В этой лабораторной вы познакомитесь с тем, как можно использовать матричное умножение для реализации простых линейных шифров и корректирующих кодов.

Справочная информация:

1. Википедия: Шифр Хилла
2. Wikipedia: Hill cipher
3. Wikipedia: Hamming(7,4)
4. Wikipedia: Hamming code

Задание 1. Шифр Хилла. В этом задании мы займёмся шифрованием.

- Возьмите русский алфавит. Можете добавить в него необходимые вам символы (пробел, точка, цифры), либо наоборот убрать заведомо ненужные буквы. Пронумеруйте знаки получившегося алфавита числами от 0 до $n-1$, где n – общее количество символов в вашем алфавите.
- Придумайте ценное сообщение из 12 символов. Именно его вам нужно будет зашифровать.
- Придумайте три матрицы-ключа: размером 2×2, 3×3 и 4×4. Чтобы всё получилось, проследите за тем, чтобы определители матриц-ключей не имели общих делителей с числом n.
- Зашифруйте ваше сообщение с помощью каждого из ключей, используя метод шифрования Хилла. Представьте три полученных варианта зашифрованного сообщения в виде строчек символов из вашего алфавита.
- Сымитируйте вредоносное вмешательство в зашифрованные сообщения. Замените в каждом из них по три символа на какие-то другие (случайные) символы из вашего алфавита.
- Расшифруйте каждое из получившихся сообщений, используя обратные матрицы от матриц-ключей.

Задание 2. Взлом шифра Хилла. В этом задании мы смоделируем следующую ситуацию: представьте, что у вас на руках два зашифрованных сообщения, в которых использовался шифр Хилла с одним и тем же ключом, который вам неизвестен. И – вот удача! – вам на руки попалась расшифровка (оригинал) одного из этих сообщений. Вообразите себя Аланом Тьюрингом и найдите способ расшифровать второе сообщение.

- Используйте алфавит, который вы составили в предыдущем задании, и какой-нибудь ключ размера 2×2. В идеале автоматизировать процесс так, чтобы ключ сгенерировался случайным образом и вы не знали его до самого конца.
- Возьмите два различных сообщения из 12 символов и зашифруйте их.
- "Забудьте" одно из исходных сообщений. Имея на руках два зашифрованных сообщения и один оригинал, найдите способ расшифровать второе сообщение.

Задание 3. Код Хэмминга. В этом задании мы займёмся кодированием.

- Возьмите русский алфавит из 32 букв. Сопоставьте каждой букве пятибитовый двоичный номер (от 00000 до 11111).
- Придумайте интересное слово из 4 букв. Закодируйте его двоичным кодом (должно получиться 20 символов).
- Разберитесь в том, как работает код Хэмминга $(7, 4)$. Составьте матрицы G и H.
- Дайте развёрнутое объяснение, почему матрицы G и H составлены именно так. Почему у них именно такие строки/столбцы? Выбираются ли эти матрицы единственным образом, или их можно составить по-разному (если да, то как)? Как соотносятся *образ* одной матрицы с *ядром* другой матрицы? Не копируйте текст из внешних источников – разберитесь и напишите своими словами.
- Закодируйте ваше слово из 4 букв, представленное двоичным кодом, с помощью матрицы G (в результате число двоичных символов должно увеличиться).
- Сымитируйте вредоносное вмешательство в закодированное сообщение. Последовательно "испортите" (замените на противоположный)
  - $\rightarrow$ 1 какой-нибудь бит;
  - $\rightarrow$ 2 каких-нибудь бита;
  - $\rightarrow$ 3 каких-нибудь бита;
  - $\rightarrow$ 4 каких-нибудь бита.
- Декодируйте каждое из "испорченных" сообщений, используя матрицу H для поиска и исправления ошибочных битов.
- Переведите каждый из полученных результатов в слово из 4 букв.

Задание 4. Код Хэмминга? Посмотрите первые 90 секунд этого видео. Напишите короткое эссе о том, как можно решить эту задачу с помощью линейной алгебры. Как при этом будет выглядеть матрица H? Какая у неё будет размерность? Какую матричную операцию нужно выполнить второму заключённому, чтобы найти ответ?