Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет информатики и радиоэлектроники

Факультет информационных технологий и управления
Кафедра интеллектуальных информационных технологий

Отчет по лабораторной работе №2
по курсу “Средства и методы защиты информации в интеллектуальных системах”
Вариант 2

Выполнил:
Студент гр. 321703 Батук Д.С.

Проверил: Сальников Д.А.

Минск 2025

ЛАБОРАТОРНАЯ РАБОТА № 2 “ПРОСТЕЙШИЕ КРИПТОГРАФИЧЕСКИЕ ПРЕОБРАЗОВАНИЯ”

Цель:

1) Реализовать в виде программы шифр (зашифрование и расшифрование) в соответствии с вариантом. Язык исходного текста русский или английский по выбору исполнителя.

2) Реализовать в виде программы атаку полным перебором ключа, используя для оценки правильности выбора ключа визуальный метод или исходный текст для автоматического сравнения результата дешифрования.

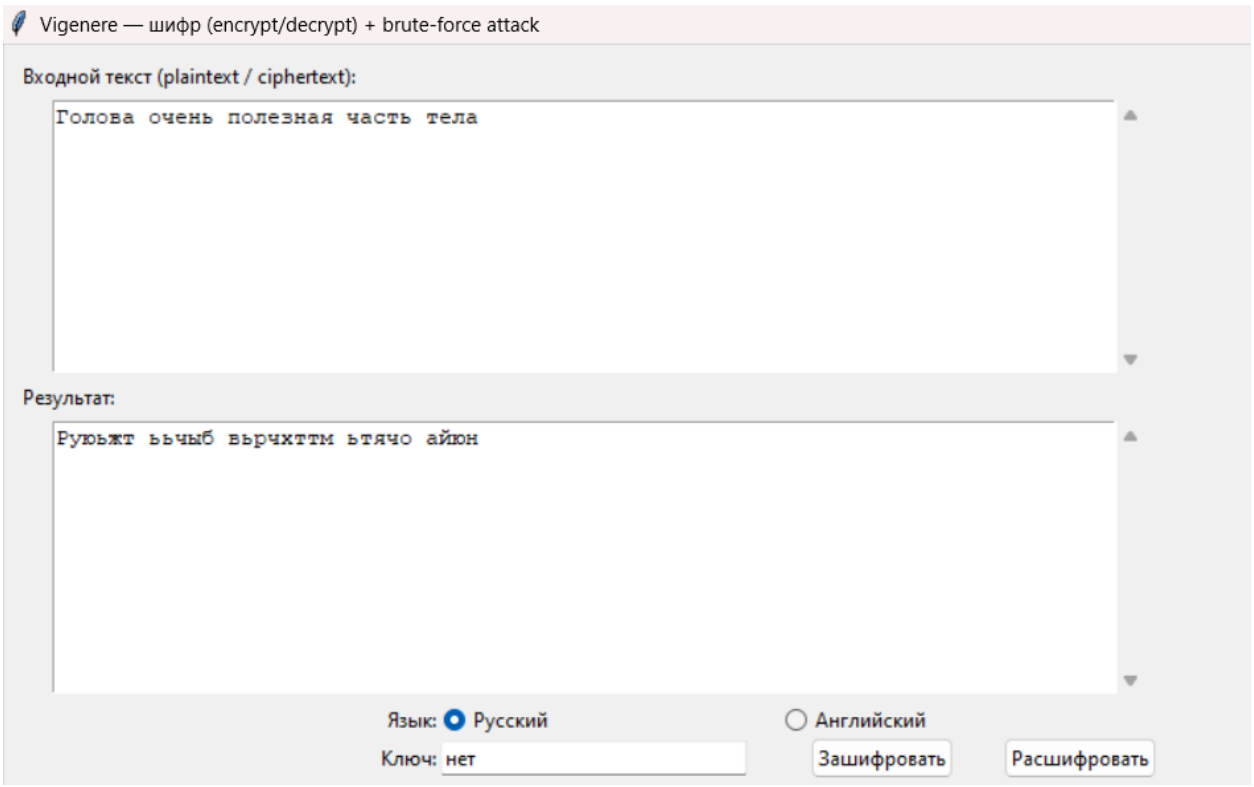
3) Оценить криптографическую стойкость реализованного шифра.

4) Предложить варианты усложнения шифра. Предложенные варианты оформить в виде алгоритма.

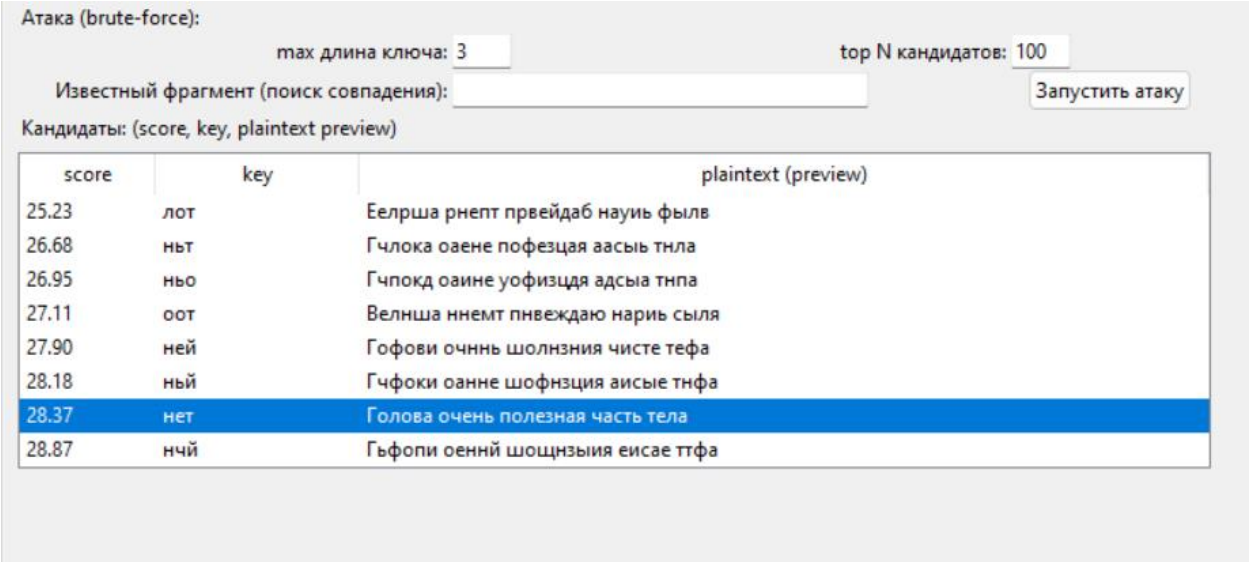
Варианты для реализации:

2) Шифр Вижинера.

1) Пример работы программы:



2) Атака полным перебором:



3) Оценка криптографической стойкости

Шифр Виженера — это классический полиалфавитный шифр, чья стойкость кардинально выше, чем у моноалфавитных шифров (например, шифра Цезаря), но абсолютно недостаточна по современным меркам.

Сильные стороны (по меркам своего времени):

1. **Полиалфавитность:** Это главное преимущество. Частота символов в шифртексте сглаживается, что ломает классический частотный анализ, эффективный против шифров like Цезаря.
2. **Большое количество ключей:** Для алфавита из N букв и ключа длиной L существует N^L возможных ключей. Для длинного ключа прямой перебор (brute-force) был неосуществим в до компьютерную эру.

Слабые стороны и атаки (почему он считается нестойким):

1. **Уязвимость к методу Казиски (Kasiski examination):**
    - **Причина:** Если ключ короче открытого текста (а так почти всегда и бывает), он повторяется. Это значит, что одинаковые последовательности в открытом тексте будут зашифрованы в одинаковые последовательности в шифртексте, если они оказались на одинаковых позициях относительно начала ключа.
    - **Атака:** Криптоаналитик ищет повторяющиеся последовательности в шифртексте, вычисляет расстояния между ними. Эти расстояния будут кратны длине ключа. Найдя несколько таких кратных чисел, можно с высокой вероятностью определить длину ключа (L).
2. **Уязвимость к частотному анализу с индексом совпадений (Index of Coincidence):**

- **После определения длины ключа L:** Шифртекст разбивается на L групп. В первую группу попадают 1-й, (L+1)-й, (2L+1)-й... символы, во вторую — 2-й, (L+2)-й... и т.д.
- **Суть атаки:** Каждая из этих групп была зашифрована ОДНИМ и тем же сдвигом (одной буквой ключа). Таким образом, каждая группа является моноалфавитным шифром (шифром Цезаря). К каждой группе применяется стандартный частотный анализ для восстановления буквы ключа, отвечающей за эту группу.

3. **Ключ часто является осмысленным словом:** Это сужает пространство ключей и позволяет проводить атаки по словарю.

4) Усовершенствование алгоритма:

Алгоритм усложнения:

1. Возьмите открытый текст (P).
2. Выберите **первый ключ** (K1) и зашифруйте текст шифром Виженера: C1 = Виженер(P, K1).
3. Выберите **второй ключ** (K2, лучше другой длины) и зашифруйте результат C1 еще раз: C2 = Виженер(C1, K2).

Вывод: Изучил разновидности шифров, реализовал шиф Виженера и его взлом. Провел анализ стойкости и предложил усовершенствование алгоритма.