Университет ИТМО

Кафедра ВТ

Методы и средства защиты компьютерной информации

Лабораторная работа №5

Вариант 9

Выполнил: Фролов Сергей

Гр. Р3415

2017

Задание

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

Выполнение

1. **Простая перестановка**

Криптограмма:

ЕЩУССЮУВТТОНМГ РП ИО НИПЧОК ТОМЫР ОЬЛОЗПТАВЕОМ ЬОЛ ТЕНЖАЗ ХЕТЕТЬОТСОА ТЯЛЬВЕЛСД ВС ОЫ ОГПЕЫБЕВРЯИН А ТУИТЖЕНЕ ИНАЕЛСАРК ЬТЫ РЙОВ СЕРДСАЕЛЭК НОРНТП ЙОО ЫТЧЧЫБО ТС ЕТН ЬТЖАВТРОЕПС АЙИ А МБОЕХНМИДОО ЬТПСЧУЛИОИ ЬНТМРОАФ ЮИСЦЙАСТ ОК ТАЙЫР ОЬРАИВТЕУ РЕВТТОЗ ВА ИСИМВИТС ОС ТТОЫНА РК ЗОИОРОЙТПТОР ЕЛВНАПАЗР ЧЭСМО

Открытый текст:

СУЩЕСТВУЮТ МНОГО ПРИЧИН ПО КОТОРЫМ ПОЛЬЗОВАТЕЛЬ МОЖЕТ НЕ ЗАХОТЕТЬ ОСТАВЛЯТЬ СЛЕДЫ СВОЕГО ПРЕБЫВАНИЯ ТУТ И НЕЖЕЛАНИЕ РАСКРЫТЬ СВОЙ АДРЕС ЭЛЕКТРОННОЙ ПОЧТЫ ЧТОБЫ НЕ СТАТЬ ЖЕРТВОЙ СПАМА И НЕОБХОДИМОСТЬ ПОЛУЧИТЬ ИНФОРМАЦИЮ С САЙТА КОТОРЫЙ ВАРЬИРУЕТ ОТВЕТ В ЗАВИСИМОСТИ ОТ СТРАНЫ ИЗ КОТОРОЙ ОТПРАВЛЕН ЗАПРОС

Ключ:

43251

Протокол криптоанализа

Вероятные длины ключа были 1 и 5. Очевидно, 5 ближе к верной длине. Затем в начале было замечено зашифрованное слово СУЩЕСТВУЮТ из 10 букв, с помощью которого стало довольно просто подобрать ключ.

2. Перестановка с использованием путей Гамильтона

Криптограмма:

ОИНКОГ БЕН ДУЕ ТВОДМР ЕКМОЕМС УРЕЕД КОНИ НИЗМЙИ ЬЕДНВ ОКСВНЗОР МПЕОМЕ ЕНАЗДУРЕНЫТХРГ АИДНЛТ ОКЬОЛБ ЕХЫ РОМКХЫ ЬОКМВЕ ТЫБСЫРЙОП РЕМЛМКЬ ХАО ОВЙОТЛ КЬОРКЫСИШ ЕНГКИ ОРМР ЕКШЫ Н ИСГЕАКН ИГООИ ЯПТА ЬЗЕЧР ИТТНИЕ ЙИПОЯЗЬТ ВАЕТТРИМ НПЙО ОРШООЛГНДЕН ЕУНЫЬ ЕИЕДЛИ АЗЫМ ЙНИОЯС

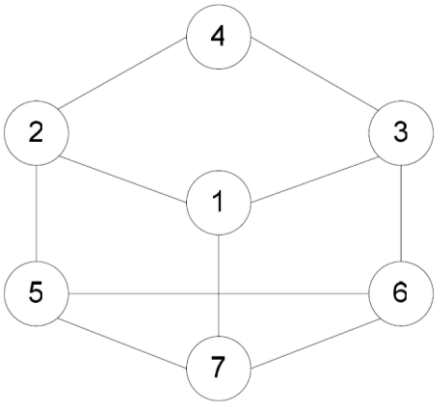
Открытый текст:

НИКОГО НЕ БУДЕТ В ДОМЕ КРОМЕ СУМЕРЕК ОДИН ЗИМНИЙ ДЕНЬ В СКВОЗНОМ ПРОЕМЕ НЕЗАДЕРНУТЫХ ГАРДИН ТОЛЬКО БЕЛЫХ МОКРЫХ КОМЬЕВ БЫСТРЫЙ ПРОМЕЛЬК МАХОВОЙ ТОЛЬКО КРЫШИ СНЕГ И КРОМЕ КРЫШ И СНЕГА НИКОГО И ОПЯТЬ ЗАЧЕРТИТ ИНЕЙ И ОПЯТЬ ЗАВЕРТИТ МНОЙ ПРОШЛОГОДНЕЕ УНЫНЬЕ И ДЕЛА ЗИМЫ ИНОЙСЯ

Ключ:

4213657

Исходный граф



	1	**2**	**3**	**4**	**5**	**6**	**7**
1	-	+	+	-	-	-	+
2	+	-	-	+	+	-	-
3	+	-	-	+	-	+	-
4	-	+	+	-	-	-	-
5	-	+	-	-	-	+	+
6	-	-	+	-	+	-	+
7	+	-	-	-	+	+	-

Протокол криптоанализа

После ввода данных о графе программе перебираем несколько вариантов ключа. При одном из этих вариантов третье слово становится похоже на слово БУДЕТ. После ввода в поиск этого слова, текст расшифровывается.

3. Табличная перестановка

Криптограмма:

ПИИВНАРССКНРЕИМ НЖЛООПО ИРКА ВЛНМЮВОС АУ ГУАМБМИ ЧАЛО ИПЯЛСЯНР

Открытый текст:

ИСПРАВНИК СМИРЕННО ПОЛОЖИЛ В КАРМАН СВОЮ БУМАГУ И МОЛЧА ПРИНЯЛСЯ

Ключ:

28176453

Таблица вероятностей

Таблица диграмм P(i,j)								
i\j	1	2	3	4	5	6	7	8
1	--	52	53	34	51	42	61	54
2	55	--	33	48	53	50	39	62
3	34	37	--	30	44	43	43	30
4	43	41	42	--	53	51	37	39
5	49	54	58	55	--	54	46	47
6	33	50	49	49	51	--	57	51
7	51	45	45	37	52	62	--	50
8	62	55	40	44	50	52	48	--

Протокол криптоанализа

Судя по исходной таблице первый и последний столбцы не содержат пробелов, значит в них довольно длинные слова (минимум 8 букв). По последнему столбцу довольно просто из букв составилось слово ПРИНЯЛСЯ, благодаря чему был разгадан весь текст.