Министерство образования и науки Российской Федерации Федеральное государственное автономное образовательное учреждение высшего образования

САНКТ-ПЕТЕРБУРГСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ

Факультет: Cистемы управления и робототехники

**Отчет по лабораторной работе**

**№1 «Кодирование и шифрование»**

**Преподаватель**:

Перегудин А. А.,

Ассистент фак. СУиР

**Выполнили**:

студентка гр. R3135

Нгуен Кхань Нгок

Санкт-Петербург 2023

Содержание

[Теорема Шифра Хилла 3](#_Toc146492756)

[Шифр Хилла 3](#_Toc146492757)

[Шаги по зашифрованию и расшифрованию 3](#_Toc146492758)

[Hamming(7,4) 4](#_Toc146492759)

[Задачи 4](#_Toc146492760)

[Задание 1 4](#_Toc146492761)

[Задание 2 4](#_Toc146492762)

[Задание 3 4](#_Toc146492763)

## Теорема Шифра Хилла

### Шифр Хилла

* Шифр Хилла — полиграммный [шифр подстановки](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80_%D0%BF%D0%BE%D0%B4%D1%81%D1%82%D0%B0%D0%BD%D0%BE%D0%B2%D0%BA%D0%B8), основанный на [линейной алгебре](https://ru.wikipedia.org/wiki/%D0%9B%D0%B8%D0%BD%D0%B5%D0%B9%D0%BD%D0%B0%D1%8F_%D0%B0%D0%BB%D0%B3%D0%B5%D0%B1%D1%80%D0%B0) и [модульной арифметике](https://ru.wikipedia.org/wiki/%D0%A1%D1%80%D0%B0%D0%B2%D0%BD%D0%B5%D0%BD%D0%B8%D0%B5_%D0%BF%D0%BE_%D0%BC%D0%BE%D0%B4%D1%83%D0%BB%D1%8E).
* Изобретен Лестером С. Хиллом в 1929 году.
* Первый шифр замены более чем трех символов открытого текста.
* Направление алгоритма состоит в том, чтобы взять m линейных комбинаций (на кольце ) из m буквенных символов plaintext, преобразуя тем самым в m буквенных символов зашифрованного сообщения (ciphertext).
* Процесс преобразования plaintext в ciphertext называется шифрованием.
* Наоборот, процесс преобразования plaintext в ciphertext называется расшифровкой
* Ключ K будет задан n-обратимой квадратной матрицей. K =
* Необходимым и достаточным уисловием обратимости квадратной матрицы является то, что det(K) ≠ 0, тогда обратная матрица K равна: (где C — матрица, сопряженная с K)
* Ключ K — это набор обратимых квадратных ключевых матриц порядка n на кольце , когда определителем матрицы K будут взаимно простые числа с n, или, другими словами, det(K) ≠ 0 и НОД(det(K),n) = 1.

### Шаги по зашифрованию и расшифрованию

#### Зашифрование информации:

Сначала нам нужно создать алфавит с количеством букв n

Нужна ключевая матрица K (обратимая квадратная матрица размера n × n), такая, что определитель матрицы и n взаимно просты).

Затем преобразуйте сообщение в ряд цифр, чтобы каждая буква представляла собой число, основанное на таблице алфавитов (нумерация от 0 до n-1).

Пример:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| А | Б | В | Г | Д | Е | Ё | Ж | З | И | Й | К | Л | М | Н | О | П | Р | С | Т | У | Ф | Х |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 |
| Ц | Ч | Ш | Щ | Ъ | Ы | Ь | Э | Ю | Я |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 |  |  |  |  |  |  |  |  |  |  |  |  |  |

Затем мы делим последовательность на группы по m чисел и формируем матрицы сообщений с именем такие, что (где С: матрица зашифрования)

Заменив каждое только что найденное число в матрице С буквами алфавита, мы получим зашифрованное сообщение.

#### Расшифрованию

* Для расшифрования воспользуемся формулой: (где D: матрица расшифрования)

### Hamming(7,4)

## Задачи

### Задание 1: Шифр Хилла

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| А | Б | В | Г | Д | Е | Ё | Ж | З | И | Й |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| К | Л | М | Н | О | П | Р | С | Т | У | Ф |
| 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 |
| Х | Ц | Ч | Ш | Щ | Ъ | Ы | Ь | Э | Ю | Я |
| 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 |

* n = 33
* Ценное сообщение из 12 символов: л и н е й н а я а л г б
* Ключенные матрицы:

, ,

* det( ≠ 0

=> НОД (1,33) = 1

* det( ≠ 0

=> НОД (33,40) = 1

* det(

=> НОД (7,33) = 1

У нас сообщение: л и н е й н а я а л г б

=>

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| л | и | н | е | й | н | а | я | а | л | г | б |
| 12 | 9 | 14 | 5 | 10 | 14 | 0 | 32 | 0 | 12 | 3 | 1 |

1. ***Зашифруем сообщение с помощью каждого из ключей, используя метод шифрования Хилла***

Формула:

* **Для :**

=>

mod (33)

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 18 | 21 | 10 | 19 | 31 | 24 | 28 | 32 | 27 | 12 | 23 | 4 |
| С | Ф | Й | Т | Ю | Ч | Ы | Я | Ъ | Л | Ц | Д |

линейнаяалгб сф йт юч ыя ъл цд

* **Для**

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 2 | 22 | 12 | 16 | 30 | 31 | 31 | 23 | 31 | 10 | 29 | 27 |
| С | Ф | Й | Т | Ю | Ч | Ы | Я | Ъ | Л | Ц | Д |

линейнаяалгб вчлпэююцюйьъ

=>

* **Для**

=>

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 2 | 23 | 15 | 15 | 24 | 15 | 0 | 19 | 15 | 27 | 1 | 17 |
| В | Ц | О | О | Ч | О | А | Т | О | Ъ | Б | Р |

линейнаяалгб вцоочоатоъбр

1. ***Расшифруйте каждое из получившихся сообщений, используя обратные*** ***матрицы от матриц-ключей.***

Формула: ,

* **Для :**

=>

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 12 | 9 | 14 | 5 | 10 | 14 | 0 | 32 | 0 | 12 | 3 | 1 |
| л | и | н | е | й | н | а | я | а | л | г | б |

сфйтючыяълцд линейнаяалгб

* **Для :**

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

=>

=>

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 12 | 9 | 14 | 5 | 10 | 14 | 0 | 32 | 0 | 12 | 3 | 1 |
| л | и | н | е | й | н | а | я | а | л | г | б |

вчлпэююцюйьъ линейнаяалгб

* **Для :**

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

)

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 12 | 9 | 14 | 5 | 10 | 14 | 0 | 32 | 0 | 12 | 3 | 1 |
| => | => | => | => | => | => | => | => | => | => | => | => |

вчлпэююцюйьъ линейнаяалгб

### Задание 2

### Задание 3