Учреждение образования

«Белорусский государственный технологический университет»

**Основы информационной безопасности**

**Лабораторная работа №5**

**«Криптографическая защита информации**

**с помощью алгоритмов симметричного**

**шифрования»**

Выполнил:

Студент 2 курса 2 группы ФИТ

Мойсеёнок Денис

Преподаватель:

Ржеутская Надежда Викентьевна

Минск 2025

**Цель**: овладеть основными криптографическими алгоритмами симметричного шифрования.

Ответы на вопросы:

1. Что такое криптография?

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

2. В чем особенность симметричных криптосистем?

Симметричные алгоритмы шифрования (или криптография с секретными ключами) основаны на том, что отправитель и получатель информации используют один и тот же ключ. Этот ключ должен храниться в тайне и передаваться способом, исключающим его перехват.

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

Слову, фраза или набор чисел.

4. Как происходит расшифровка сообщений в системе Виженера?

Для латинского алфавита: где P – буква изначального сообщения, C – буква шифрованного сообщения, K – буква ключа.

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

Шифр "двойной квадрат" использует сразу две таблицы, размещенные по одной горизонтали, а шифрование идет биграммами, как в шифре Плейфейра.

Перед шифрованием исходное сообщение разбивают на биграммы.

Каждая биграмма шифруется отдельно.

Первую букву биграммы находят в левой таблице, а вторую букву - в правой таблице.

Затем мысленно строят прямоугольник так, чтобы буквы биграммы лежали в его противоположных вершинах.

Другие две вершины этого прямоугольника дают буквы биграммы шифртекста.

Задания:

1. Зашифруйте сообщение с использованием нижеперечисленных шифров и полученного секретного ключа (по номеру варианта (см. номер студента в журнале группы) и ключевому слову «Защита»):

− шифр Цезаря;

− шифр Трисемуса;

− шифр Плейфейра;

− шифр Виженера.

В качестве сообщения используйте свое полное имя (Фамилия Имя Отчество).

Сообщение: МОЙСЕЁНОК ДЕНИС СЕРГЕЕВИЧ

Вариант (ключ) 15

**Шифр Цезаря:**

Сдвиг на 15 букв вправо по алфавиту, получаем следующее:

ЫЭШАУФЬЭЩ ТУЬЧА АУЯСУУРЧЁ

**Шифр Трисемуса:**



k = 15

N = 35

М = (13+15) mod35 = 28 -> Ы

О = (15+15) mod35 = 30 -> Э

Й = (10+15) mod35 = 25 -> Ш

С = (18+15) mod35 = 33 -> Пробел

Е = (5+15) mod35 = 20 -> У

Ё = (6+15) mod35 = 21 -> Ф

Н = (14+15) mod35 = 29 -> Ь

О = (15+15) mod35 = 30 -> Э

К = (11+15) mod35 = 26 -> Щ

Пробел = (33+15) mod35 = 13 -> М

Д = (4+15) mod35 = 19 -> Т

Е = (5+15) mod35 = 20 -> У

Н = (14+15) mod35 = 29 -> Ь

И = (9+15) mod35 = 24 -> Ч

С = (18+15) mod35 = 31 -> Ю

Пробел = (33+15) mod35 = 13 -> М

С = (18+15) mod35 = 31 -> Ю

Е = (5+15) mod35 = 20 -> У

Р = (17+15) mod35 = 32 -> Я

Г = (3+15) mod35 = 18 -> С

Е = (5+15) mod35 = 20 -> У

Е = (5+15) mod35 = 20 -> У

В = (2+15) mod35 = 17 -> Р

И = (9+15) mod35 = 24 -> Ч

Ч = (24+15) mod35 = 4 -> Д

Полученный текст:

ЫЭШ УФЬЭЩМТУЬЧЮМЮУЯСУУРЧД

**Шифр Плейфейра:**

Одна строка: сдвиг по строке вправо

Один столбец: сдвиг по столбцу вниз

Разные строка и столбец: противоположные диагонали по прямоугольнику

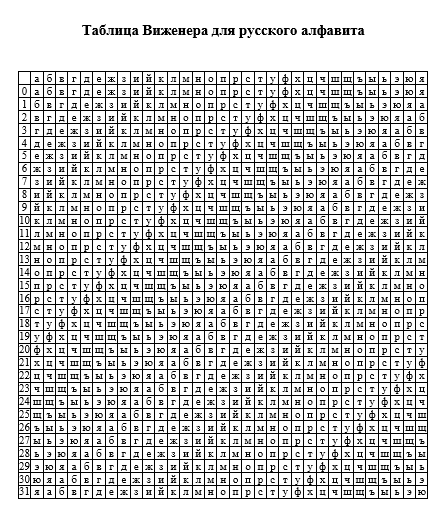
МО ЙС ЕЪ ЕН ОК ДЕ НИ СЪ СЕ РГ ЕЪ ЕВ ИЧ

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 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 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| МО | ЙС | ЕЪ | ЕН | ОК | ДЕ | НИ | СЪ | СЕ | РГ | ЕЪ | ЕВ | ИЧ |
| ДХ | СЫ | ЖШ | ЖД | ДУ | ЕЖ | ГЙ | РЫ | ЙП | ЩЦ | ЖШ | АМ | ЗЫ |

Зашифрованный текст: ДХ СЫ ЖШ ЖД ДУ ЕЖ ГЙ РЫ ЙП ЩЦ ЖШ АМ ЗЫ

**Шифр Виженера:**



Сообщение (сверху): МОЙСЕЕНОК ДЕНИС СЕРГЕЕВИЧ

Ключевое слово (слева): ЗАЩИТАЗАЩ ИТАЗА ЩИТАЗАЩИТ

Зашифрованное сообщение: УОВЩЧЕФОГ МЧНПС КНВГМЕЫРЙ

2. Расшифруйте сообщения по индивидуальному заданию.

Зашифрованное сообщение: \_ \_еоовипи\_ \_ \_ы\_о\_ввв\_тттыыытуоо\_ \_ \_атмтерем\_у,сес,б\_ \_тшт \_ычкьиьгттт,л,дь

Ключ: Февраль

Одиночная перестановка по ключу

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| А | В | Е | Л | Р | Ф | Ь |
| \_ | \_ | е | о | о | в | и |
| п | и | \_ | \_ | \_ | ы | \_ |
| о | \_ | в | в | в | \_ | т |
| т | т | ы | ы | ы | т | у |
| о | о | \_ | \_ | \_ | а | т |
| м | т | е | р | е | м | \_ |
| у | , | с | е | с | , | б |
| \_ | \_ | т | ш | т | \_ | ы |
| ч | к | ь | и | ь | г | т |
| т | т | , | л | , | д | ь |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 6 | 3 | 2 | 5 | 1 | 4 | 7 |
| Ф | Е | В | Р | А | Л | Ь |
| в | е | \_ | о | \_ | о | и |
| ы | \_ | и | \_ | п | \_ | \_ |
| \_ | в | \_ | в | о | в | т |
| т | ы | т | ы | т | ы | у |
| а | \_ | о | \_ | о | \_ | т |
| м | е | т | е | м | р | \_ |
| , | с | , | с | у | е | б |
| \_ | т | \_ | т | \_ | ш | ы |
| г | ь | к | ь | ч | и | т |
| д | , | т | , | т | л | ь |

Расшифрованное сообщение: вы там, где вы есть, и тот, кто вы есть, потому что вы решили тут быть