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. Проследите за тем, чтобы определители матриц-ключей не имели общих делителей с числом n и были разными между собой.
- 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.

Ожидаемые результаты:

- Приведена таблица соответствий символов алфавита и их численных номеров.
- Приведены исходное сообщение и полученное путём замены символов на соответствующие номера.
- Приведены три матрицы и соответствующие им определители по модулю n.
- Описан подход шифрования Хилла. Для каждого ключа приведены расчёты численных номеров символов зашифрованных сообщений. Приведены сообщения, полученное путем замены номеров на соответствующие им символы.

- Приведены расчёты обратного преобразования ключа. Выполнена проверка дешифрации сообщения.
- Повторно приведены сообщения с выделенными символами, которые будут заменены на случайные. Приведены сообщения с вредоносным вмешательством. Приведены расшифрованные сообщения.

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.

Ожидаемые результаты:

- Приведены оба зашифрованных сообщения. Приведена одна из расшифровок.
- Подробно описан процесс поиска матрицы ключа, основанный на применении свойств линейной алгебры. Приведены соответствующие расчёты. Приведены найденные матрицы ключа и его обратная.
- Расшифровано второе сообщение. Проведена проверка первого сообщения.

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 $(7, 4)$ и каким образом выбираются матрицы. Составьте G и H.
- 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.

Ожидаемые результаты:

- Приведена таблица соответствий символов алфавита и их численных значений.
- Приведены исходное сообщение и полученное путём замены символов на соответствующие двоичные значения.
- Приведены выбранные матрицы G и H. Описано, как эти матрицы были составлены.
- Приведено закодированное сообщение и соответствующий расчёт.
- Повторно приведен двоичный код с выделенными значениями, которые будут заменены на обратные. Приведены декодированные сообщения с вредоносным вмешательством.
- Приведены расчеты, необходимые для поиска испорченных символов. Приведены двоичные значения «исправленного» кода и декодированы в соответствующие символы.

Контрольные вопросы по проделанной работе:

- Что такое линейное преобразование? Что такое векторное пространство? В поле каких чисел мы работаем в каждом задании этой работы?
- Как кодируются и декодируются сообщения методом шифрования Хилла?
- Как находить обратную матрицу, когда она существует? Почему определитель не должен иметь общих делителей с числом n?
- Что такое rank матрицы и как он связан с определителем?
- Что такое Алгоритм Евклида и как может быть применён при решении первого задания?
- На какие части сообщения влияют ошибки при дешифрации? Какая зависимость?
- Как подобрать матрицу ключа, чтобы одна ошибка в коде соответствовала одной ошибке в дешифрованном сообщении?
- Что такое линейно (не)зависимые векторы? Чему равен определитель матрицы, состоящей из линейно зависимых столбцов?
- Матричное представление линейной системы уравнений и их аналитическое решение.
- Как составляются матрицы G и H, за что они отвечают?
- Что такое линейная оболочка (Span)? Что такое Range (Im) и Nullspace (Ker) матрицы? Для каких матриц из третьего задания эти пространства совпадают и почему?
- Сколько можно найти ошибок в сообщении кода Хэмминга? Как их найти и устранить? Как обратно восстановить сообщение?