Лабораторная работа №1. Простейшие алгоритмы шифрования
(4 часа)

Лабораторная работа №1.1 Шифрование методами перестановок.
(2 часа)

1.1. ЦЕЛЬ РАБОТЫ – Изучение способов шифрования информации в криптографических системах, основанных на методе перестановки.

1.2. ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

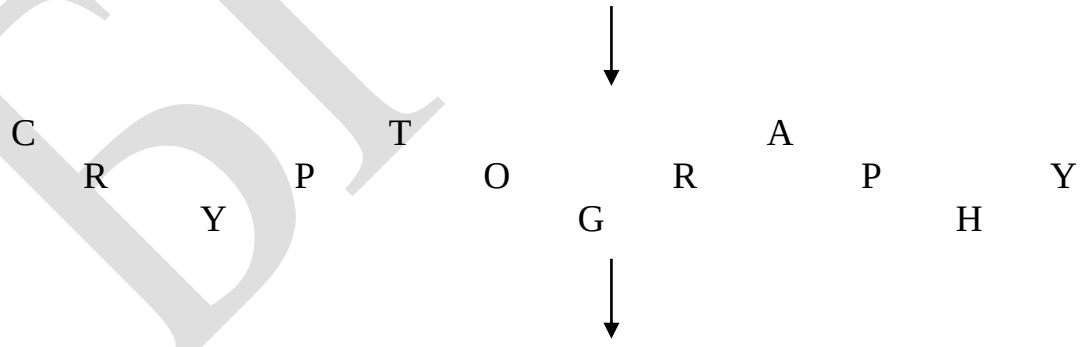
Суть методов перестановки состоит в том, что входной поток исходного текста делится на блоки, в каждом из которых выполняется перестановка символов по определённым правилам, при этом используются только символы исходного (незашифрованного) текста.

В классической криптографии закон, по которому переставляются символы шифруемого текста, задается какой-нибудь геометрической фигурой. Ключ определяет характеристики фигуры. Процедура шифрования состоит из двух шагов – записи и чтения. Сначала исходный текст заполняет фигуру по правилам записи. Затем шифротекст получается из заполненной фигуры по правилам чтения.

«Железнодорожная изгородь»

Простейшим представителем этого метода является метод «железнодорожной изгороди». В этом случае символы исходного текста записываются в виде, напоминающем по форме забор. Символы зашифрованного текста считываются из полученной записи построчно. Следующий пример иллюстрирует этот метод:

M = CRYPTOGRAPHY



C=CTARPORPYYGH

M=CRYPTOGRAPHY – исходный текст (M), C=CTARPORPYYGH соответствующий шифротекст (C). Высота изгороди *K* является ключом, в нашем примере *K*=3. Для того, чтобы расшифровать полученный текст, требуется выполнить действия, обратные выполненным при шифровании, и использовать тот же ключ.

«Ключевая фраза»

Одной из наиболее известных модификаций метода перестановки является использование ключевого слова или фразы в качестве правила перестановки столбца. Слово КРИПТОГРАФИЯ может быть использовано как ключ. Буквам ключевого слова назначаются номера в соответствии с алфавитом, если буква встречается несколько раз, то нумерация определяется порядком следования повторяющихся букв в ключевом слове.

Исходный текст: ЭТО–_ЛЕКЦИЯ_ПО_АЛГОРИТМАМ_ШИФРОВАНИЯ

Ключ: КРИПТОГРАФИЯ

К	Р	И	П	Т	О	Г	Р	А	Ф	И	Я
5	8	3	7	10	6	2	9	1	11	4	12
Э	Т	О	–	_	Л	Е	К	Ц	И	Я	_
П	О	_	А	Л	Г	О	Р	И	Т	М	А
М	_	Ш	И	Ф	Р	О	В	А	Н	И	Я

ШИФРОТЕКСТ: ЦЕОЯЭЛ–ТК_И_ИО_МПГАОРЛТААОШИМРИ_ВФНЯ

Расшифрование выполняется в следующем порядке:

1. Шифротекст разбивается на блоки по 12 символов:

ЦЕОЯЭЛ–ТК_И_ ИО_МПГАОРЛТА АОШИМРИ_ВФНЯ

1 2 3

Номер блока соответствует номеру строки

2. Каждый блок записывается в соответствующую строку в порядке, определяемом ключевым словом. Например, для первого блока:

Ц – 1; Е – 2; О – 3;Я – 4; …

К	Р	И	П	Т	О	Г	Р	А	Ф	И	Я
5	8	3	7	10	6	2	9	1	11	4	12
Э	Т	О	–	_	Л	Е	К	Ц	И	Я	

Метод поворачивающейся решетки

Использовался Германией во время Первой мировой войны. Суть метода – исходный текст зашифровывался через отверстия решетки, которая по мере заполнения поворачивалась на 90^0 градусов. Решетка с отверстиями является ключем при выполнении операций шифрования и дешифрования.

X – вырезанные ячейки

X			
			X
		X	
	X		

Исходный текст: ЭТО ЛЕКЦИЯ ПО КРИПТ

Ключ:

1	2	3	1
3	4	4	**2**
2	4	**4**	3
1	**3**	2	1

Исходный текст разбивается на блоки по 4 символа. Каждый блок кодируется за один проход, заполнением ячеек решетки в указанных позициях ключа. После заполнения ячеек решетки решетка поворачивается вправо на 90 градусов для последующего заполнения.

Исходный текст, разбитый на блоки: ЭТОЛ ЕКЦИ ЯПОК РИПТ

Исходная решетка

Заполнение

После заполнения

Э			
			Т
		Л	
	О		

Поворот

После поворота

			Э
О			
	Л		
		Т	

Решетка после первого заполнения

Э			
			Т
		Л	
	О		

Решетка после поворота и второго заполнения

Е			Э
О			К
	Л	И	
	Ц	Т	

Решетка после поворота и третьего заполнения

Я		О	Е
Ц	Л		П
Т	И	К	
	О	К	Э

Решетка после поворота и четвертого заполнения

Р	Т	Ц	Я
О	И	Л	И
К	К	Т	О
Э	П	П	Е

Решетка после поворота и перед формированием шифротекста

Э	К	О	Р
П	К	И	Т
П	Т	Л	Ц
Е	О	И	Я

Шифрованный текст получаем вычитывая построчно строки заполненной решетки:

ЭКОР ПКИТ ПТЛЦ ЕОИЯ -> ЭКОРПКИТПТЛЦЕОИЯ

Расшифрование осуществляется похожим способом, вычитывая символы исходного текста из ячеек ключа заполненной решетки.

Решетка с заполненным шифротекстом	Выбор символов исходного текста согласно ключу	Поворот заполненной решетки	Выбор символов исходного текста согласно ключу

Э	К	О	Р
П	К	И	Т
П	Т	Л	Ц
Е	О	И	Я

Э	К	О	Р
П	К	И	**Т**
П	Т	**Л**	Ц
Е	**О**	И	Я

Е	П	П	Э
О	Т	К	К
И	Л	И	О
Я	Ц	Т	Р

Е	П	П	Э
О	Т	К	**К**
И	Л	**И**	О
Я	**Ц**	Т	Р

и т.д.

ЭТОЛ **ЕКЦИ**

Расшифрованный текст:

ЭТОЛ ЕКЦИ ЯПОК РИПТ

Сделать решетку достаточно легко, строится матрица 4х4:

1	2	3	1
3	4	4	2
2	4	4	3
1	3	2	1

Ячейки нумеруются следующим образом: ячейки, которые при повороте на 90^0 занимают одинаковое положение, нумеруются одинаково. Затем вырезается по одному квадрату с одинаковым номером.

Примеры готовых решеток:

1	2	3	1
3	4	4	2
2	4	4	3
1	3	2	1

Решетка 4х4

1	2	3	4	1
4	5	6	5	2
3	6	7	6	3
2	5	6	5	4
1	4	3	2	1

Решетка 5х5

1	2	3	4	5	1
5	6	7	8	6	2
4	8	9	9	7	3
3	7	9	9	8	4
2	6	8	7	6	5
1	5	4	3	2	1

Решетка 6х6

1.3. ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

Исходный текст (не менее 20 символов) должен содержать фамилию или имя.

Реализовать шифратор и дешифратор на основе трех рассмотренных методов.

Лабораторная работа №1.2 Шифрование методами подстановок.
(2 часа)

2.1. ЦЕЛЬ РАБОТЫ – Изучение способов шифрования информации в криптографических системах, основанных на методе подстановки.

2.2. ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

Криптографические системы, основанные на методе подстановки, разделяются на четыре основных класса:

1) monoalphabetic;
2) homophonic;
3) polyalphabetic;
4) polygram.

В системах класса monoalphabetic символ исходного текста заменяется другим символом таким образом, что между ними существует однозначное соответствие. То есть каждый символ исходного текста однозначно заменяется его подстановкой. Криптографическим ключем такой системы является таблица соответствия исходного алфавита алфавиту подстановки. Например, для английского алфавита существует 26! = 4*1026 различных криптографических систем первого класса. Наиболее простые системы данного класса предполагают аналитическое описание подстановок. Так, простейший шифратор, основанный на принципе подстановки, сдвигает каждую букву английского алфавита на k позиций, где k является ключом шифра. В так называемом алгоритме Цезаря i-я буква алфавита заменяется $(i+k)$-й буквой по модулю 26. Юлий Цезарь использовал подобную систему для k=3. Аналитически криптосистема Цезаря описывается выражением

$$E_k(i) = (i+k) \bmod 26. \qquad (1)$$

Например, в соответствии с приведенным выражением буква A исходного английского алфавита, имеющая номер i=0, заменяется буквой D, имеющей номер $(i+k)$ mod 26 = (0+3) mod 26 = 3, а буква z (i=25) заменяется буквой C, имеющей номер $(i+k)$ mod 26 = (25+3) mod 26 = 2. Следующий пример иллюстрирует алгоритм шифрования Цезаря:

Исходный текст :CRYPTOGRAPHYANDDATASECURITY.
Шифротекст :FUBSWRJUDSKBDQSGDWDVHFXULWB.

Алгоритм дешифрования имеет вид

$$D_k(i) = (i+26-k) \bmod 26. \qquad (2)$$

Существуют более сложные методы подстановки. Шифраторы, основанные на умножении номера каждого символа исходного текста на значение ключа k, описываются следующим общим отношением:

$E_k(i) = (i*k) \bmod n,$ (3)

где i - номер символа исходного текста, n - количество символов в исходном алфавите (n=26 для английского алфавита и n=256 для ASCII-кодов), k – ключ.

При этом:

- n и k должны быть взаимно простыми;
- для проведения операций шифрования и дешифрования используются два различных ключа k_e и k_d, которые связаны между собой следующим образом: $(k_e * k_d) \bmod n = 1$

Пример:

- $n = 26$ (*символы английского алфавита*);
- $k_e = 7$, $k_d = 15$.

$$(k_e * k_d) \bmod n = (7 * 15) \bmod 26 = 105 \bmod 26 = 1$$

Алгоритм шифрования имеет вид

$$E_k(i) = (i * k_e) \bmod n. \quad (3.1)$$

Алгоритм дешифрования имеет вид

$$D_k(i) = (i * k_d) \bmod n. \quad (3.2)$$

2.3. ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

Исходный текст (не менее 20 символов) должен содержать фамилию или имя.

1) Реализовать шифратор и дешифратор на основе формулы (1).
2) Реализовать шифратор и дешифратор на основе формулы (3.1, 3.2).