**Міністерство освіти і науки України**

**Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського"**

**Фізико-технічний інститут**

КРИПТОГРАФІЯ

КОМП’ЮТЕРНИЙ ПРАКТИКУМ №2

Криптоаналіз шифру Віженера

Виконали студенти групи ФБ-23:

Кушнарьов Данііл та Присєвок Оксана

Київ - 2024

**Мета роботи:**

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

**Хід роботи:**

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.

Візьмемо очищений текст з першого практикуму alice.txt. Напишемо python скрипт для шифрування тексту

Зображення, що містить текст, знімок екрана, Шрифт, дизайн

Автоматично згенерований опис

Результат роботи скрипту

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

|  |  |
| --- | --- |
| r | Індекс відповідності |
| 0 | 0.056068885604446096 |
| 2 | 0.043673001963028306 |
| 3 | 0.039348326727504775 |
| 4 | 0.0338853889680147 |
| 5 | 0.036760750911957525 |
| 10 | 0.033915491956681615 |
| 11 | 0.03316810089075136 |
| 12 | 0.03280935328828137 |
| 13 | 0.03272622555717658 |
| 14 | 0.03264492789228932 |
| 15 | 0.03226036027642827 |
| 16 | 0.03218618448749635 |
| 17 | 0.032177411047408094 |
| 18 | 0.03222342516415893 |
| 19 | 0.03213328181400982 |
| 20 | 0.03229078873796835 |

3. Використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст (згідно свого номеру варіанта).