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:

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. 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

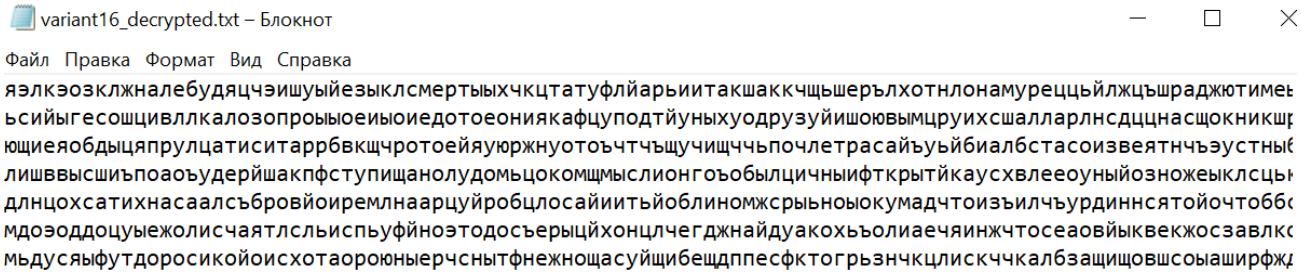
3. Знайдемо довжину ключа:

```
r1: 0.03245496672548515
r2: 0.03245561760349361
r3: 0.033896205532041306
r4: 0.032429335877703316
r5: 0.03246018755054984
r6: 0.03382381890930997
r7: 0.040513431069383474
r8: 0.032444795182563914
r9: 0.03373433200373389
r10: 0.03251838771690495
r11: 0.03237662248203208
r12: 0.03377049055801163
r13: 0.03227251486604992
r14: 0.040512685213937895
r15: 0.0339164008897365
r16: 0.032299574855754624
r17: 0.0323775906228407
r18: 0.03359358035941385
r19: 0.032095759175432816
r20: 0.03245642457551121
r21: 0.05604181594429104
r22: 0.032190833633378615
r23: 0.03218053750059905
r24: 0.03384755132636488
r25: 0.03217705039985122
```

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

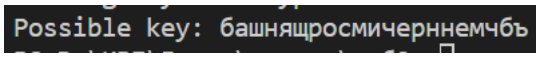
4. Спробуємо знайти ключ. Для цього розіб’ємо текст на 21 блок та порахуємо кількість літр у кожному блоці. Зробімо припущення, що літра яка зустрічається найчастіше в кожному блоці – це зашифрована літра "о". На основі цього отримуємо ключ:

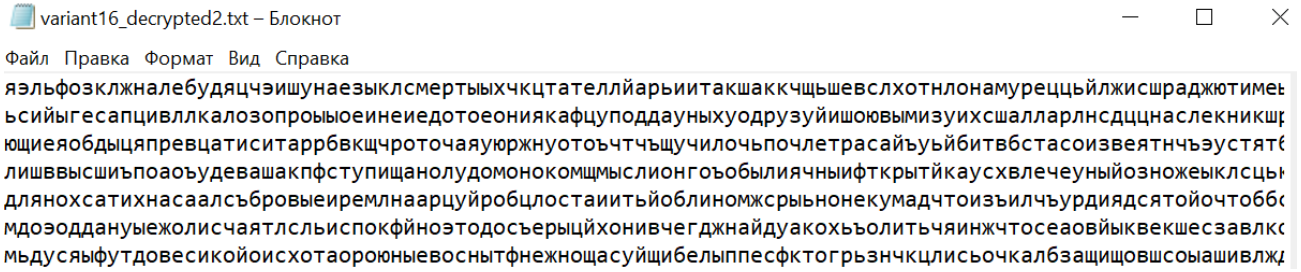
```
Possible key:башяцщросмичерннемчбъ
```



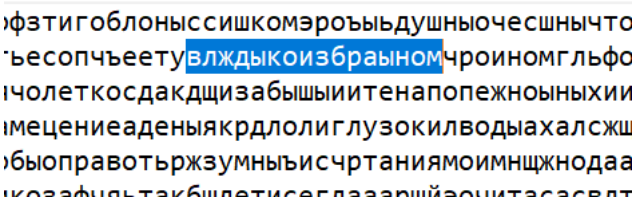
Текст все ще незрозумілий, тому я зробув припущення, що перше слово в ключі "башня".

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.