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

Лабораторна робота №2

З дисципліни «Криптографія»

Виконали:

студенти 3 курсу ФТІ
групи ФБ-83
Волинко Д.В.
Бондаренко.Р.С.

Перевірив:

Чорний О. М.

Вариант - 5

Мета роботи:

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

Порядок виконання:

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)Ознайомилися з теоретичними відомостями та всіма вказівками.

2)Підготували текстовий файл розміром 3Кб для першого завдання (EncriptionText.txt).

3)Далі ми зашифрували текст з різними ключами , та порахували індекси відповідності для відкритого тексту та зашифрованих текстів.

Индекс соотвествия ВТ - 0.05549296441520718 для обранного тексту

Индекс соотвествия ШТ - 0.04486943797006428 для першого ключа

Индекс соотвествия ШТ - 0.04105011960440199 для другого ключа

Индекс соотвествия ШТ - 0.03778844101474191 для третього ключа

Индекс соотвествия ШТ - 0.03676068539297959 для четвертого ключа

Индекс соотвествия ШТ - 0.0345510076327341 для п'ятого ключа

4)Обрали варіант шифрованого тексту, розбили текст на блоки з різними періодами, потім порахували індекси відповідності для кожного блоку, згідно цих даних було встановлено довжину ключа, яка становить 16

r = 2, Индекс соответствия - 0.033631268875074165;

r = 3, Индекс соответствия - 0.03570226108032251;

r = 4, Индекс соответствия - 0.03452251797910123;

r = 5, Индекс соответствия - 0.03531192705774224;

r = 6, Индекс соответствия - 0.03395206632390157;

r = 7, Индекс соответствия - 0.03578339575530587;

r = 8, Индекс соответствия - 0.045355614428367635;

r = 9, Индекс соответствия - 0.03678394657114987;

r = 10, Индекс соответствия - 0.03303412274000509;

r = 11, Индекс соответствия - 0.03473939674101468;

r = 12, Индекс соответствия - 0.034068246776520754;

r = 13, Индекс соответствия - 0.03838558247450494;

r = 14, Индекс соответствия - 0.035363408521303256;

r = 15, Индекс соответствия - 0.035698412925979556;

r = 16, Индекс соответствия - 0.05347523536635285;

r = 17, Индекс соответствия - 0.03409781707654048;

r = 18, Индекс соответствия - 0.032527746084431076;

r = 19, Индекс соответствия - 0.0327683615819209;

r = 20, Индекс соответствия - 0.03402457757296467;

r = 21, Индекс соответствия - 0.03674917631156543;

r = 22, Индекс соответствия - 0.03189748340280994;

r = 23, Индекс соответствия - 0.03767793294204952;

r = 24, Индекс соответствия - 0.04358443096048542;

r = 25, Индекс соответствия - 0.03451313260730301;

r = 26, Индекс соответствия - 0.034905455335796566;

r = 27, Индекс соответствия - 0.03470756531119554;

r = 28, Индекс соответствия - 0.03557788944723618;

r = 29, Индекс соответствия - 0.036431347150259065;

r = 30, Индекс соответствия - 0.033925593697889715;

r = 31, Индекс соответствия - 0.03161448741559239;

5)В кожному з блоків визначили найбільш зустрівану букву та зіпоставили її з найпопулярнішою буквою в алфавіті.

6)Зайшли розшифровку блоків по найчастішим літерам:

For о :девелииоборойдей

For е :нолофссчкчщчтнот

For а :турущццьпьюьчтуч

For и :клилсоофзфцфпклп

For н :ежгжмййпвпспкежк

For с :бвявиеелюлнлжбвж

For т :абюбзддкэкмкеабе

For р :вгагйжжмямомзвгз

На основі чого робимо висновок, що ключ - *делолисоборотней*

Розшифруємо текст та знайдемо індекси відповідності для шифрованого і розшифрованого текстів для п'ятого варінту:

Индекс соответствия дли шифрованого текста 5-го варианта - 0.03532444245066751

расшифрованого - 0.05548687137872912

Висновок: у цій роботі ми отримали навички криптоаналізу простих шифрів. Було зашифровано шифром Віженера кілька власних зразків та дешифровано один зразок для нашого варіанту.