Государственное образовательное учреждение

«Белорусский государственный технологический университет»

Отчет

*по лабораторной работе №5*

ТЕМА ЗАНЯТИЯ: КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ С ПОМОЩЬЮ АЛГОРИТМОВ СИММЕТРИЧНОГО ШИФРОВАНИЯ

|  |  |
| --- | --- |
|  | **Исполнитель:**  Студента (-ка) группы 2  Специальность\_\_\_\_ИСиТ\_\_\_  Гулевич Никита Максимович  (Ф.И.О.) |
|  | **Преподаватель**:  Ржеутская Н. В. |

Минск, 2025

Цель: овладеть основными криптографическими алгоритмами симметричного шифрования.

1. Что такое криптография?

Криптография – наука о методах обеспечения конфиденциальности (невозможности прочтения информации посторонним) и аутентичности (целостности и подлинности авторства) информации.

1. В чем особенность симметричных криптосистем?

симметричные (с секретным, единым ключом, одноключевые, single-key). Их ключ шифрования такой же как и ключ расшифрования.

1. Что можно использовать в качестве ключа в симметричных криптосистемах?

 **Случайные битовые строки**: Генерация случайного ключа определенной длины (например, 128, 192 или 256 бит) с помощью генераторов случайных чисел.

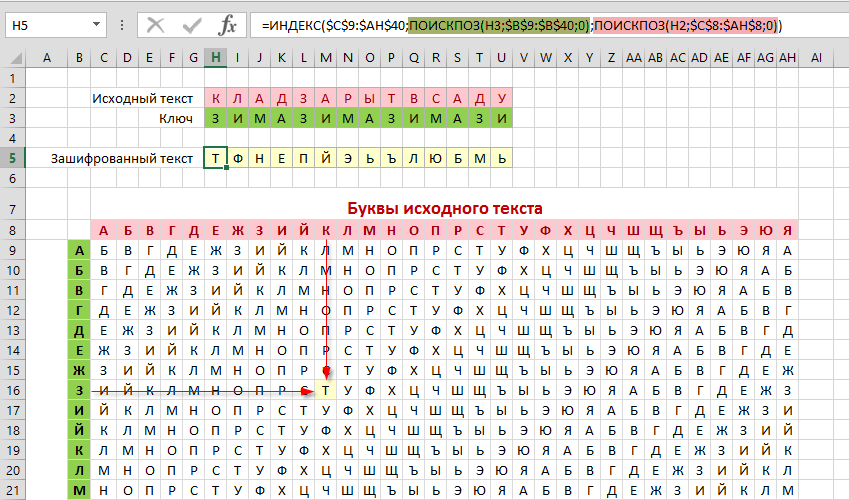
 **Пароли**: Человеческий ввод в виде пароля, который затем преобразуется в ключ с помощью криптографической хеш-функции и других методов (например, PBKDF2, bcrypt).

 **Секретные фразы**: Долгие и сложные фразы, которые могут быть обработаны для получения ключа.

 **Ключи, сгенерированные аппаратными модулями**: Специальные устройства (например, HSM - Hardware Security Module), которые могут генерировать и хранить ключи.

 **Ключи, производные от других ключей**: Использование алгоритмов для генерации новых ключей из существующих (например, с помощью функций Derive Key).

1. Как происходит расшифровка сообщений в системе Виженера?



1. Расскажите об алгоритме шифрования «двойной квадрат» Уитстона.

В 1854 г. англичанин Чарльз Уитстон разработал новый метод шифрования биграммами, который называют "двойным квадратом". Свое название этот шифр получил по аналогии с полибианским квадратом. Шифр Уитстона открыл новый этап в истории развития криптографии. В отличие от полибианского шифр "двойной квадрат" использует сразу две таблицы, размещенные по одной горизонтали, а шифрование идет биграммами, как в шифре Плейфейра. Эти не столь сложные модификации привели к появлению на свет качественно новой криптографической системы ручного шифрования. Шифр "двойной квадрат" оказался очень надежным и удобным и применялся Германией даже в годы второй мировой войны.

Поясним на примере процедуру шифрования этим шифром. Пусть имеются две таблицы со случайно расположенными в них русскими алфавитами (рис. 5). Перед шифрованием исходное сообщение разбивают на биграммы. Каждая из них шифруется отдельно. Первую букву биграммы находят в левой таблице, а вторую ‑ в правой. Затем мысленно строят прямоугольник так, чтобы буквы биграммы лежали в его противоположных вершинах. Другие две вершины этого прямоугольника дают буквы биграммы шифртекста.

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Ж | Щ | Н | Ю | Р |  | И | Ч | Г | Я | Т |
| И | Т | Ь | Ц | Б |  | , | Ж | Ь | М | О |
| Я | М | Е | . | С |  | З | Ю | Р | В | Щ |
| В | Ы | П | Ч |  |  | Ц | : | П | Е | Л |
| : | Д | У | О | К |  | Ъ | А | Н | . | Х |
| З | Э | Ф | Г | Ш |  | Э | К | С | Ш | Д |
| Х | А | , | Л | Ъ |  | Б | Ф | У | Ы |  |

**ВАРИАНТ 7**

А Б В Г Д Е Ё Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ

Ш Щ Ъ Ы Ь Э Ю Я В Е С Н А Б Г Д Ё Ж З И Й К Л М О П Р

Ъ Ы Ь Э Ю Я

Т У Ф Х Ц Ч

гэ ишн зижшпэг оюжи <=не так страшен чёрт

**ЗАДАНИЕ 2**

**ФИО –** ГУЛЕВИЧ НИКИТА МАКСИМОВИЧ

ШИФР ЦЕЗАРЯ +7  
 ЙЪТЛИПЮ ФПСПЩЖ УЖСШПУХИПЮ

| **А** | **Б** | **В** | **Г** | **Д** | **Е** | **Ж** | **З** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **И** | **Й** | **К** | **Л** | **М** | **Н** | **О** | **П** |
| **Р** | **С** | **Т** | **У** | **Ф** | **Х** | **Ц** | **Ч** |
| **Ш** | **Щ** | **Ъ** | **Ы** | **Ь** | **Э** | **Ю** | **Я** |

| **З** | **А** | **Щ** | **И** | **Т** | **Б** | **В** | **Г** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Д** | **Е** | **Ж** | **Й** | **К** | **Л** | **М** | **Н** |
| **О** | **П** | **Р** | **С** | **У** | **Ф** | **Х** | **Ц** |
| **Ч** | **Ш** | **Ъ** | **Ы** | **Ь** | **Э** | **Ю** | **Я** |

**ФИО –** ГУЛЕВИЧ НИКИТА МАКСИМОВИЧ

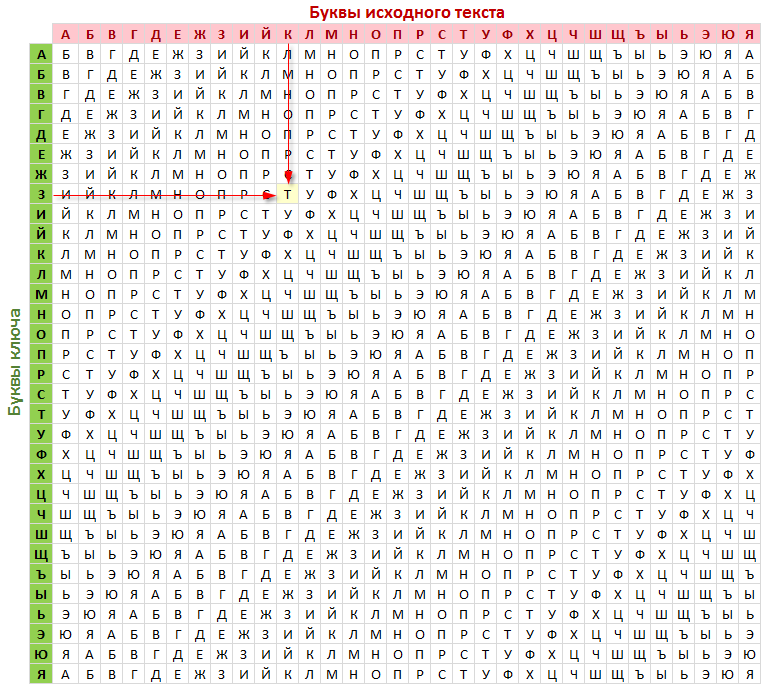
НЬФПМЙЗ ЦЙУЙКЕ ХЕУЫЙХЧМЙЗ

ШИФР ПЛЕЙФЕРА  
  
РАЗОБЬЕМ НА БИГРАММЫ  
 ГУ ЛЕ ВИ ЧН ИК ИТ АМ АК СИ МО ВИ ЧЪ

| **З** | **А** | **Щ** | **И** | **Т** | **Б** | **В** | **Г** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Д** | **Е** | **Ж** | **Й** | **К** | **Л** | **М** | **Н** |
| **О** | **П** | **Р** | **С** | **У** | **Ф** | **Х** | **Ц** |
| **Ч** | **Ш** | **Ъ** | **Ы** | **Ь** | **Э** | **Ю** | **Я** |
|  |  |  |  |  |  |  |  |

ЦТ МЖ ГТ ДЯ ЙТ ТБ ЕВ ЕТ ЫЙ ХД ГТ ШЫ

**ВИЖЕНЕР**



**ФИО –** ГУЛЕ ВИЧ НИК ИТА МА КС ИМ ОВИЧ

ЗАЩИ ТАЗ АЩИ ТАЗ ЗА ЩИ ТА ЗАЩИ

ЛФЕО ХЙЯ МВУ ЫУИ ФБ ДЪ ЫН ЦГВА

**Список использованных источников**

1. Н. В. Ржеутская, О. А. Нистюк, Н. И. Уласевич ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ Лабораторный практикум