**МИНОБРНАУКИ РОССИИ САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ ЭЛЕКТРОТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ «ЛЭТИ» ИМ. В.И. УЛЬЯНОВА (ЛЕНИНА)**

**Кафедра Информационной безопасности**

**ОТЧЕТ**

**по лабораторной работе №1**

**по дисциплине «Криптографические методы защиты информации»**

**ТЕМА: ИЗУЧЕНИЕ КЛАССИЧЕСКИХ ШИФРОВ SCYTALE, SUBSTITUTION, HILL**

|  |  |  |
| --- | --- | --- |
| Студентка гр. 9363 |  | Труханова В.А. |
| Преподаватель |  | Племянников А.К. |

Санкт-Петербург

2023

Цель работы: исследовать шифры Railfence, Substitution, Hill и получить практические навыки работы с ними, в том числе с использованием приложения CrypTool 1 и CrypTool 2.

1. **Шифр «Сцитала» (Scytale)**

**Задание:**

1. Найти шифр в CrypTool 1: Encrypt/Decrypt –> Symmetric(Classic)

Scytal/Rail Fence.

2. Создать файл с открытым текстом, содержащим последовательность

цифр.

3. Запустить шифр и выполнить зашифровку и расшифровку созданного

текста несколько раз.

4. Установить, как влияют на шифрование параметры Number of Edges и

Offset.

5. Зашифровать и расшифровать текст, содержащий только фамилию

(транслитерация латиницей), вручную и с помощью шифра при Number of Edges > 2, Offset ≥ 2. Убедиться в совпадении результатов.

6. Выполнить самостоятельную работу: взять в CrypTool 2 шаблон атаки

на шифр методом «грубой силы» и модифицировать этот шаблон, заменив блок с шифротекстом на блок ввода открытого текста и блок зашифрования. Изучить принципы этой автоматической атаки.

**Реализация в CrypTool 1:**

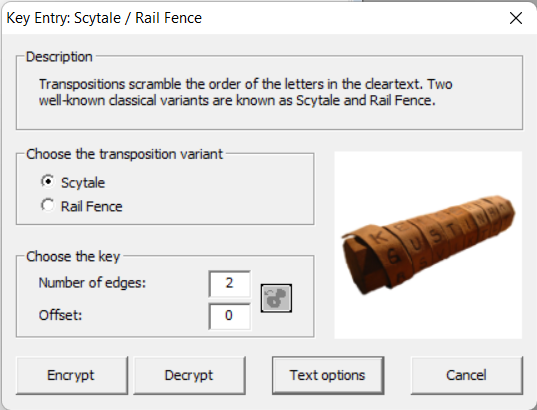
****

Рисунок 1 – Окно задания параметров для шифра

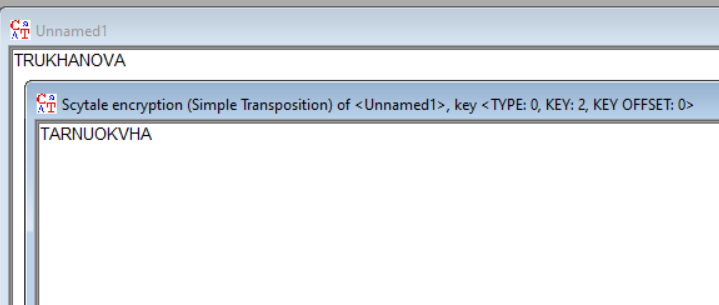
****

Рисунок 2 – Результат работы после нажатия кнопки «Encrypt»

**Схема, поясняющая работу шифра:**

Открытый текст: ПРИМЕРШИФРАСЧИТАЛА

Шифротекст: ПШЦРИИИФТМРАЕАЛРСА

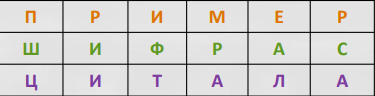
****

Рисунок 3 – Представление работы шифра в виде таблицы

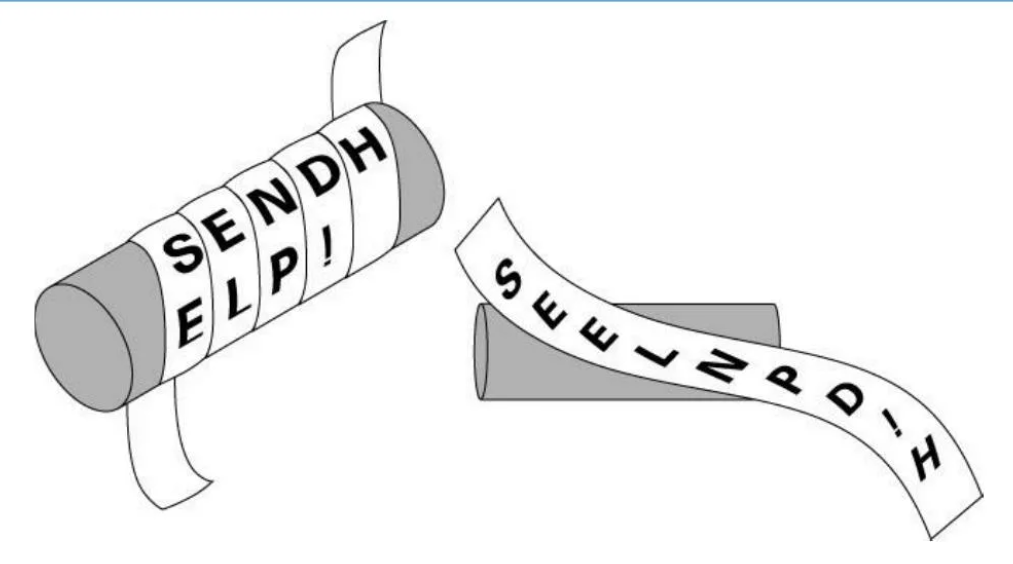
****

Рисунок 3 – Представление работы шифра в виде цилиндра и ленты

**Пример работы шифра:**

Выбранные параметры:

* Количество ребер 4;
* Смещение 2;
* Заглавные буквы алфавита.

Исходный текст: TRUKHANOVA

Шифротекст: RHOUAVTKNA

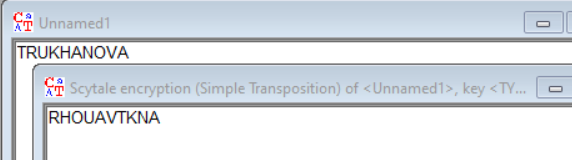
****

Рисунок 4 – Результат шифрования

*Таблица 1 «Демонстрирование работы смещения»*

|  |  |  |
| --- | --- | --- |
|  |  | T |
| R | U | K |
| H | A | N |
| O | V | A |

**Основные характеристики шифра:**

* Тип шифра перестановка;
* Ключ шифра количество строк и смещение;
* Сложность атаки грубой силы .

1. **Шифр Substitution**

**Задание:**

1. Найти шифр в CrypTool 1: Encrypt/Decrypt –> Symmetric(Classic).

2. Зашифровать и расшифровать текст, содержащий только вашу фами-

лию (транслитерация латиницей), вручную и с помощью шифра c выбранным ключом и смещением Offset ≠ 0. Убедиться в совпадении результатов.

3. Выполнить зашифрование и расшифрование с различными паролями

и смещениями Offset и разобраться, как формируется алфавит шифротекста.

4. Выбрать абзац (примерно 600 символов) из файла English.txt (папка

CrypTool/reference) и зашифровать его.

5. Выполнить атаку на шифротекст, используя приложение из Analysis –>Symmetric Encryption(classic) –> Cipher Text Only.

6. Повторить шифрование и атаку для тестов примерно в 300 и 150 сим-

волов.

7. Изучить возможности CrypTool 1 для автоматизации выполнения руч-

ного расшифрования для текстов размером менее 300 символов.

8. Выбрать новый абзац (примерно 600 символов) из файла English.txt

(папка CrypTool/reference) и зашифровать его.

9. Дешифровать этот абзац, используя приложение Analysis –> Tools for

Analysis и Analysis –> Symmetric Encryption(classic) –> Manual Analysis.

10. Выполнить самостоятельную работу:

а) зашифровать текст из 200 символов, сохранить ключ и обменяться

шифровками с коллегой по учебной группе для дешифровки;

б) изучить одну из атак, реализованных в CrypTool 1 и 2, опираясь

на Help и ссылки на статьи.

**Реализация:**

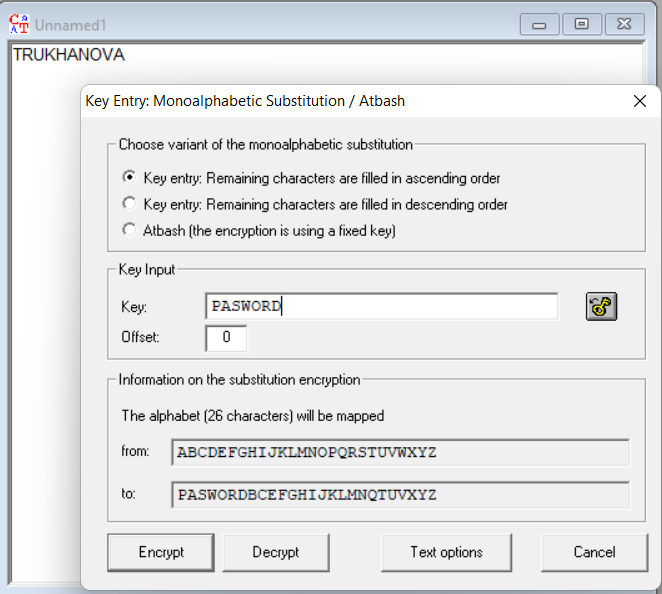
****

Рисунок 5 – Реализация шифра Substitution в CrypTool 1

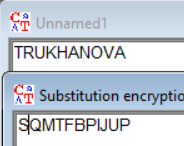
****

Рисунок 6 – Зашифрованный текст

**Пример работы шифра:**

Выбранные параметры:

* Ключевое слово PASWORD;
* Смещение 0 и смещение 5;
* Заглавные буквы алфавита.

Исходный текст: TRUKHANOVA

Шифротекст (смещение 0): SQMTFBPIJUP

Шифротекст (смещение 5): NLHQPCKWOTK

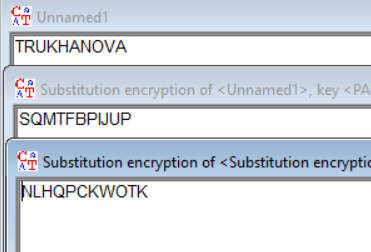
****

Рисунок 7 – Разные параметры зашифровки

При смещении m кодовое слово, ставится начиная с позиции m+1, где предыдущие m позиций в алфавитном порядке занимают буквы, отсутствующие в кодовом слове.

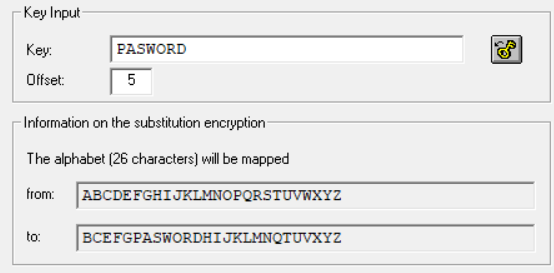


Рисунок 8 – Демонстрация работы смещения

**Основные характеристики шифра:**

* Тип шифра замена;
* Ключ шифра кодовое слово и смещение;
* Сложность атаки n! (n длина алфавита);

**Выполненная процедура атаки:**

На данный шифр возможна атака частотным анализом.

Возьмем шифротекст длиной примерно 600 символов. С помощью Analysis -> Tools for Analysis -> Histogram построим гистограмму частот символов текста.

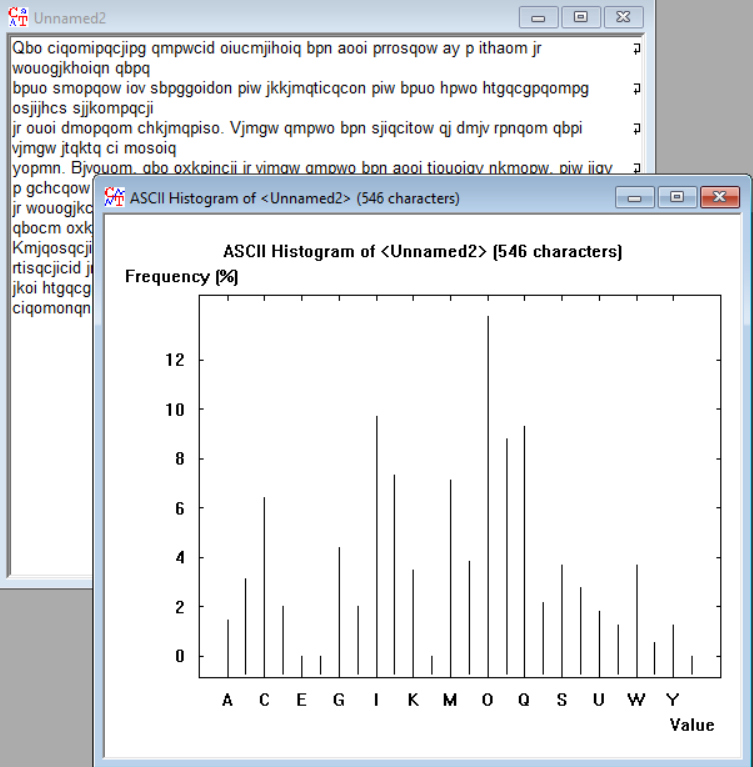


Рисунок 9 – Частоты символов в шифротексте

Для более точной дешифровки эталонный текст для сравнения частот должен быть достаточно большим. Возьмем текст в 115000 символов и с помощью той же функции узнаем частоты символов.

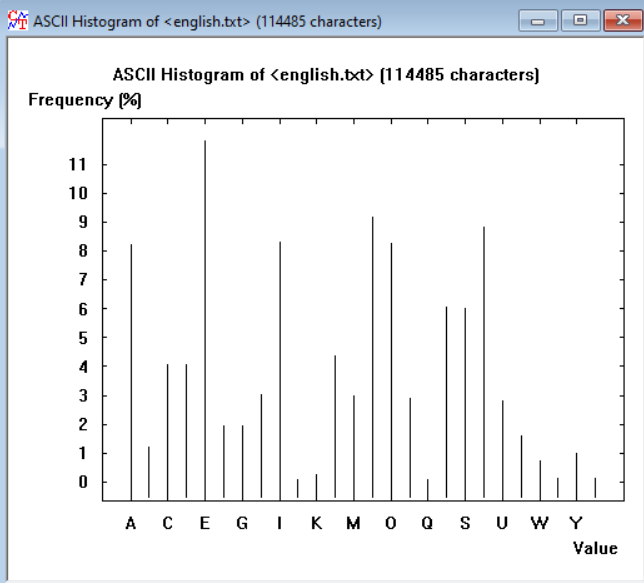


Рисунок 10 – Частоты символов в эталонном тексте

На основе этих данных утилита Analysis –> Tools for Analysis и Analysis –> Symmetric Encryption(classic) проводит частотный анализ и дешифрует текст.

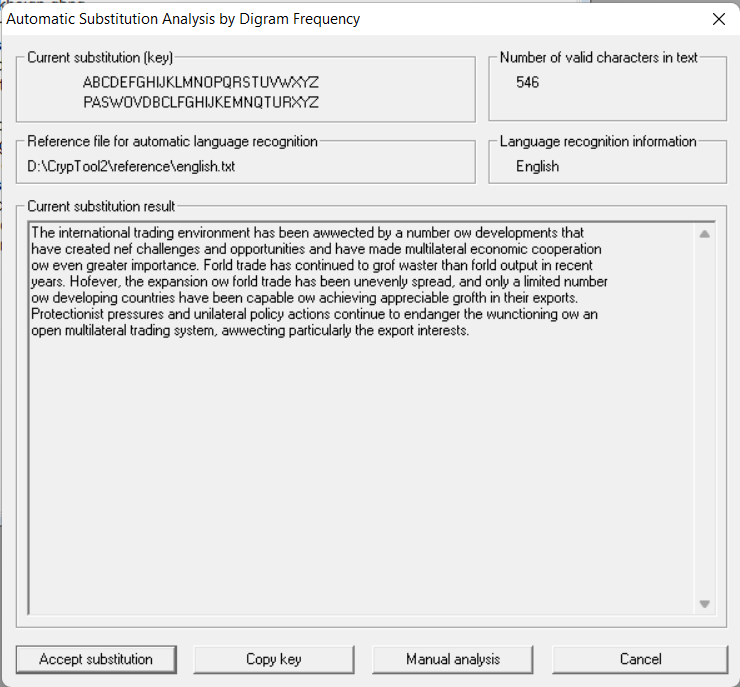


Рисунок 11 – Результат частотного анализа

1. **Шифр Хилла (Hill)**

**Задание:**

1. Найти шифр в CrypTool 1: Encrypt/Decrypt –> Symmetric(Classic).

2. Зашифровать и расшифровать текст, содержащий только вашу фами-

лию (транслитерация латиницей), вручную и с помощью шифра c выбранным

ключом 2 × 2. Убедиться в совпадении результатов. Проверить обратимость

шифрующей матрицы (ключа).

3. Зашифровать текст с произвольным сообщением в формате «DEAR

MR ФАМИЛИЯ ИМЯ ОТЧЕСТВО THANK YOU VERY MUCH», используя

транслитерацию латиницей и шифрующую матрицу 3 × 3.

4. Выполнить атаку на основе знания открытого текста, используя при-

ложение из Analysis –> Symmetric Encryption(classic) –> Known Plaintext.

5. Выполнить самостоятельную работу: обменяться шифровками с кол-

легой по учебной группе для дешифрования при условии, что формы обра-

щения и завершения сообщения известны. Размерность использованного

ключа держать в секрете.

**Схема и математические формулы, поясняющие работу шифра:**

Перед шифрованием необходимо каждому символу алфавита сопоставить код равный порядковому номеру символа в алфавите.

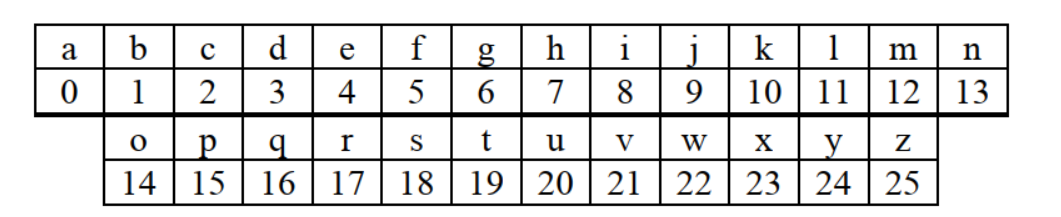


Рисунок 12 – Пронумерованный алфавит

Затем коды символов открытого текста записываются в матрицу размером и создается шифрующая матрица . Для шифрования матрица открытого текста умножается на шифрующую матрицу и вычисляется остаток от деления значения элементов матрицы-произведения на число символов выбранного алфавита. На рисунке 13 показана схема шифрования текста «*HILLCIPHEREXAMPLES*».

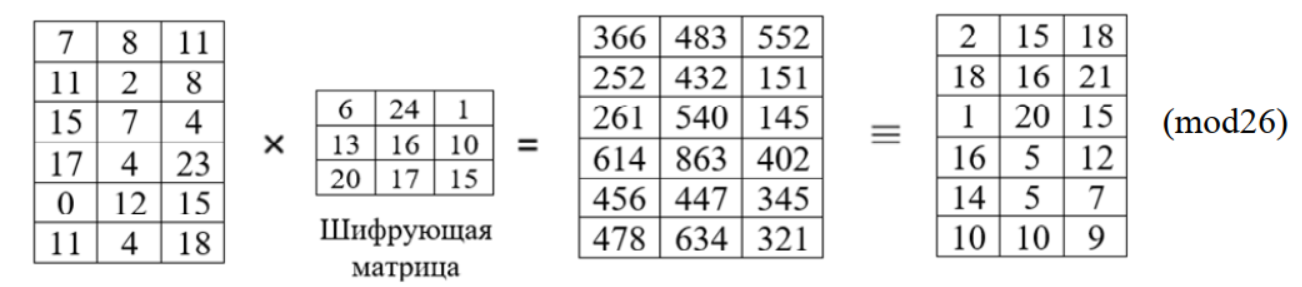


Рисунок 13 – Схема шифрования текста «*HILLCIPHEREXAMPLES*»

Шифротекст: *CPSSQVBUPQFMOFHKKJ.*

Для расшифровки необходимо шифротекст умножить на матрицу, которая является мультипликативной инверсией по отношению к шифрующей для выбранного алфавита. На рисунок 19 показана схема расшифровки.

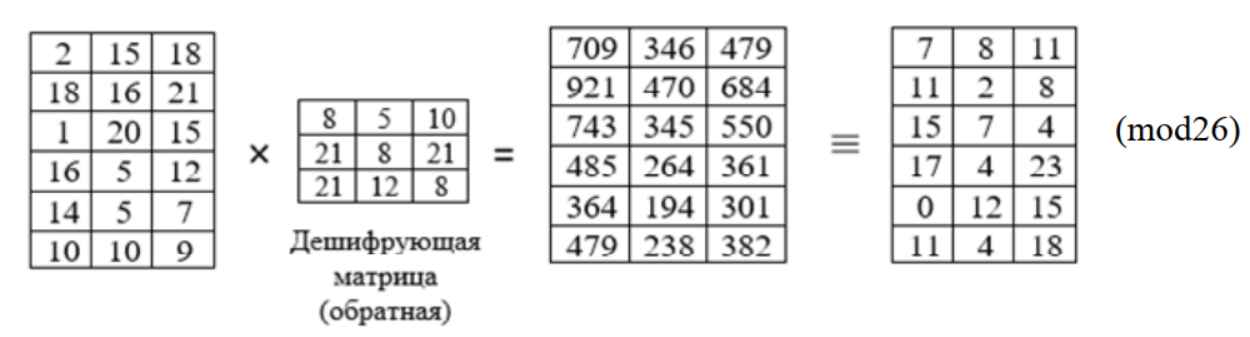


Рисунок 14 – Схема расшифровки

Получаем открытый текст: HILLCIPHEREXAMPLES.

**Реализация в CrypTool 1:**

В окне шифра Хилла сгенерируем случайный ключ размером 3 на 3

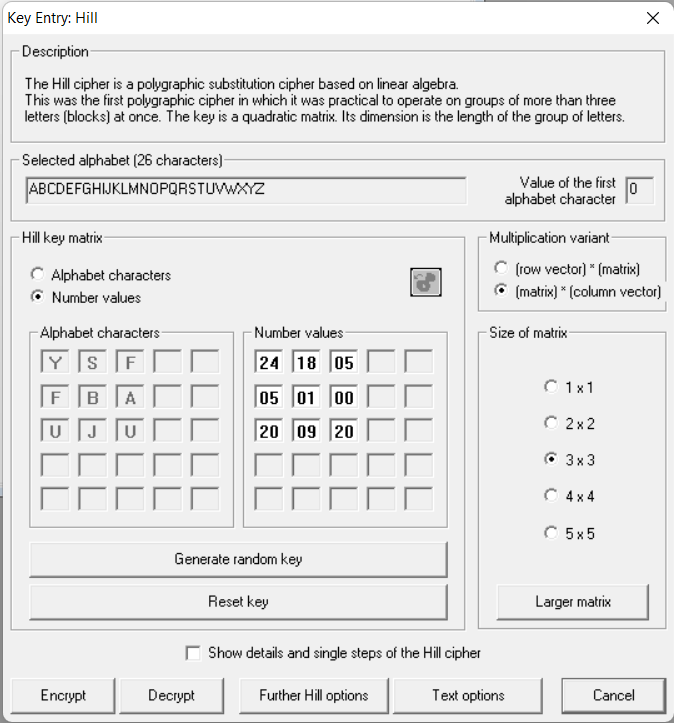
****

Рисунок 15 – Реализация шифра

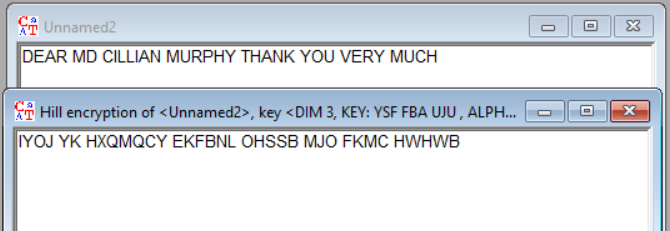
****

Рисунок 16 – Результат шифрования

**Пример работы шифра:**

Выбранные параметры:

* Матрица шифрования ;
* Матрица дешифрования (мультипликативная инверсия);
* Заглавные буквы алфавита.

Исходный текст: TRUKHANOVA

Шифротекст: FDYKJOZSTA

На рисунке 17 один был взят исходный текст и зашифрован транспонированной матрицей шифрования, затем шифротекст был зашифрован транспонированной матрицей дешифрования.

Матрицы были транспонированы чтоб нивелировать отличия между способами перемножения матриц.

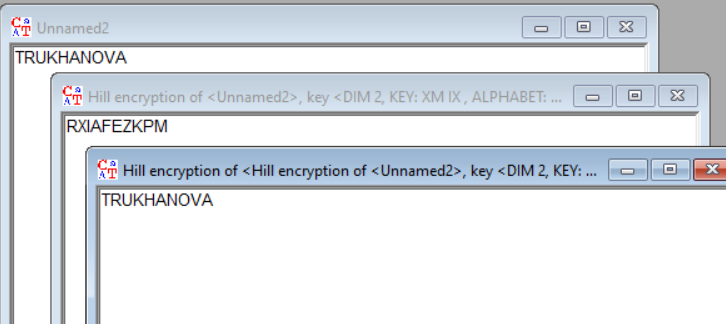
****

Рисунок 17 – Результаты шифрования двумя матрицами

Процесс шифрования:

Процесс дешифрования:

**Основные характеристики шифра:**

* Тип шифра замена;
* Ключ шифра шифрующая матрица размера ;
* Сложность атаки (n длина алфавита, m размер шифрующей матрицы).

**Описание атаки на шифр:**

Возможна атака на ключ на основе знания исходного текста.

Возьмем наш исходный текст и зашифруем его с помощью случайно сгенерированной матрицы 3 на 3.

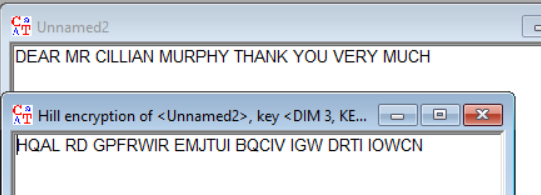


Рисунок 18 – Исходный и зашифрованный текст

Выполним атаку с помощью CrypTool 1.0, используем функцию *Analysis –> Symmetric Encryption(classic) –> Known Plaintex.*

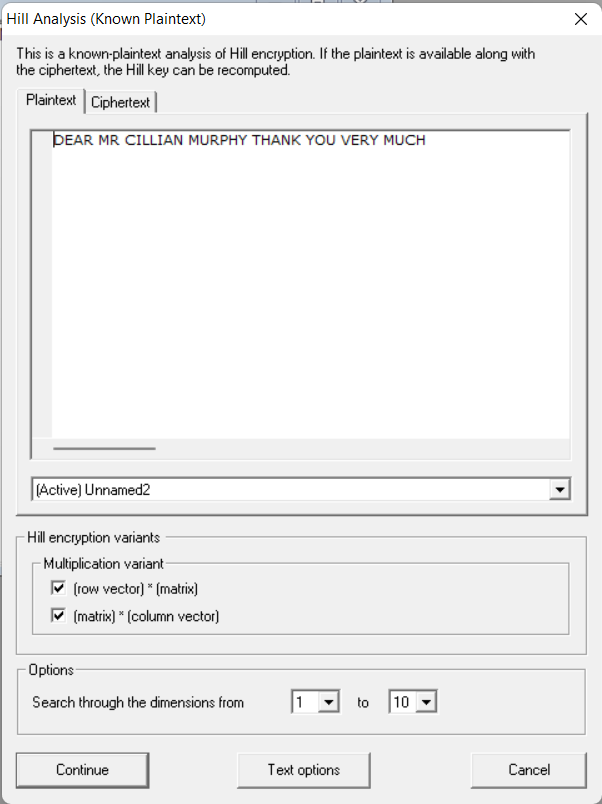


Рисунок 19 – Задание параметров

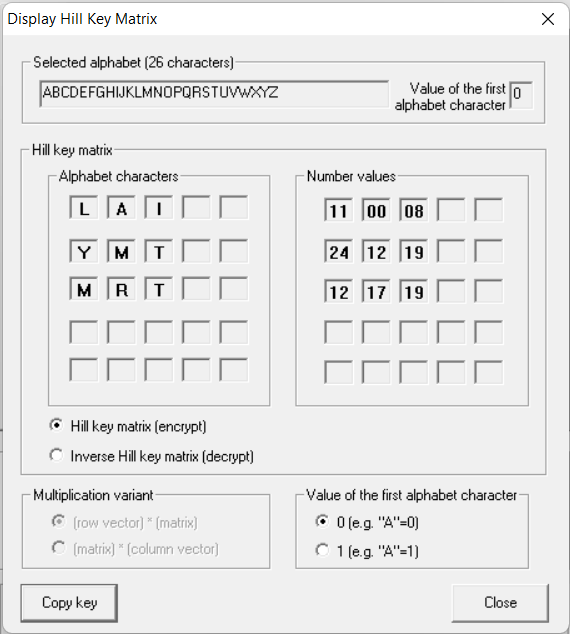


Рисунок 20 – Результат работы анализа

Проверим результат, попробовав расшифровать шифротекст полученной матрицей.

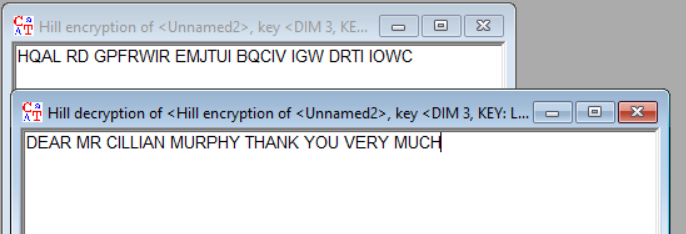


Рисунок 21 – Успешная атака

**Заключение:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Название шифра** | **Тип шифра** | **Ключ шифра** | **Подходящая атака** | **Оценка сложности атаки «грубой силой»** |
| **Scytale** | **Перестановка** | **Количество строк и смещение** | **Полный перебор возможного количества строк и смещений** | **(n длина сообщения)** |
| **Substitution** | **Замена** | **Кодовое слово и смещение** | **Частотный анализ шифротекста** | **, n число букв в алфавите** |
| **Hill** | **Замена** | **Шифрующая матрица** | **Атака на ключ, зная часть открытого текста** | **, n число букв в алфавите, m размер шифрующей матрицы** |