Лабораторная работа № 9

«Разработка классической сети Фейштеля»

9.1 Разработка программы генерации 64 битного секретного ключа

Первый шаг. Для полного связного неориентированного графа (гамильтоново куба), представленного матрицей смежности (рисунок 1), необходимо получить все возможные гамильтоновы циклы для вершины графа «1».

	1	2	3	4	5	6	7	8
1	-	1	1				1	
2	1	-		1				1
3	1		-	1	1			
4		1	1	-		1		
5			1		-	1	1	
6				1	1	-		1
7	1				1		-	1
8		1				1	1	-

Рисунок 1 – Матрица смежности неориентированного графа

Программа должна на основе выбранного алгоритма определить 12 гамильтоновых циклов для выбранной вершины. Нумерация циклов должна быть ранжирована по возрастанию.

Например: 1. 1-2-4…, 3. 1-2-8…, 5. 1-3-4…, 7. 1-3-5…, 9. 1-7-5…,

11. 1-7-8…

Из 12 гамильтоновых циклов необходимо выбрать два по следующему правилу:

- Если текущая дата месяца 1<= N <= 11, то номер гамильтоново цикла будет N и N+1;

– Если текущая дата N равна 12 , тогда номер цикла равен N и N-11;
– Если текущая дата месяца 13<= N <=31, то номер цикла равен N mod 12 и N mod 12+1.

Результатом такого выбора будут последовательности номеров вершин графа, входящих в гамильтоновы циклы от 1 до 8. Эти цепочки чисел являются ключами $К_1$ и $К_2$.

Например: $К_1$ = 13465782 (номера строк матрицы) и

$К_2$ = 13578642 (номера столбцов).

Второй шаг. Представить исходную матрицу 64 битного ключа в следующем виде (рисунок 2). Матрица получена в качестве примера для текущей даты 15 февраля 2022 года.

		Коды ASCII							
Число даты	1	0	0	1	1	0	0	0	1
	5	0	0	1	1	0	1	0	1
Первые три буквы месяца	Ф	1	0	0	1	0	1	0	0
	е	1	0	1	0	0	1	0	1
	в	1	0	1	0	0	0	1	0
Три последние цифры года	0	0	0	1	1	0	0	0	0
	2	0	0	1	1	0	0	1	0
	2	0	0	1	1	0	0	1	0

Рисунок 2 – Исходная матрица 64 битного ключа

Третий шаг. Получение секретного ключа для первого раунда сети Фейштеля.

Для матрицы (рисунок 2) применить **комбинированный (композиционный) метод шифрования** перестановки по строкам и

столбцам. В качестве ключей для перестановки использовать выбранные на первом шаге ключи $К_1$ и $К_2$.

После перестановки реализовать циклический сдвиг влево на 3 символа для нечётных номеров матрицы и сдвиг вправо на 3 символа для чётных. В результате получим ключ для первого раунда $К_{1р}$.

Четвёртый шаг. Для реализации процедуры шифрования получить ключи для второго и третьего раунда по следующему правилу:

- $К_{2р} = К_{1р} \oplus$ Борислав;
- $К_{3р} = К_{2р} \oplus$ Антонина.

Пятый шаг. Разработать программу шифрования массива с помощью классической сети Фейштеля (рисунок 3) для трёх раундов при следующих условиях:

– Разбить исходный текст на два блока по 64 бит каждый;

– К правой части применить перестановку комбинированным шрифтом при значении ключей $К_1 = 5$ (все шифруемые символы заменяются по методу Цезаря с ключом 5) и $К_2 = 74362158$ (в блоке из восьми символов производится перестановка с ключом 74362158);

– Ключ первого раунда $К_{1р}$ складывается по модулю 2 с результатом, полученным на предыдущем шаге;

– К полученному результату шифрования применить двойную перестановку с теме же ключами $К_1 = 5$ и $К_2 = 74362158$;

– Поменять блоки местами и повторить шаги алгоритма с ключами для второго и третьего раундов;

– Исходный текст для шифрования выбрать из таблицы 1. Номера в таблице соответствую вашим номерам в списке группы. Для кодировки использовать русский алфавит на 33 символа и таблицу ASCII.

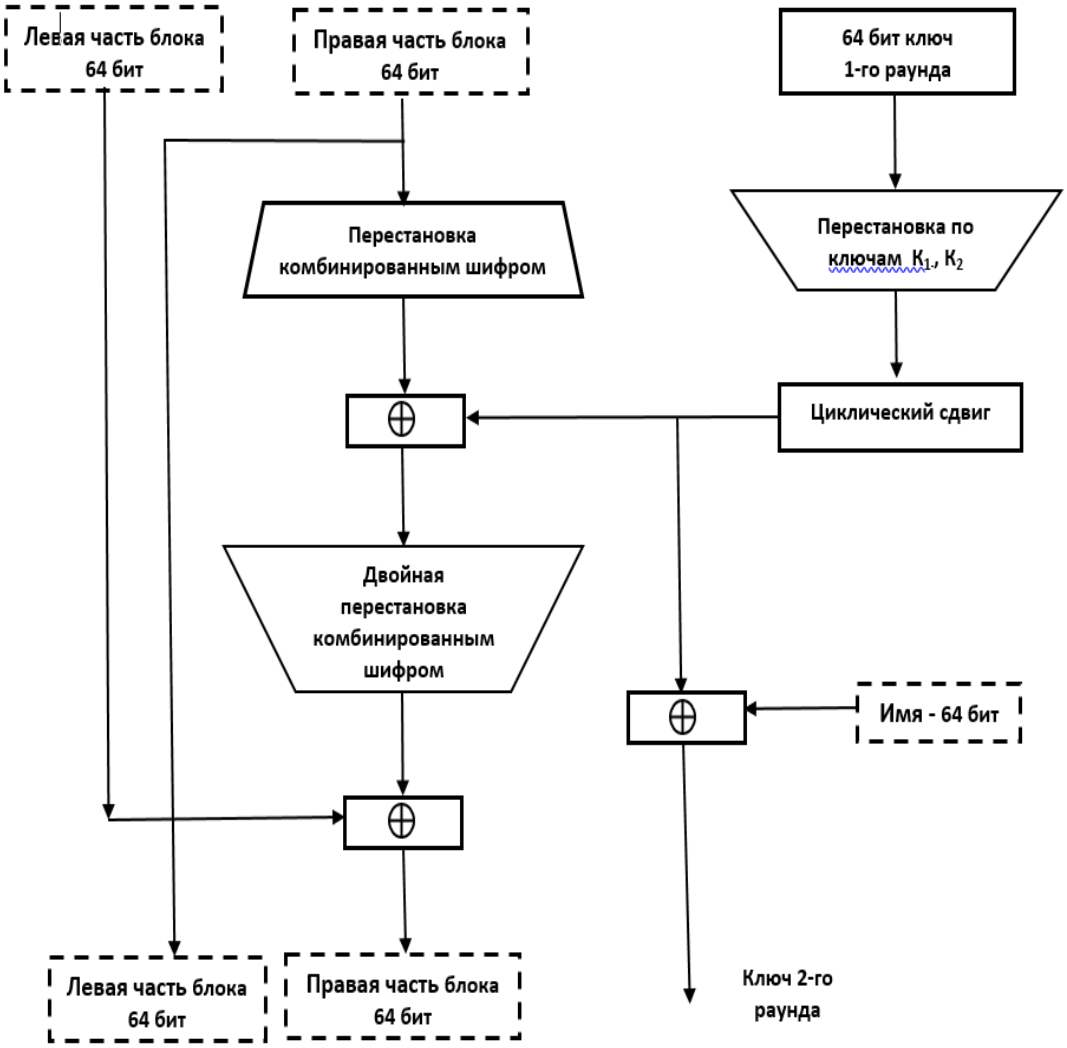

Рисунок 3 – Алгоритм шифрования Фейштеля

Таблица 1- Исходный текст для шифрования

№ п/п	ИТ	№ п/п	ИТ	№ п/п	ИТ
1	Гидрометаллургия	9	Дистрибутивность	17	Демонстрирование
2	Дезинфицирование	10	Информационность	18	Детерминирование
3	Дезинфицирование	11	Альтернативность	19	Гидромеханизатор
4	Законодательство	12	Ангажированность	20	Знаменательность
5	Интеллектуальный	13	Гидромеханизация	21	Демонстрирование
6	Капиталовложение	14	Изобретательство	22	Индивидуальность
7	Автосигнализация	15	Кардиостимулятор	23	Действительность
8	Гипнотизирование	16	Консервативность	24	Аргументирование