Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

Кафедра информатики и прикладной математики

Методы и средства защиты компьютерной информации

Перестановки

Лабораторная работа 5

Вариант 17

Старался: Шкаруба Н.Е.

Группа: P3418

Цель работы:

Научиться методу шифрования и расшифровки текста методом перестановок.

Простые перестановки

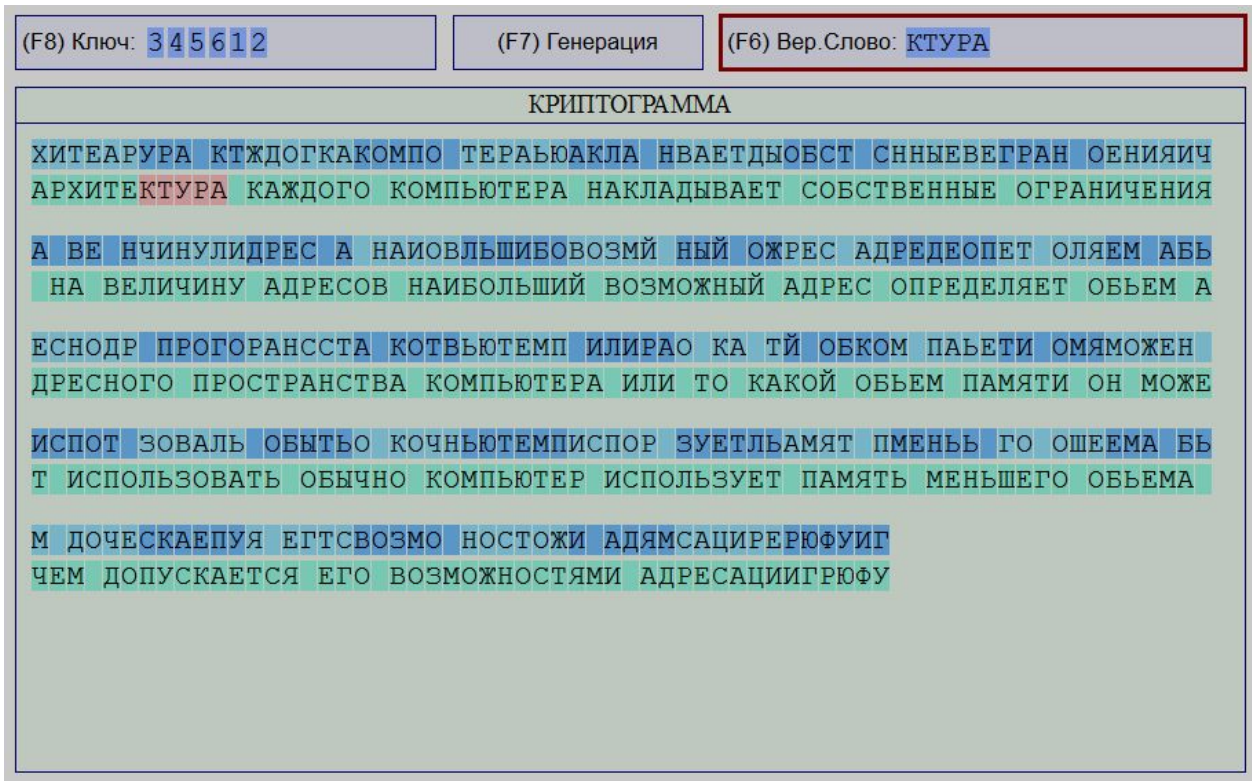
Исходный текст

Ключ

345612

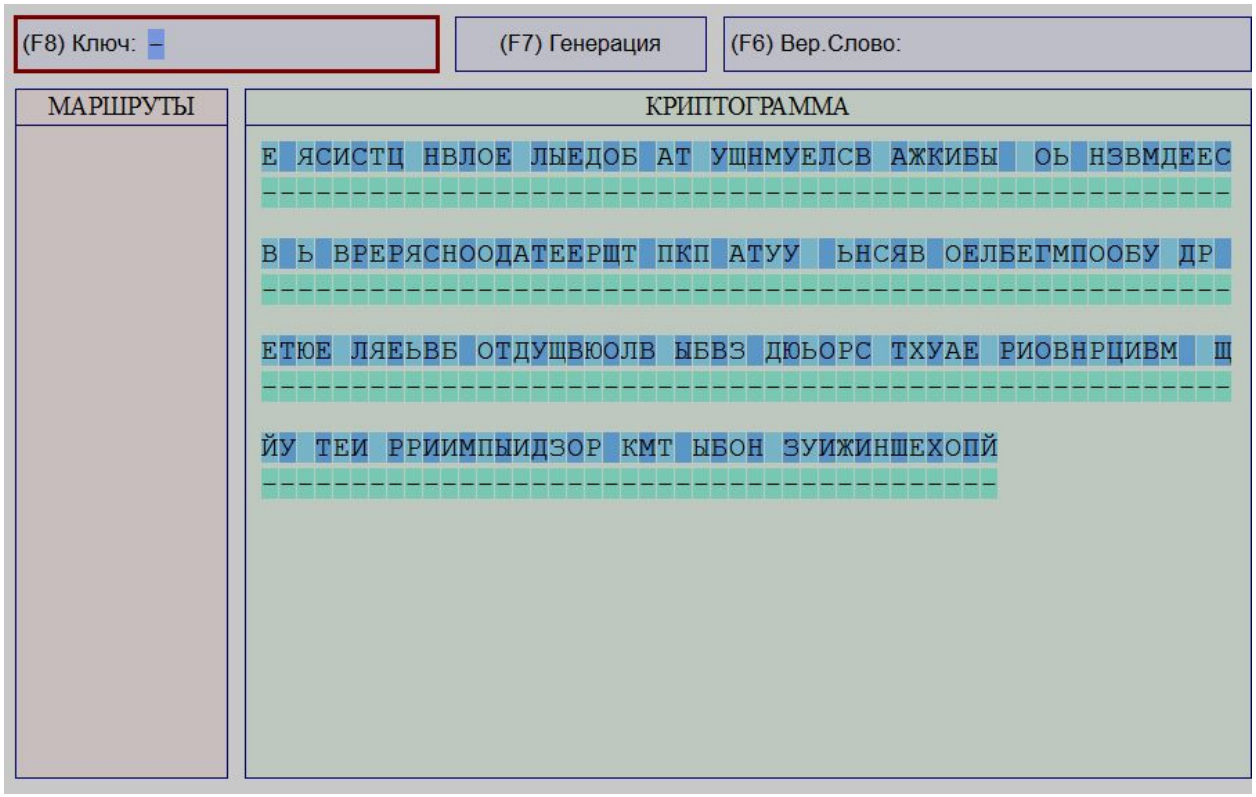
Протокол криптоанализа

1) В первом слове я увидел вначале ЛИТЕРАТУРА, потом АРХИТЕКТУРА, поэтому я начал играться с длинами ключа, и в итоге выбрал длину 5, потом 6, и сделал вероятностное слово КТУРА.



Пути Гамильтона

Исходный текст



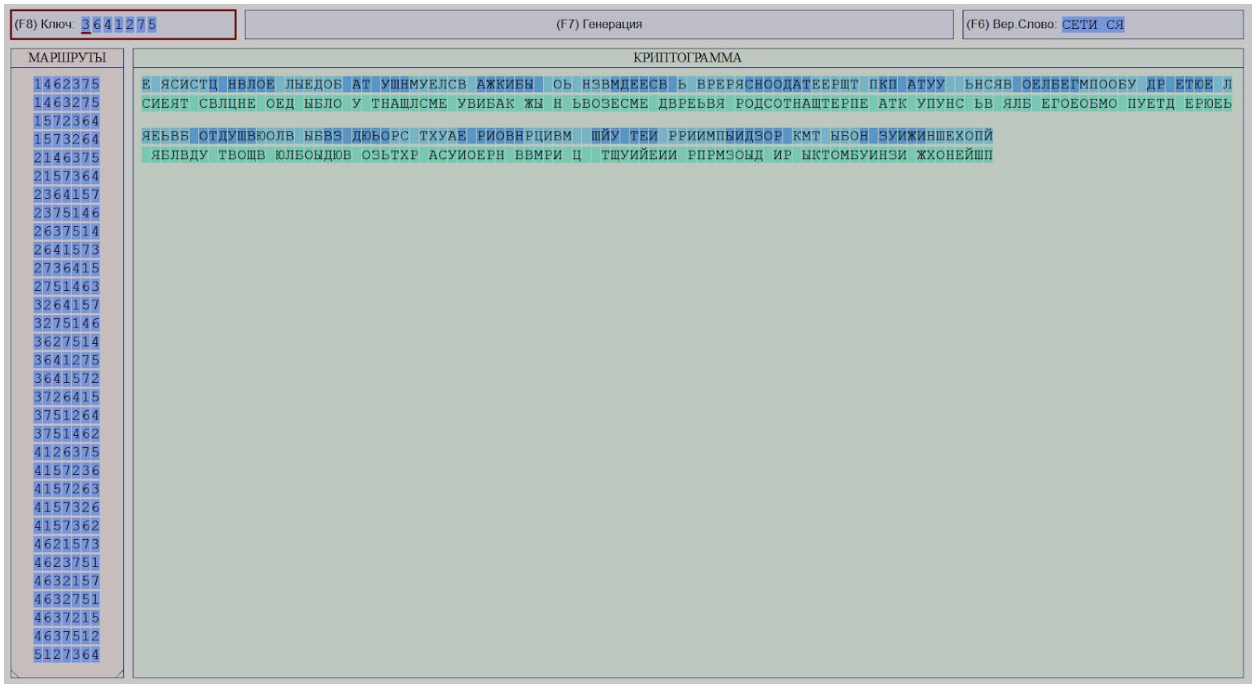
Ключ

4637215

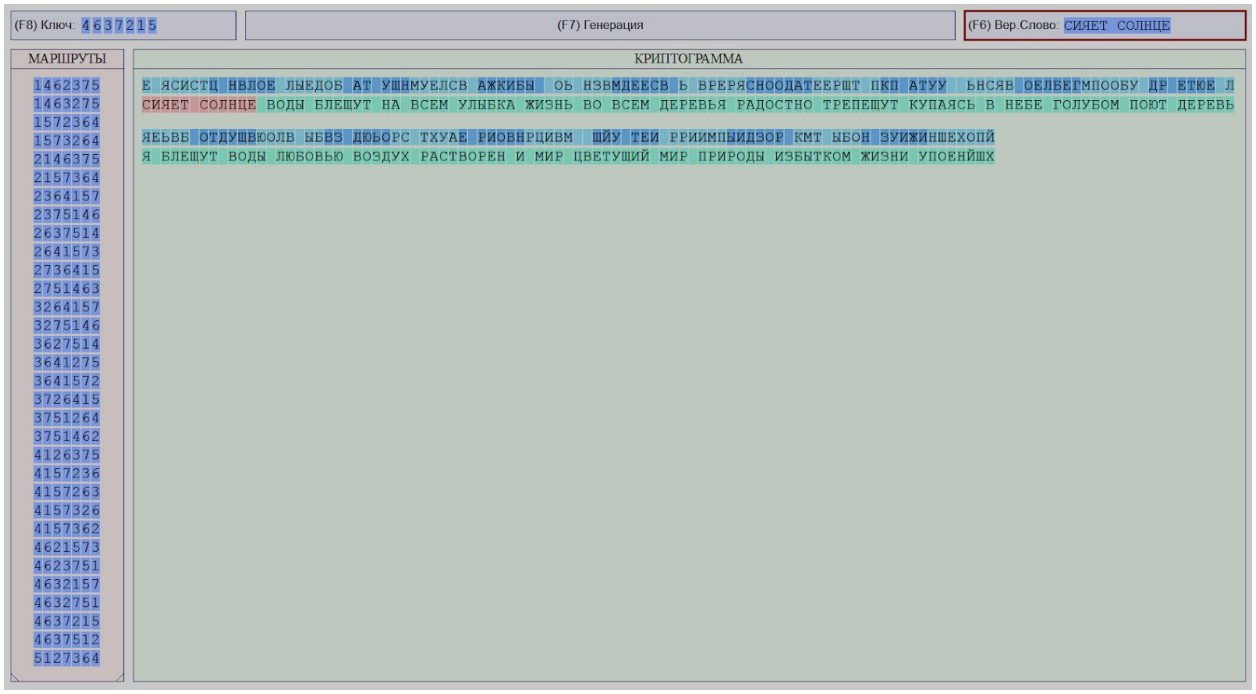
Протокол криптоанализа

1) Построил граф, я получил свои маршруты, но пока не решил ими пользоваться, ибо в прошлом задании я разгадал довольно просто. Попробовав минут 15 угадывать по началу текста - бросил

2) Стал перебирать маршруты, и в итоге натолкнулся на такой

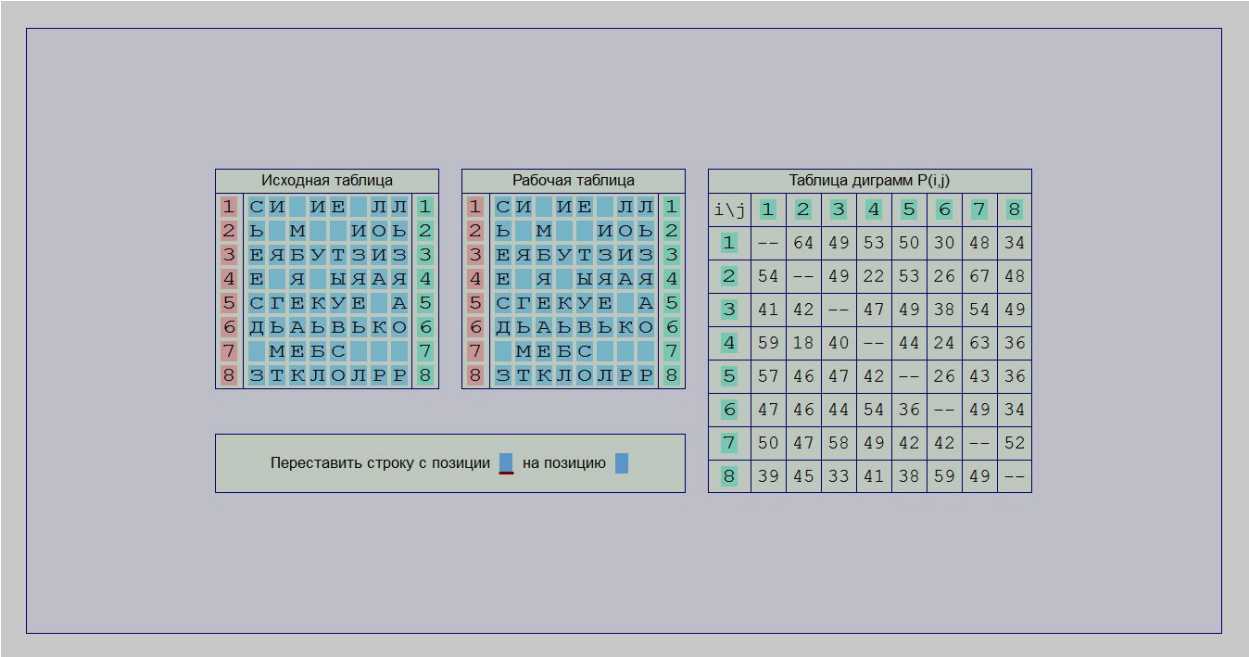


3) Увидел СИЯЕТ СОЛНЦЕ, и разгадал криптограмму



Табличные перестановки

Исходный текст



Исходная таблица								
1	С	И		И	Е		Л	Л	1
2	Ь		М			И	О	Ь	2
3	Е	Я	Б	У	Т	З	И	З	3
4	Е		Я		Ы	Я	А	Я	4
5	С	Г	Е	К	У	Е		А	5
6	Д	Ь	А	Ь	В	Ь	К	О	6
7		М	Е	Б	С				7
8	З	Т	К	Л	О	Л	Р	Р	8

Рабочая таблица								
1	С	И		И	Е		Л	Л	1
2	Ь		М			И	О	Ь	2
3	Е	Я	Б	У	Т	З	И	З	3
4	Е		Я		Ы	Я	А	Я	4
5	С	Г	Е	К	У	Е		А	5
6	Д	Ь	А	Ь	В	Ь	К	О	6
7		М	Е	Б	С				7
8	З	Т	К	Л	О	Л	Р	Р	8

Таблица диграмм P(i,j)								
i\j	1	2	3	4	5	6	7	8
1	--	64	49	53	50	30	48	34
2	54	--	49	22	53	26	67	48
3	41	42	--	47	49	38	54	49
4	59	18	40	--	44	24	63	36
5	57	46	47	42	--	26	43	36
6	47	46	44	54	36	--	49	34
7	50	47	58	49	42	42	--	52
8	39	45	33	41	38	59	49	--

Ключ

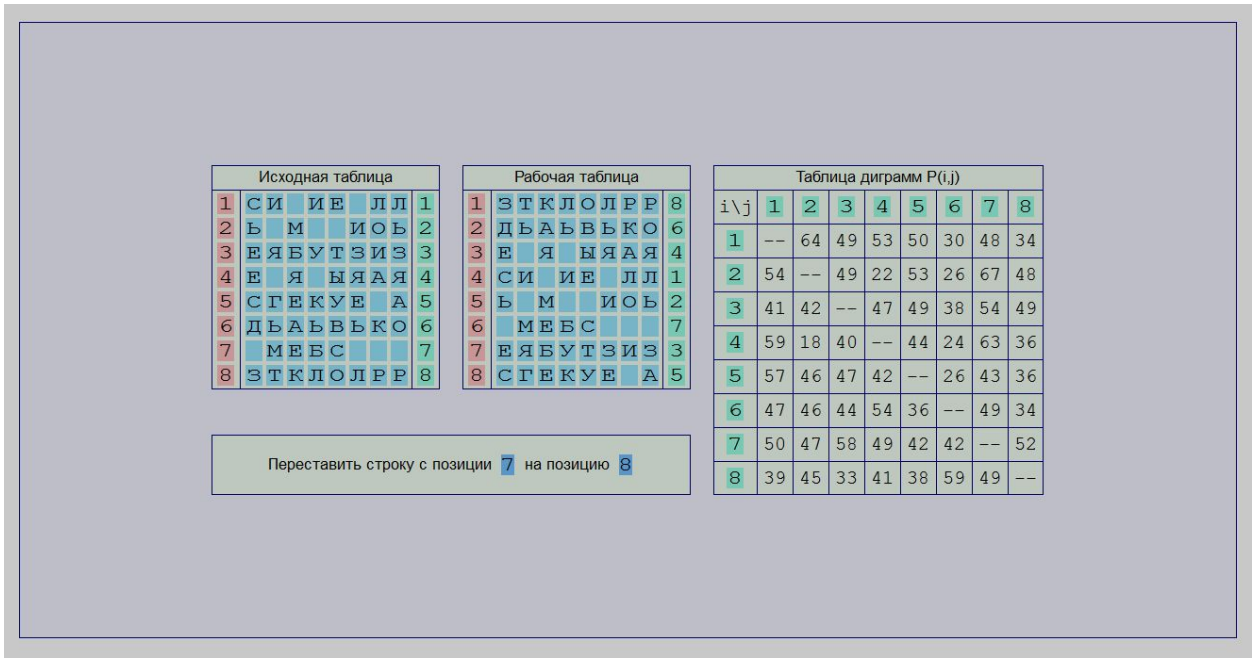
86312735

Протокол криптоанализа

1) Если честно, я так и не разобрался с таблицей, но решил просто поугадывать.

2) Вначале в последнем столбце я увидел слово РОЗА, и переставил, но ничего так и не нашел. Зато в первом столбце я увидел слово ЗДЕСЬ, поигравшись с которым я

расшифровал криптограмму



Исходная таблица

1	С	И		И	Е		Л	Л	1
2	Ь		М			И	О	Ь	2
3	Е	Я	Б	У	Т	З	И	З	3
4	Е		Я		Ы	Я	А	Я	4
5	С	Г	Е	К	У	Е		А	5
6	Д	Ь	А	Ь	В	Ь	К	О	6
7		М	Е	Б	С				7
8	З	Т	К	Л	О	Л	Р	Р	8

Рабочая таблица

1	З	Т	К	Л	О	Л	Р	Р	8
2	Д	Ь	А	Ь	В	Ь	К	О	6
3	Е		Я		Ы	Я	А	Я	4
4	С	И		И	Е		Л	Л	1
5	Ь		М			И	О	Ь	2
6		М	Е	Б	С				7
7	Е	Я	Б	У	Т	З	И	З	3
8	С	Г	Е	К	У	Е		А	5

Переставить строку с позиции 7 на позицию 8

Таблица диграмм P(i,j)

i\j	1	2	3	4	5	6	7	8
1	--	64	49	53	50	30	48	34
2	54	--	49	22	53	26	67	48
3	41	42	--	47	49	38	54	49
4	59	18	40	--	44	24	63	36
5	57	46	47	42	--	26	43	36
6	47	46	44	54	36	--	49	34
7	50	47	58	49	42	42	--	52
8	39	45	33	41	38	59	49	--