**КРИПТОГРАФІЯ**

**КОМП’ЮТЕРНИЙ ПРАКТИКУМ №2**

**Криптоаналіз шифру Віженера**

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

**Порядок виконання роботи:**

1. Уважно прочитати методичні вказівки до виконання комп’ютерного практикуму.
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 для відкритого тексту та всіх одержаних шифртекстів і порівняти їх значення.
4. Використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст (згідно свого номеру варіанта).

**Хід роботи:**

1. Зашифруємо текст шифром Віженера.

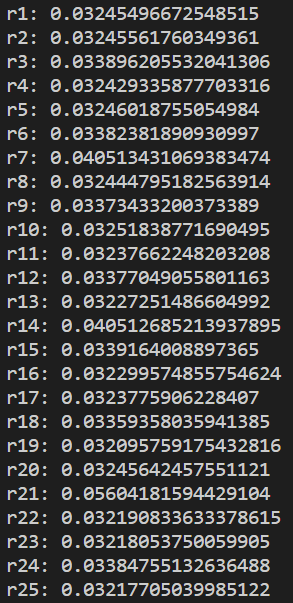
Ключі:

|  |  |
| --- | --- |
| r | Ключ |
| 2 | ви |
| 3 | жен |
| 4 | шифр |
| 5 | текст |
| 10 | шифротекст |
| 15 | ходлабораторной |
| 20 | методовкриптоанализа |

2. Порахуємо індекси відповідності:

|  |  |
| --- | --- |
| Текст | Індекс відповідності |
| Відкритий | 0.055948665211298945 |
| r=2 | 0.04386069364509475 |
| r=3 | 0.03891484896049458 |
| r=4 | 0.03648883516457082 |
| r=5 | 0.036951906712131874 |
| r=10 | 0.03439960067596418 |
| r=15 | 0.03498415333080749 |
| r=20 | 0.033147503322688704 |

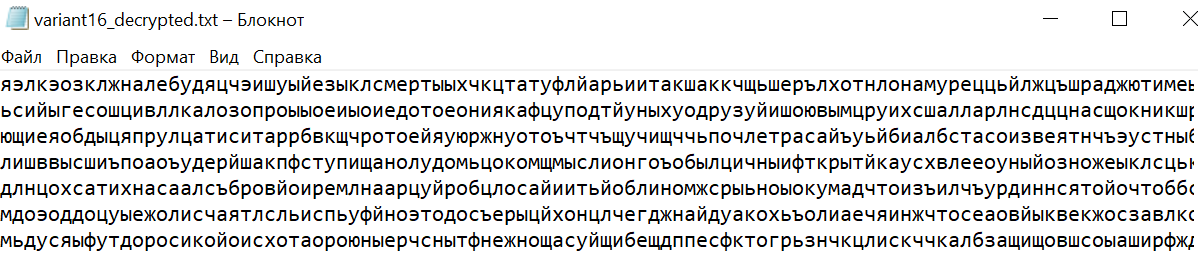
3. Знайдемо довжину ключа:



Схоже що ключ довжини 21, тому що індекс відповідності для 21 найблищий до відкитого тексту.

4. Спробуємо знайти ключ. Для цього розіб’ємо текст на 21 блок та порахуємо кількість літр у кожному блоці. Зробімо припущення, що літра яка зустрічається найчастіше в кожному блоці – це зашифрована літра "о". На основі цього отримуємо ключ:

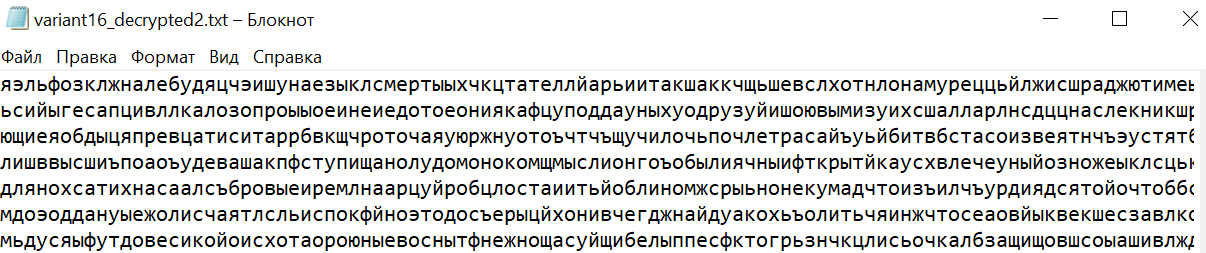




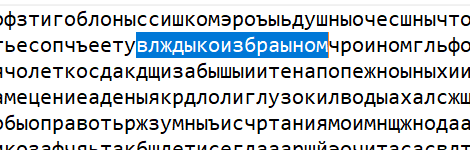
Текст все ще незрозумілий, тому я зробув припущення, що перше слово в ключі "башня".

Новий ключ і текст:





Текст все ще незрозумілий, але, погортавши трохи далі, я побачив цікавмй фрагмент:



Схоже що перше слово має бути "владыка" або "владыки" або "владык о", а друге слово однозначно "избранном". Тобто мені потрібно щоб замість "ж" була "а", а замість "ы" – "н". Після деяких розрахунків я зрозумів, що мені потрібно змінити 16-ту та 6-ту літри в ключі.

Отримали новий ключ – "башняяросмичерныемчбъ". Тут я вже побачив, що ключ – "башня ярости черные ...". І після невеличкого пошуку в Гугл, я дізнався, що останнє слово "маки". Таким чином повний ключ – "башняяростичерныемаки".

**Висновок:**

В ході цієї лабораторної я дізнався про індекс відповідності та навчився використовувати частотний аналіз для розшифрування шифру Віженера.