

**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: Р3418

Цель работы:

Научиться методу шифрования и расшифровки текста методом перестановок.

Простые перестановки

Исходный текст

(F8) Ключ: <input type="text" value="-"/>	(F7) Генерация	(F6) Вер. Слово:
КРИПТОГРАММА		
ХИТЕАРУРА КТЖДОГКАКОМПО ТЕРАЬКАКЛА НВАЕТДЫОБСТ СННЬЕВЕГРАН ОЕНИЯИЧ -----		
А ВЕ НЧИНУЛИДРЕС А НАИОВЛЬШИБОВОЗМЙ НЬИ ОЖРЕС АДРЕДЕОПЕТ ОЛЯЕМ АБЬ -----		
ЕСНОДР ПРОГОРАНССТА КОТВЬЮТЕМП ИЛИРАО КА ТИ ОБКОМ ПАЬЕТИ ОМЯМОЖЕН -----		
ИСПОТ ЗОВАЛЬ ОБЫТЬО КОЧНЬЮТЕМПИСПОР ЗУЕТЛЬАМЯТ ПМЕНЬ ГО ОШЕЕМА БЬ -----		
М ДОЧЕСКАЕПУЯ ЕГТСВОЗМО НОСТОЖИ АДЯМСАЦИРЕРЮФУИГ -----		

Ключ

345612

Протокол криптоанализа

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

(F8) Ключ: 345612	(F7) Генерация	(F6) Вер. Слово: КТУРА
-------------------	----------------	------------------------

КРИПТОГРАММА
ХИТЕАРУРА КТЖДОГКАКОМПО ТЕРАЬЮАКЛА НВАЕТДЫОВСТ СННЬЕВЕТРАН ОЕНИЯИЧ АРХИТЕКТУРА КАЖДОГО КОМПЬЮТЕРА НАКЛАДЫВАЕТ СОБСТВЕННЫЕ ОГРАНИЧЕНИЯ А ВЕ НЧИНУЛИДРЕС А НАИОВЛЬШИБОВОЗМЙ ННЙ ОЖРЕС АДРЕДЕОПЕТ ОЛЯЕМ АБЬ НА ВЕЛИЧИНУ АДРЕСОВ НАИБОЛЬШИЙ ВОЗМОЖНЫЙ АДРЕС ОПРЕДЕЛЯЕТ ОБЪЕМ А ЕСНОДР ПРОГОРАНССТА КОТВЬЮТЕМП ИЛИРАО КА ТЙ ОБКОМ ПАЬЕТИ ОМЯМОЖЕН ДРЕСНОГО ПРОСТРАНСТВА КОМПЬЮТЕРА ИЛИ ТО КАКОЙ ОБЪЕМ ПАМЯТИ ОН МОЖЕ ИСПОТ ЗОВАЛЬ ОБЫТЬО КОЧНЬЮТЕМП ИСПОР ЗУЕТЛЪАМЯТ ПМЕНЬ ГО ОШЕЕМА БЬ Т ИСПОЛЬЗОВАТЬ ОБЫЧНО КОМПЬЮТЕР ИСПОЛЬЗУЕТ ПАМЯТЬ МЕНЬШЕГО ОБЪЕМА М ДОЧЕСКАЕПУЯ ЕГТСВОЗМО НОСТОЖИ АДЯМСАЦИРЕРЮФУИТ ЧЕМ ДОПУСКАЕТСЯ ЕГО ВОЗМОЖНОСТЯМИ АДРЕСАЦИИГРЮФУ

Пути Гамильтона

Исходный текст

(F8) Ключ: <input type="text"/>	(F7) Генерация	(F6) Вер.Слово:
МАРШРУТЫ	КРИПТОГРАММА	
	Е ЯСИСТП НВЛОЕ ЛЫЕДОБ АТ УШНМУЕЛСВ АЖИБЫ ОЬ НЗВМДЕЕС	
	В Ъ ВРЕРЯСНООДАТЕЕРШТ ПКП АТУУ ЪНСЯВ ОЕЛБЕГМПООБУ ДР	
	ЕТЮЕ ЛЯЕЬВВ ОТДУШВЮОЛВ ЪВВЗ ДЮЬОРС ТХУАЕ РИОВНРЦИВМ Ш	
	ЙУ ТЕИ РРИИМПЫИДЗОР КМТ ЪБОН ЗУИЖИНШЕХОПЙ	

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

(F8) Ключ: 3641275	(F7) Генерация	(F6) Вер. Слово: СЕТИ СЯ
МАРШРУТЫ	КРИПТОГРАММА	
1462375	Е ЯСИСТЦ НВЛОЕ ЛЬЕДОВ АТ УШМУЕЛСВ АЖИВН ОБ НЗВМДЕСВ Ъ ВРЕРЯСНОДАТЕЕРШТ ПКП АТУУ ЪНСЯВ ОЕЛБЕТМПООБУ ДР ЕТЮЕ Л	
1463275	СИЕЯТ СВЛЦНЕ ОЕД ЫБЛО У ТНАШЛСМЕ УВИБАК ЖИ Н ЪВОЗЕСМЕ ДВРЕВЬЯ РОДСОТНАШТЕРНЕ АТК УПУНС ЪВ ЯЛБ ЕРОЕОБМО ПУЕТД ЕРЮЕЪ	
1572364	ЯЕБЪВ ОДУШВЮОЛВ ЫЕВЗ ДЮБОРС ТХУАБ ЕИОВНРЦИВ ШИУ ТЕИ РРИИМПИИДЗОФ КМТ ЫОН ЗУИЖИНШЕХОП	
1573264	ЯБЛВДУ ТВОШВ ЮЛБОЯДОВ ОЗЪТХР АСУИОЕРН ВММРИ Ц ТШУИЙЕИ РПРМЗОЯД ИР ЫКТОМБУИНЗИ ЖХОНЕЙШП	
2146375		
2157364		
2364157		
2375146		
2637514		
2641573		
2736415		
2751463		
3264157		
3275146		
3627514		
3641275		
3641572		
3726415		
3751264		
3751462		
4126375		
4157236		
4157263		
4157326		
4157362		
4621573		
4623751		
4632157		
4632751		
4637215		
4637512		
5127364		

3) Увидел СИЯЕТ СОЛНЦЕ, и разгадал криптограмму

(F8) Ключ: 4637215	(F7) Генерация	(F6) Вер. Слово: СИЯЕТ СОЛНЦЕ
МАРШРУТЫ	КРИПТОГРАММА	
1462375	Е ЯСИСТЦ НВЛОЕ ЛЬЕДОВ АТ УШМУЕЛСВ АЖИВН ОБ НЗВМДЕСВ Ъ ВРЕРЯСНОДАТЕЕРШТ ПКП АТУУ ЪНСЯВ ОЕЛБЕТМПООБУ ДР ЕТЮЕ Л	
1463275	СИЯЕТ СОЛНЦЕ ВОДЫ БЛЕШУТ НА ВСЕМ УЛЫБКА ЖИЗНЬ ВО ВСЕМ ДЕРЕВЬЯ РАДОСТНО ТРЕПЕШУТ КУПАЯСЬ В НЕБЕ ГОЛУБОМ ПОЮТ ДЕРЕВЬ	
1572364	ЯЕБЪВ ОДУШВЮОЛВ ЫЕВЗ ДЮБОРС ТХУАБ ЕИОВНРЦИВ ШИУ ТЕИ РРИИМПИИДЗОФ КМТ ЫОН ЗУИЖИНШЕХОП	
1573264	Я БЛЕШУТ ВОДЫ ЛЮБОВЬЮ ВОЗДУХ РАСТВОРЕН И МИР ЦВЕТУШИЙ МИР ПРИРОДЫ ИЗБЫТКОМ ЖИЗНИ УПОЕНИШХ	
2146375		
2157364		
2364157		
2375146		
2637514		
2641573		
2736415		
2751463		
3264157		
3275146		
3627514		
3641275		
3641572		
3726415		
3751264		
3751462		
4126375		
4157236		
4157263		
4157326		
4157362		
4621573		
4623751		
4632157		
4632751		
4637215		
4637512		
5127364		

Табличные перестановки

Исходный текст

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

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

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	--

Переставить строку с позиции на позицию

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