2) структурирование урока: разделение на вводную часть, основную часть и заключение обеспечивает логичность и последовательность;

3) использование интерактивных методов обучения: групповые задания и обсуждения повышают активность учащихся;

4) визуальные средства: диаграммы, графики и анимации помогают лучше усвоить материал;

5) проверка понимания: краткие тесты и самопроверка позволяют оценить уровень усвоения материала.

УДК 512.624, 519.682

А. М. АНТОНЮК, А. А. ТРОФИМУК
Беларусь, Брест, БрГУ имени А. С. Пушкина

ПОЛИГРАММНЫЙ ШИФР ХИЛЛА

Шифр Хилла представляет собой полиграммный метод шифрования, основанный на применении линейной алгебры над конечными полями. Разработанный Лестером Хиллом в 1929 году, данный алгоритм относится к классу блочных шифров и демонстрирует устойчивость к частотному криптоанализу при корректном выборе параметров. В работе рассматриваются математические основы шифра, процедуры шифрования и дешифрования, а также осуществлена его реализация.

Описание шифра Хилла

В шифре Хилла [1] текст предварительно преобразуют в цифровую форму и разбивают на последовательности (блоки) по n последовательных цифр. Такие последовательности называются n-граммами. Выбирают обратимую по модулю m $(n\times n)$-матрицу $A = (a_{ij})$, где m – число букв в алфавите. Выбирают случайный n-вектор $\mathbf{f} = (f_1, \ldots, f_n)$, после чего n-грамма открытого текста $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ заменяется n-граммой шифрованного текста $\mathbf{y} = (y_1, y_2, \ldots, y_n)$ по формуле:

$$\mathbf{y} = \mathbf{x}A + \mathbf{f} \mod m. \tag{1}$$

Расшифрование проводится по правилу:

$$\mathbf{x} = (\mathbf{y} - \mathbf{f})A^{-1} \mod m. \tag{2}$$

Соответствие букв и их положения в алфавите

Для английского алфавита ($m = 26$) соответствие букв и чисел следующее:

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Пример шифрования

Преобразуем английский алфавит в числовую форму ($m = 26$) следующим образом: $A \to 0$, $B \to 1$, $C \to 2$, $\ldots$, $Z \to 25$. Выберем для примера $n = 2$. Запишем слово «STUDENTS». Каждой букве поставим в соответствие её номер в алфавите:

$$\text{S} = 18,\ \text{T} = 19,\ \text{U} = 20,\ \text{D} = 3,\ \text{E} = 4,\ \text{N} = 13,\ \text{T} = 19,\ \text{S} = 18$$

Выберем квадратную матрицу шифрования A в виде:

$$A = \begin{pmatrix} 4 & 5 \\ 3 & 4 \end{pmatrix}.$$

Эта матрица обратима по mod 26, так как её определитель равен 1 и взаимно прост с $m = 26$. Обратная матрица равна:

$$A^{-1} = \begin{pmatrix} 4 & -5 \\ -3 & 4 \end{pmatrix}.$$

Пусть $\mathbf{f}$ – нулевой вектор. Тогда из (1) следует:

$$\mathbf{y} = \mathbf{x}A \mod m = (18, 19) \cdot \begin{pmatrix} 4 & 5 \\ 3 & 4 \end{pmatrix} \mod 26 = (25, 10).$$

Выполняем это действие до последней пары букв:

$$(20, 3) \cdot \begin{pmatrix} 4 & 5 \\ 3 & 4 \end{pmatrix} \mod 26 = (11, 8),$$

$$(4, 13) \cdot \begin{pmatrix} 4 & 5 \\ 3 & 4 \end{pmatrix} \mod 26 = (3, 20),$$

$$(19, 18) \cdot \begin{pmatrix} 4 & 5 \\ 3 & 4 \end{pmatrix} \mod 26 = (0, 11).$$

Результатом является: $(25, 10)$, $(11, 8)$, $(3, 20)$, $(0, 11)$. Сопоставим числа с буквами по таблице:

$$25 = \text{Z},\ 10 = \text{K},\ 11 = \text{L},\ 8 = \text{I},\ 3 = \text{D},\ 20 = \text{U},\ 0 = \text{A},\ 11 = \text{L}.$$

Итог: ZKLIDUAL – зашифрованная строка.

Пример расшифрования

Чтобы расшифровать строку ZKLIDUAL, нужно использовать формулу (2). Используя алгоритм, приведенный выше, мы получим:

$$(18{,}19)\ (20{,}3)\ (4{,}13)\ (19{,}18) = \text{STUDENTS}.$$

Реализация

Разработано консольное приложение, выполняющее шифрование и расшифрование по алгоритму Хилла. Программа обрабатывает следующие ошибки:

1) ввод не целых чисел в матрицу;

2) отсутствие обратной матрицы.

На рисунках 1 и 2 показаны примеры работы программы, включая обработку ошибочного ввода. При возникновении ошибок программа запрашивает повторный ввод корректных данных.

```
Введите текст для шифрования: students
Введите элементы матрицы 2x2 (4 числа через пробел): 1.1 0 3 4
Ошибка ввода! Пожалуйста, введите 4 целых числа.
Введите элементы матрицы 2x2 (4 числа через пробел): 1 1 1 1
Ошибка: Определитель матрицы (0) не имеет обратного по модулю 26.
Попробуйте другую матрицу.
```

Рисунок 1 – Пример работы программы

```
Введите текст для шифрования: students
Введите элементы матрицы 2x2 (4 числа через пробел): 4 5 3 4

Обработанный текст: STUDENTS
Ключевая матрица:
[4 5]
[3 4]

Зашифрованный текст: ZKLIDUAL
Расшифрованный текст: STUDENTS
```

Рисунок 2 – Пример ошибочного ввода данных

Шифр Хилла представляет особую ценность в учебном процессе как наглядный пример соединения теоретических основ линейной алгебры с практическими задачами криптографии. Этот алгоритм демонстрирует применение матричных операций, модульной арифметики и теории обратимости матриц в реальных вычислительных системах, что делает его исключительно полезным для обучения фундаментальным концепциям алгебры, теории чисел и программирования.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Криптографические методы защиты информации: учеб. пособие / С. М. Владимиров, Э. М. Габидулин, А. И. Колыбельников, А. С. Кшевецкий. – М. : МФТИ, 2016. – 265 с.

УДК 371.31

А. М. АСТРАХАНЦЕВА, Е. В. ПАНТЕЛЕЕВА
Беларусь, Брест, БрГУ имени А. С. Пушкина

МЕТОДИЧЕСКИЕ АСПЕКТЫ ПОДГОТОВКИ К ЦЭ/ЦТ ПО МАТЕМАТИКЕ С АКЦЕНТОМ НА ПРОИЗВОДНУЮ

Подготовка учащихся к централизованному экзамену (ЦЭ) и централизованному тестированию (ЦТ) по математике представляет собой сложный и многогранный процесс, который требует от педагога не только глубоких предметных знаний, но и владения современными методиками обучения. В структуре экзаменационных заданий особое место занимает тема производной.

Анализ результатов централизованного тестирования показывает, что задания по теме производной традиционно вызывают затруднения. Трудности, с которыми сталкиваются учащиеся, могут быть следующими: недостаточное понимание смысла производной, особенно скорости изменения функции или углового коэффициента касательной; ошибки при применении правил дифференцирования, в частности при работе с составными, дробными и тригонометрическими функциями; затруднения при исследовании функций: нахождение интервалов возрастания и убывания, точек экстремума и построение графиков.