Министерство образования Республики Беларусь

Учреждение образования

«Гомельский государственный университет им. Франциска Скорины»

**Отчет по лабораторной работе**

**Криптосистемы**

**Выполнили: Студенты гр. MC-22**

**Скрежендевский А. В.**

**Проверил: Соколов С. И.**

**2020**

1. Расшифровать криптограмму Цезаря (русский алфавит без *ё* и *ъ*). Зашифрованный текст:

Нултхсжугчлв угкугдгхюегих пихсзю кгэлхю лрчсупгщлл сх  
рифгрнщлсрлусегррсжс зсфхцтг

Переберём все возможные комбинации. В ходе перебора находим правильную комбинацию

КРИПТОГРАФИЯ РАЗРАБАТЫВАЕТ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

Ключ 22.

1. Переведем текст с тарабарской грамоты. Зашифрованный текст:

Аццикишпая чмунна л цоноспикесьпой онемадией урпохепия, лшяфаппой  
ло лсохепиер фатопари цилкмищукишполки, пафишаекля тосьдор

Текст переводится простой заменой символов по правилам тарабарской грамоты. Расшифрованный текст;

АДДИТИВНАЯ ГРУППА С ДОПОЛНИТЕЛЬНОЙ ОПЕРАЦИЕЙ УМНОЖЕНИЯ, СВЯЗАННОЙ СО СЛОЖЕНИЕМ ЗАКОНАМИ ДИСТРИБУТИВНОСТИ, НАЗИВАЕТСЯ КОЛЬЦОМ

1. Расшифруем постолбцовый вариант маршрутной транспозиции. Зашифрованый текст.

Сзветмтлаельаеемлонялдыивазьоскеуанвлоккнааягааиятмоесмьичсаа

Подберём размеры прямоугольника, в который впишется шифр постолбцовой записью. И преобразуется в связный текст.

Расшифрованый текст.

следовать

замыслями

великогоч

еловекаес

тьнаукаса

маязанима

тельная

1. Используя таблицу Виженера, зашифруем фразу «A» с помощью ключевого слова «B».

Фраза А: ХУЖЕ ВСЕГО ТО, ЧТО КТО СМОЛОДУ ПЛОХО ОБУЧЕН, ТОТ ДО СТАРОСТИ В ЭТОМ НЕ СОЗНАЕТСЯ. ПЕТРОНИЙ

Ключ: Время

Зашифрованный текст: ЧГЛС ДБКПН ВУ, ЩВУ ЙФЮ ЭЛРЫУРТ ЯРЪФР УНТЩХТ, ФЮЧ ГР ЦЮЯТЮЦЮЗ Т ЙСРЬ ЩД БУУМВХЧЭЮ. ФССТЮТФИ

1. Взломаем шифр Виженера.

Зашифрованный текст:

ЫЮУ ЖЬЪЬГ ЦГТЧГЖГФ ДБФЦЗЯХТГВЮБ У ТХВШКНЫМЬ, РУАЧСТ АЬТЭЭМЧС ЪЕЪЪФЪЭЦ СЬЧРШ ТЬРЬШЩКВЮЗС АЪНЖГЪЕЖГФКБ Ф ЪХЪЕЧМШ ИУЧКМЦЩНЬЭ: ВСЭСЬЙЦН ЮМЙ АСХЧМШ ГВЦУЕТЧДУГ, Х ЩЕЩ ОЧГБЗС УЬЦДБФТЭЭМГЗВЛ ЦЪМИГВЦРГЮЩУ. СЦЗН ХХШЧНМЩЛ Ч УЕБЦГЕВЩЛЬ, ЦЕЖСКЮЭЖЭД ГСРЬВЩАК ЩКЩЯЭЧХГЦУЧ. ИГБНУВЯЭАЮ ФРЭ ЦШЕЮЬЦРЬ ЧГЪИПГ ЯЦБЦБТЬГЭД, СЦАЩ ФГХДШЗЩЮБ ЮМЙ ЦПУ ЮЬЦГЭ... М ЧЯЮ ВСШКЯ ЩЕ ХЯХВЯХ ЪСЫЕК ФМ ЮЬЦХ ФРЭ ЪЧХ ЦХХЬЩК ГЛИГВЮКВ. РРВЗК ВЩНЖЖЬЙЭГСРСЮЬ ГГЩУЖРЮЦФ Ц ДЯРЭИИФЗХЮФГ ЮМЙ ЩБ ВЦРУЖГМЧЯЯШ, С НБЦКЮЭЦ ИАСУТГЦ ШЧЦГБЬ – ВЦЫХЭРУТЬЮЩУ... Э ОУГТЕК БММАЩГТГ ЬЧВЯДКВЩС АПРКЮ Ц ЖУЬНБ ОТЬЙЩНБ ЩКЩЯЭЧХГЦЕБ: УЩЮЬИГ ЮДШЯЮНЗ ЬЙВЯ, ЩБЯИГФЬ ЩБЯИГЦ... ЫУТГЬСИ ЦЧГ БУМЦЮ, ИЮУЦМ КШЯ ФГУСЙЬЮФК У УЦКСЦЗУС ЦМЧУ АЪНФГЩУ ЯЦХИЧМГОЩШ, ХЬРЫЦЩ ИИФЧРУМЧС ФЬ ЖМХХЫЮКЕ Ф ВБМЗР О ЖУЬНК ДШЗЫМЬ. ЩЕЩЯ ШМЩЮАЧСЮБ Щ ЦГВЮЕЧ ЫХЭВЯЧЖГОШУКФЬ: ЮУ, ГЧГ ОАЪЯОКЗ Я ЧМДШМЩОЕЬЭЬИГ ЭСЬЖ З ЯНЮЬВЮЗЬ РХИШСО Щ ЦЧЦЪЦЗЮФПГУ, ЦДРКЗ ЩКДБФДЗЮЬ ИВЧАНСЮБ У ФЕЩЭШЗВЮЗЭЩ ЛЬЮЗ, ЩЧН ЯЮЫХ, НАЩ ШМЩЮКАР... ЬЪЬЮИ ЧСТТГ ЮЕЯЧС ЖЪСЙЭГИ ЪС ЧЬЭ, МГЬЖР ЩЕЖЭСЭЯС ФЕЩДРХВИ ЯВЮЕЗЩ З ЯНЦЗСЩУЧЫС ГТЕКШЯ ХХШПУЧЯЪЕ У

Взлом будет проводиться по методу частотного крипто анализа.

Данный метод состоит из двух этапов:

1. Получение длинны ключевого слова;
2. Вычисление букв ключвого слова.

Метод нахождения длинны ключа, основан на том факте, что вероятность совпадения двух случайных букв в некотором достаточно длинном тексте (индекс совпадений) — это постоянная величина. Таким образом, если разбить текст на L групп символов, каждая из которых зашифрована шифром простой замены (напомню, это и означает, что L — длина ключевого слова), то индексы совпадений для каждой из групп будут довольно близки к теоретическому значению этой величины; для всех других разбиений индексы совпадений будут гораздо ниже. Индекс совпадений можно посчитать по формуле

https://habrastorage.org/getpro/habr/post_images/48a/3df/e1a/48a3dfe1ad263173759b23ce5dd9103d.png

(fi — количество i-х букв алфавита в тексте, а n — его длина)

Полученная длина ключа равна 4.

Для получения букв ключа требуется поделить зашифрованный текст на 4 групы. Группы выбираются таким образом:

1 группа – каждый i∙4 символ;

2 группа – каждый i∙4+1 символ;

3 группа – каждый i∙4+2 символ;

4 группа – каждый i∙4+3 символ;

где i = 1, 2, …

Так как в группах остаётся мало символов для качественного частотного анализа, то проведем упрощённый частотный анализ.

Самая не распространённая буква в русском алфавите буква “Ъ”, ее частота в разы меньше чем у остальных букв, что делает ее лучшим вариантом для поиска смещения группы. В каждой группе требуется найти самый не распространённый символ.

Группы настолько малы, что некоторые символы в них не встречаются:

1 группа – нет символов соответствующих символу ключа Л Н С Ф;

2 группа – нет символов соответствующих символу ключа Ж И М П;

3 группа – нет символов соответствующих символу ключа Е И Я;

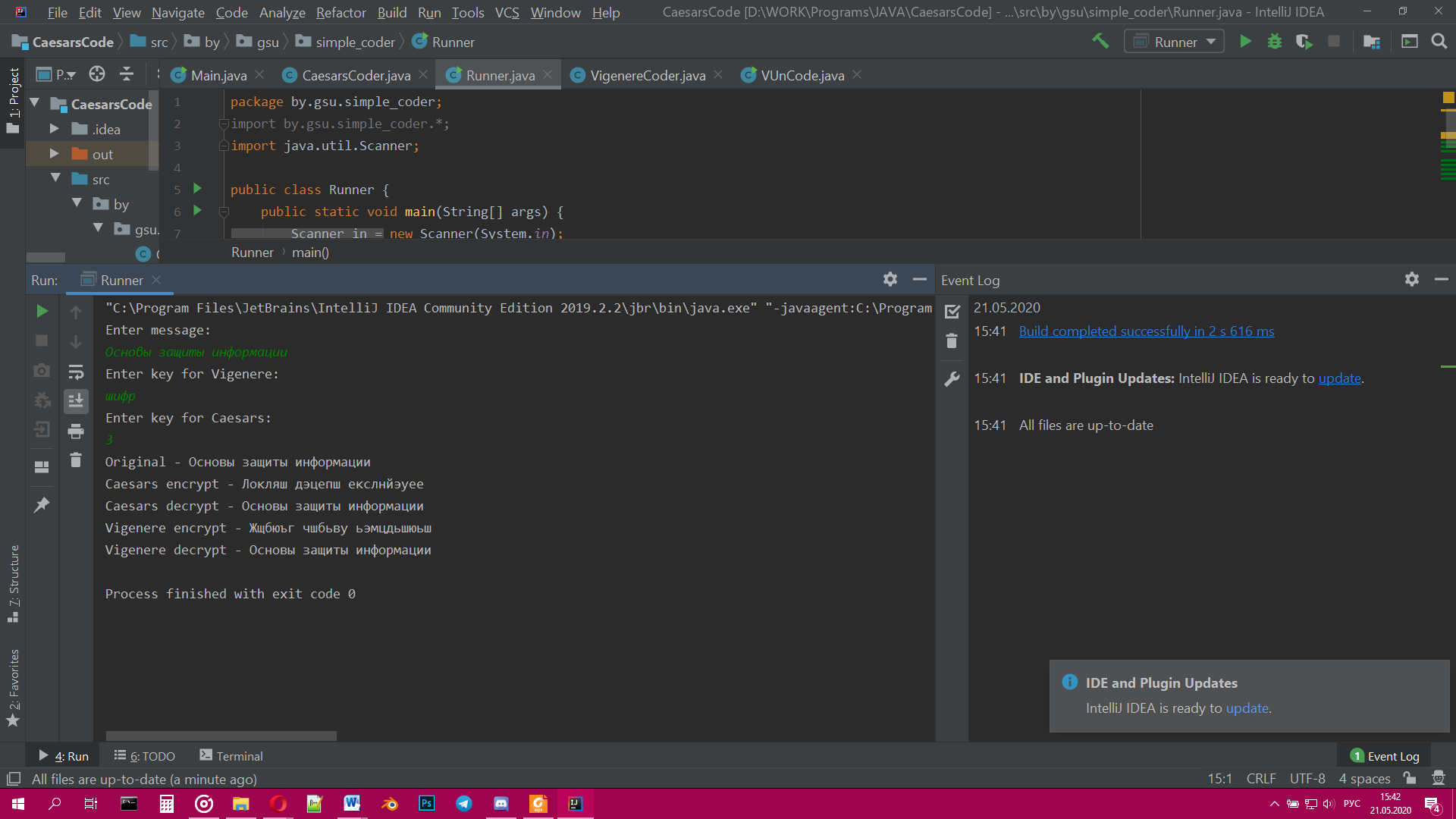
4 группа – нет символов соответствующих символу ключа П С Х;

Из данных символов, соблюдая последовательность, можно составить единственное слово – СМЕХ.

Ключ шифра найден.

**6.** Составим алгоритмическое и программное обеспечение: процедур шифрования и расшифрования с использованием шифра Цезаря при вводе с клавиатуры ключа и исходного или зашифрованного текста. Программа представлена на рисунке 1.

**7.** Составим алгоритмическое и программное обеспечение: процедур шифрования и расшифрования с использованием шифра Вижинера при вводе с клавиатуры ключа и исходного или зашифрованного текста. . Программа представлена на рисунке 1.



**Рисунок 1 – результат работы программы**

**Вывод:**

В ходе данной лабораторной работы были рассмотрены основные исторические криптосистемы защиты информации от несанкционированного доступа. Данные системы были использованы на практике.