяснимоечувствозаставляетменязадержатьсявозлестеныздан
ияпогруженноговтеньтеньмояподругамоялюбовницамоянапарницаяпрячусьвтенияжи
вувнейтолькоонавсегдаготовапринятьменяспастиотстрелзлобносверкающихвлунно
йночиклинковилиоткровожадныхзолотыхглаздемоновтенькакговоритдобрыйжрецсаг
ота
...
```

Висновки

Після виконання даного комп’ютерного практикуму, я засвоїв методи частотного криптоаналізу. Також я здобув навички роботи та аналізу потокових шифрів гамування адитивного типу на прикладі шифру Віженера.

Контрольні запитання

1. На які види поділяються класичні шифри? У чому між ними відмінність?
   На шифри підстановки та перестановки. На мою думку, основна відмінність між ними (окрім принципу роботи) – це те, що перші вразливі до частотного аналізу (особливо моноалфавітні).
2. Що таке шифри моно- та поліалфавітної підстановки?
   Це шифри підстановки, використання моноалфавітої підстановки означає те, що кожна літера замінюється однозначно та кожен раз однаково. Для поліалфавітної підстановки, літера не замінюється кожен раз тією ж само.
3. Що таке шифр Віженера?
   Шифр Віженера – це шифр поліалфавітної підстановки, ключем для якого є слово або уривок тексту. Для шифрування до кожної букви відкритого тексту

додається відповідка буква з ключа, коли букви в ключі закінчуються, знову починають з першої його букви. Розшифровка проходить зворотнім способом – буква з ключа віднімається від букви шифротексту.

4. Що таке індекс відповідності?
   Це метод криптоаналізу шифру Віженера, він позначає ймовірність того, що дві частини тексту збіжаться.
5. Чому не потрібно підраховувати індекс відповідності для шифртексту з r=1? Чому він дорівнює?
   Тому що такий шифртекст складається з одного символу, що повторюється, це не має сенсу. Довжині тексту.
6. Яка модель відкритого тексту розглядається при криптоаналізі шифру Віженера? З 32 літерами, без пробілів, всі літери маленькі.
7. Завдяки чому можливий криптоаналіз шифру Віженера?
   Ключ значно менший за довжину тексту й тому сукупність кожної n-ї літери, де n – довжина ключа, зберігає частотний розподіл літери мови, на якій написаний відкритий текст.
8. Що таке частотний аналіз?
   Це метод криптоаналізу, при якому після аналізу частот літер у шифротексті, вона зіставляється з частотою літер у мові, якою написаний відкритий текст та на основі цього проходить розшифрування шифротексту.