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

КРИПТОГРАФІЯ

КОМП'ЮТЕРНИЙ ПРАКТИКУМ №2

Криптоаналіз шифру Віженера.

Варіант – 10

Виконав:
студент III курсу ФТІ
групи ФБ-95
Колесник Вікторія
студент III курсу ФТІ
групи ФБ-96
Ліпатова Софія
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.

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

Хід роботи

В якості тексту для шифрування був взятий уривок роману «Фауст» Гётте. Труднощі виникли на етапі отримання ключа, де осмисленність ключа псувалась однією літерою. Проблема була вирішена за допомогою автоматизованої підстановки наступних за популярністю літер алфавіту у формулу $k = (y^* - x^*) \bmod m$

Індекси відповідності

```
i = 1371533.5129660885
```

```
i = 82197.90960451978
```

```
i = 77703.08615819209


i = 72310.89689265536


i = 80680.98163841809
i = 74647.24576271187
```

Текст, який було обрано для шифрування:

Как принято считать, базовые сценарии поведения пользователей набирают популярность среди определенных слоев населения, а значит, должны быть в равной степени предоставлены сами себе. В рамках спецификации современных стандартов, явные признаки победы институционализации в равной степени предоставлены сами себе. Сложно сказать, почему некоторые особенности внутренней политики призывают нас к новым свершениям, которые, в свою очередь, должны быть подвергнуты целой серии независимых исследований. Внезапно, действия представителей оппозиции представляют собой не что иное, как квинтэссенцию победы маркетинга над разумом и должны быть объективно рассмотрены соответствующими инстанциями. С другой стороны, выбранный нами инновационный путь выявляет срочную потребность стандартных подходов. Не следует, однако, забывать, что понимание сути ресурсосберегающих технологий выявляет срочную потребность системы обучения кадров, соответствующей насущным потребностям. Высокий уровень вовлечения представителей целевой аудитории является четким доказательством простого факта: высокое качество позиционных исследований позволяет выполнить важные задания по разработке новых принципов формирования материально-технической и кадровой базы. Господа, реализация намеченных плановых заданий говорит о возможностях вывода текущих активов. Имеется спорная точка зрения, гласящая примерно следующее: активно развивающиеся страны третьего мира лишь добавляют фракционных разногласий и своевременно верифицированы. Следует отметить, что курс на социально-ориентированный национальный проект говорит о возможностях приоритизации разума над эмоциями.

Ключи шифрування:

```
r = ['ка', 'при', 'зова', 'попул', 'евнаселенияаз']
```

Відповідні зашифровані тексти можна знайти у репозитерії під назвами “0..4.txt”

Висновки: в ході виконання компьютерного практикуму мною були досліджені методи розшифрування тексту зашифрованного шифром Віженера. Також було обрано один із методів и відвтворенно на мові програмування python. У ході розшифрування був використан метод співставлення індексів відповідності для відтворення довжини ключа, та розшифрування серії шифртекстів закодованних шифром цезаря, за допомогою частотного аналізу.