Національний технічний університет України «КПІ» імені Ігоря Сікорського
Фізико-технічний інститут

Лабораторна робота 2

Криптографія

Виконали:

студенти ФБ-14

Кот Микита Сергійович

Чавалах Артем Дмитрович

Перевірила:

Селюх П. В.

Мета роботи

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

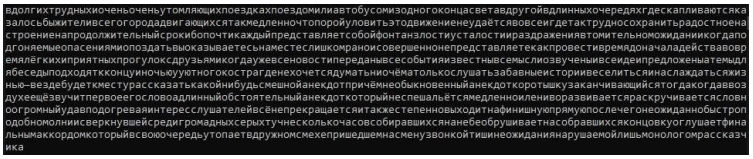
Порядок виконання роботи

0. Уважно прочитати методичні вказівки до виконання комп’ютерного практикуму.

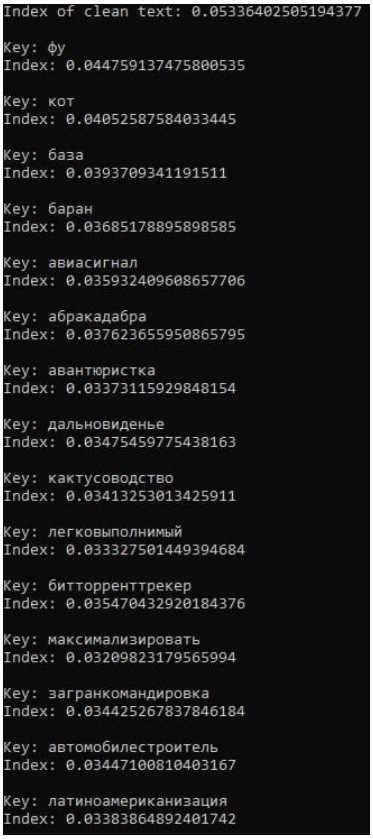
1. Самостійно підібрати текст для шифрування (2-3 кб) та ключі довжини r = 2, 3, 4, 5, а також довжини 10-20 знаків. Зашифрувати обраний відкритий текст шифром Віженера з цими ключами.

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

Відредагований текст (без пробілів, ловеркейс, розділових знаків).



Шифрування шифром Віженера з ключами:



Як можна побачити, спочатку індекс відповідності великий, коли маємо чистий текст та при меньшому значенні ключа. Коли ключ стає більшим, індекс зменшується зі збільшенням ключа стає більш-менш однаковим.

3. Використовуючи наведені теоретичні відомості, розшифрувати наданий

шифртекст (варіант 9).

Спочатку визначаємо індекс відповідності зашифрованого тексту. Потім визначаємо індекс для різних r.

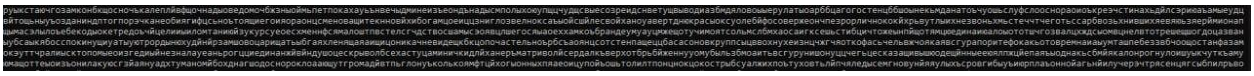
```
Index of encrypted text: 0.0328460148020796

Index for r=1: 0.0328460148020796
Index for r=2: 0.03288907383913786
Index for r=3: 0.03280270806685515
Index for r=4: 0.032776586401747916
Index for r=5: 0.03281053998522203
Index for r=6: 0.032805493488069416
Index for r=7: 0.03272796104838353
Index for r=8: 0.03283440009895609
Index for r=9: 0.03269883173876473
Index for r=10: 0.03285327344856936
Index for r=11: 0.03276673213881401
Index for r=12: 0.032616530753538216
Index for r=13: 0.032876786821307354
Index for r=14: 0.03278042052494595
Index for r=15: 0.03262709665317097
Index for r=16: 0.03304101176307603
Index for r=17: 0.05539037433155081
Index for r=18: 0.03262856070999888
Index for r=19: 0.03288426955603722
Index for r=20: 0.03255886368565288
Index for r=21: 0.03281434392668897
Index for r=22: 0.03286955316619862
Index for r=23: 0.032783212941565554
Index for r=24: 0.032637774210807914
Index for r=25: 0.03271734599351552
Index for r=26: 0.033028484053788214
Index for r=27: 0.032470414513807624
Index for r=28: 0.03256476584763565
Index for r=29: 0.03294449398258896
Index for r=30: 0.032496753050019894
Index for r=31: 0.03270273941847026
Index for r=32: 0.033009000177655956
```

Бачимо, що індекс для r=17, значно відрізняється від усіх інших.

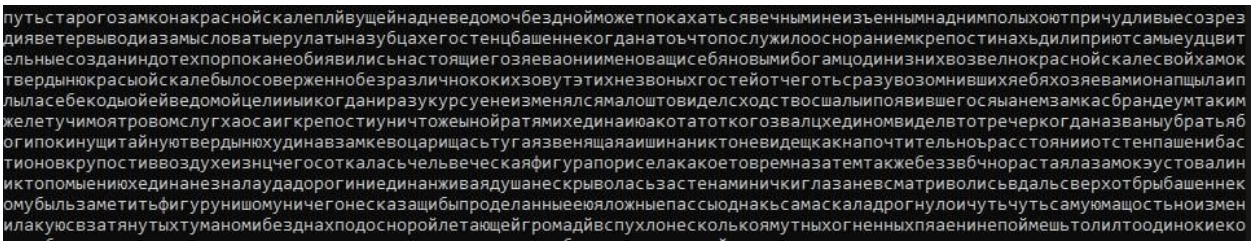
Знаходимо ключ для цього значення.

```
боаяамахчэндшпиэь
```

Тепер розшифруємо текст цим ключем.



Отримали не дуже зрозумілий текст. Потім спробували змінити букву э на букву л, бо слово «эндшпиль» було найочевиднішим варіантом. Після цього намагалися заміняти різні літери, щоб виходили якісь слова, і через достатньо великий проміжок часу розшифрований текст ставав більш зрозумілим і читабельним. Нарешті, прийшли до ключа: «войнамагаэндшпиль».



Труднощі

У ході виконання лабораторної роботи зіткнулися із труднощами з визначенням ключа для зашифрованого тексту. Була невелика проблема із відступами в зашифрованому тексті, не одразу їх помітили. Дуже довго і складно визначали ключ: змінювали по одній літері, дивились на результат и намагались зрозуміти слова в тексті.

Висновки

У ході виконання лабораторної роботи, ми набули практичних навичків щодо шифрування та розшифрування текстів шифром Віженера, оцінили значення індекса відповідності при маленькому та більшому розмірі ключа. На реальному прикладі розшифрували текст, знайшли ключ.