Национальный исследовательский университет информационных технологий,
механики и оптики.
Кафедра вычислительной техники.
Методы и средства защиты компьютерной информации.

Лабораторная работа №5

Перестановки.

11 вариант

Работу выполнил студент группы P3415
Халанский Дмитрий

2017

1. Цель работы

- Расшифровать криптограмму, зашифрованную методом перестановок;
- Расшифровать криптограмму, полученную методом перестановок по путям Гамильтона;
- Расшифровать криптограмму, зашифрованную методом табличной перестановки.

2. Простая перестановка

2.1. Исходный текст

НАША ИСХОДНАЯ ПРАГМАТИЧЕСКАЯ ЗАДАЧА АНАЛИЗ ЕСТЕСТВЕННОГО ЯЗЫКА С ЦЕЛЬЮ ПОСТРОЕНИЯ ДЕЙСТВУЮЩИХ СИСТЕМ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ОСНОВА ТАКИХ СИСТЕМ АЛГОРИТМЫ АНАЛИЗА И ПОРОЖДЕНИЯ СТРУКТУР ЕСТЕСТВЕННОГО ЯЗЫКА СОЗДАТЬ ТАКИЕ АЛГОРИТМЫ НЕВОЗМОЖНО БЕЗ ЧЕТКОГО ПРЕДСТАВЛЕНИЯ ПРОЦЕССОВ ПРОИСХОДЯЩИХ В МЫШЛЕНИИ И ЯЗЫКЕКЬ

2.2. Ключ

261534

2.3. Протокол криптоанализа

Мы обнаружили группу символов, которые показались анаграммой формы слова «невозможно». Перебирая вероятные длины ключей и пользуясь автоматическим поиском слов, мы добились обнаружения ключа длиной 6, при котором слово НЕВОЗМОЖ обнаружилось, и это привело к расшифровке текста.

3. Перестановка с использованием путей Гамильтона

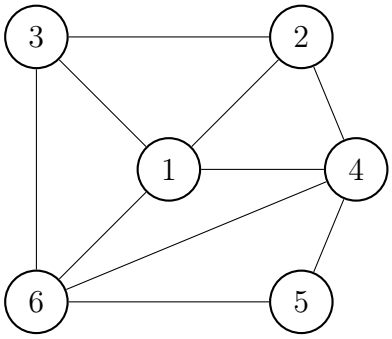
3.1. Исходный текст

ЭТО БЫЛО ЭТО БЫЛО В ТОЙ СТРАНЕ О КОТОРОЙ НЕ ЗАГРЕЗИШЬ И ВО СНЕ Я ПРИДУМАЛ ЭТО ГЛЯДЯ НА ТВОИ КОСЫ КОЛЬЦА ОГНЕВЕЮЩЕЙ ЗМЕИ НА ТВОИ ЗЕЛЕНОВАТЫЕ ГЛАЗА КАК ПЕРСИДСКАЯ БОЛЬНАЯ БИРЮЗА МОЖЕТ БЫТЬ ТОТ ЛЕС ДУША ТВОЯ МОЖЕТ БЫТЬ ТОТ ЛЕС ЛЮБОВЬ МОЯ ИЛИ МОЖЕТ БЫТЬ КОГДА УМРЕМ МЫ В ТОТ ЛЕС НАПРАВИМСЯ ВДВОЕМ Д

3.2. Ключ

136542

3.3. Исходный граф



	1	2	3	4	5	6
1	-	+	+	+	-	+
2	+	-	+	+	-	-
3	+	+	-	-	-	+
4	+	+	-	-	+	+
5	-	-	-	+	-	+
6	+	-	+	+	+	-

3.4. Протокол криптоанализа

После сообщения программе сведений о графе мы перебрали несколько начальных вариантов, пытаясь найти знакомые последовательности символов.

На комбинации `125436` мы обнаружили слово КОТОООЙ. Тут же мы попробовали автоматический поиск слова КОТОРОЙ, что привело к полной расшифровке.

4. Табличная перестановка

4.1. Исходный текст

КАК ВСЕ И ПОЭЗИЯ ТЕРЯЕТ СВОЮ СВЯТУЮ ПРОСТОТУ КОГДА ИЗ ПОЭЗИИ ДЕЛ

4.2. Ключ

58672431

4.3. Таблица вероятностей

	1	2	3	4	5	6	7	8
1	_ _	48	51	44	29	36	41	46
2	47	_ _	49	52	51	45	39	56
3	60	48	_ _	56	45	46	45	45
4	51	44	61	_ _	48	36	54	49
5	44	30	50	47	_ _	34	44	54
6	44	47	56	36	45	_ _	53	52
7	38	60	41	56	45	48	_ _	42
8	50	57	41	58	51	62	47	_ _

4.4. Протокол криптоанализа

Мы обнаружили в третьем столбце явную анаграммую слова «теряет». Мы переставили строки так, чтобы по краям находились пробелы, а между ними располагалось данное слово. Затем мы переставили пробелы так, чтобы в первом столбце первым символом был не пробел. Так мы угадали, что в первом столбце написано «как все». После этого мы переставили строки, в которых в третьем столбце были буквы «т» и «е», чтобы добиться этих слов. Так мы получили правильный текст.