

Криптографія

Лабораторна робота 2. Криптоаналіз шифру Віженера

ФБ-13 Ігнатенко Данило

Варіант 5

Мета роботи

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

Задача

0. Прочитати методичку. Тричі
1. Вибрати шматок тексту з першої лаби, щоб не шукати новий (з поправками на наявність літери "ь")
2. Написати програму, що зашифровує та розшифровує текст шифром Віженера і зашифрувати текст обраними ключами довжини 2, 3, 4, 5 та 10-20 символів
3. Порівняти індекси відповідності для відкритого та зашифрованих текстів
4. З новими знаннями і силами розшифрувати наданий за варіантом шифротекст

Хід роботи

Для відкритого тексту довжини 2-3 кб був взятий відповідний шматок з трохи зміненого тексту, що використовувався у першій лабі, зокрема я просто підрізав два рядки у функції переформатування, що видаляли твердий знак, і пройшовся нею по тексту, після чого прибрав пробіли

Ключі обрані наступні: ио, осе, буер, зепар, рыбонуклеиновый. Імен довжини 2 в Гостії не було, а довжини 10-20 починалися на "А", що для ключа так собі

Спершу були написані функції, що видають номер літери і літеру за номером, працює на основі рядка з алфавітом і безмежних приколів пітона. Далі функції шифрування/розшифрування, які потім об'єдналися в одну з додатковим параметром. Останніми були функції для підрахунку індексу відповідності

Труднощі

Написати нормально протокол. Лаба, як на мене, легша та цікавіша за попередню, тому сидіти і писати зараз протокол – найскладніша і найнудніша частина

Шляхи розв'язання

Завжди є

Результати

Повний відкритий текст збережений у файлі fulltext.txt (щоб порахувати частоти літер), його частинка на 3 кб – у файлі sample.txt, результати шифрування – у файлах key2.txt, key3.txt, key4.txt, key5.txt та keylong.txt відповідно, шифротекст за варіантом – у файлі ciphertext5.txt, проміжні та остаточний результати розшифрування збережені у файлах ct1.txt, ct2.txt та ct3.txt відповідно. Пробіли між частинами розставлялися руками для легкості читання

Отримали теоретичне значення індексу відповідності 0.056, а практично порахували 0.058, що доволі близько. При порівнянні індексів видно стрімкий спад, проте його швидкість спадання зменшується теж дуже швидко

```
(base) C:\Users\uranus\Desktop\Crypt\ihnatenko_fb-13_cp2>python lab2.py
Теоретичне значення індексу відповідності повного тексту: 0.05586932290323541
Практичне значення індексу відповідності зразка: 0.05776291402132586
Індекс відповідності шифротексту з ключем "ио": 0.044934767142034975
Індекс відповідності шифротексту з ключем "оце": 0.03972338911773636
Індекс відповідності шифротексту з ключем "буер": 0.03924666131933965
Індекс відповідності шифротексту з ключем "зепар": 0.03589869081120763
Індекс відповідності шифротексту з ключем "рыбонуклеиновый": 0.033746165105519074
```

Було розраховано індекси відповідності шифротексту з припущенням довжин ключів від 2 до 30. Стрімкий спад значення при неправильній довжині швидко дає зрозуміти, що був використаний ключ довжини 16

Індекси відповідності шифротексту з припущенням довжини ключа

```
(2, 0.03709682620655367)
(3, 0.03535245194471151)
(4, 0.039793511667390036)
(5, 0.0354351293936251)
(6, 0.037052368586566846)
(7, 0.03522360497899179)
(8, 0.04491213203766699)
(9, 0.03545025157077616)
(10, 0.03709763005817014)
(11, 0.03506214646542888)
(12, 0.0397888484387092)
(13, 0.03550919719241092)
(14, 0.037093872461702884)
(15, 0.035384371390931875)
(16, 0.05539766505382552)
(17, 0.035524349460576386)
(18, 0.037051140206933175)
(19, 0.03531599104429486)
(20, 0.03979839848540342)
(21, 0.035056696947883076)
(22, 0.03688094981192191)
(23, 0.03526676001305198)
(24, 0.04486292731353409)
(25, 0.03531687664602463)
(26, 0.03731086887465935)
(27, 0.035247591055245484)
(28, 0.03969086727168179)
(29, 0.035584903885058694)
(30, 0.036928328869868694)
```

Найімовірніша довжина ключа: 16

Літери для ключа підбиралися доволі просто: рахували топ-3 літери у блоці по частоті і припускали, що це "о". Від порядкового значення літери блоку віднімалося порядкове значення літери "о" і отримувалося припущення для літери ключа

```
Варіанти найімовірніших літер для ключа
['д', 'ы', 'г']
['е', 'д', 'я']
['в', 'к', 'е']
['е', 'и', 'о']
['л', 'в', 'э']
['и', 'я', 'в']
['и', 'с', 'р']
['о', 'е', 'и']
['б', 'ш', 'ы']
['о', 'е', 'а']
['р', 'у', 'з']
['о', 'е', 'н']
['й', 'т', 'м']
['д', 'н', 'я']
['е', 'ь', 'в']
['й', 'г', 'а']
```

уюистинуз сеццшиу ерноелучш йьрьомц бытонибыл
ийиуделяю ццэьцды овнимания икэнчцв обеннодет
орясьхьиимтолишьбчйпотхсеткакимпрмьюлфгакинест
тилающаяндйшцчрябщепроходмсжуоигинауканихтчкпжя

уушн тноеделокуль цыб
тванесделалохбвуловекус
епятхчнцемнанообъятняь

Текст став більш змістовним, припущення виявилось правильним. Крім того, одразу пізнається шматочок фрази "понятное дело", тому припускаємо, що частинка "уушн" була в оригіналі "поня" і пробуємо розшифрувати текст отриманим ключем "делолисорботней"

понятное дело культуру насильно человек не воткнешь в голову и этак удовольствия грустную
тто много численные подразделения палаты церемоний и уделяют столько внимания д
немало людей которым пока им толишь будда знает как им причинам так не стало интересно
чно пребывает настилающая над ними общепроходимые гати науки хотя бы чисто простое
но понимание этого слова и старик обозначавшего людей иной неордусской культуры аск
й воспитанности бросается здесь в глаза даже невнимательному наблюдателю человек сд
овземлю после чего спокойно достать из рукава дорожной расшитый платок и утереть нос
ым властям в эти духовные области путь заказан насильно и не вместишь аувещание запозда
к правило оказывался здесь лишь по служебной надобности вот как сегодня несмотря на пр

Отримали зрозумілий російський текст, а отже, ключ знайдено. До речі, дякую, це вдруге, коли у нас замість sampletext чи аналогів в завданнях використовується щось змістовне, типу назв музики або, як цього разу, назв і тексту книг, і від цього робити їх стає якось приємніше

Висновки

Протягом роботи ми розібралися з поняттям індексу відповідності, а також дізналися, як його можна застосувати на практиці, зокрема розшифрувати текст, зашифрований шифром Віженера. Також звернули увагу на кілька ознак самого шифру, наприклад на факт частого повторення літер на відстанях, рівних довжині ключа