ЛАБОРАТОРНАЯ РАБОТА № 1

ИСПОЛЬЗОВАНИЕ КЛАССИЧЕСКИХ КРИПТОАЛГОРИТМОВ ПОДСТАНОВКИ И ПЕРЕСТАНОВКИ ДЛЯ ЗАЩИТЫ ТЕКСТОВОЙ ИНФОРМАЦИИ

Цель работы: изучение классических криптографических алгоритмов моноалфавитной подстановки, многоалфавитной подстановки и перестановки для защиты текстовой информации. Использование гистограмм, отображающих частоту встречаемости символов в тексте для криптоанализа классических шифров.

Описание лабораторной работы. Для выполнения лабораторной работы необходимо запустить программу **L_LUX.EXE**[*]. На экране дисплея появляется окно с размещенным в его центре текстовым редактором (для отображения зашифрованных и расшифрованных текстов), в верхней строке окна расположено главное меню, позволяющее пользователю выполнить требуемое действие. Чуть ниже основного меню размещена панель инструментов (для управления быстрыми командными кнопками и другими «горячими» элементами управления), а в самом низу окна, под текстовым редактором, находится строка состояния, в которой указывается подсказка и выводится дополнительная информация. Клавиши панели инструментов для удобства снабжены всплывающими подсказками.

Для того чтобы попасть в основное меню, необходимо нажать клавишу F10. Передвижение по главному меню осуществляется клавишами перемещения курсора. Чтобы вызвать пункт меню, нужно нажать клавишу ENTER, вернуться в главное меню или вовсе выйти из него — ESC.

Рассмотрим более подробно каждый из пунктов главного меню.

Редактор. Данный пункт основного меню содержит подпункты: создать документ, открыть файл, сохранить файл, выход из программы.

Предварительно, сразу после запуска программы, текстовый редактор недоступен, также недоступными являются почти все пункты главного меню, кроме создания документа, открытия файла, выхода из программы, информации о программе, и бóльшая часть клавиш панели управления, за исключением создания документа, открытия файла и выхода из программы.

Создать документ (Ctrl+N) — при выборе данного подпункта становится доступна работа с тестовым редактором (пользователь получает право создать свой текстовый файл, который впоследствии можно будет использовать при работе с программой), также появляется возмож-

[*]Размер программы 768512 байт. Программа не требует инсталляции.

ность использовать все недоступные до этого пункты основного меню и клавиши панели управления.

Открыть файл (Ctrl+L) — при выборе этого пункта появляется диалоговое окно, предоставляющее возможность выбора файла для загрузки. При этом содержимое файла будет отображено в окне редактора текстов.

Аналогично пункту СОЗДАТЬ ДОКУМЕНТ доступным для работы становится текстовый редактор с отображаемым текстом, а также появляется возможность использовать все недоступные до этого пункты основного меню и клавиши панели управления.

Сохранить файл (Ctrl+S) — при выборе этого пункта появляется диалоговое окно, позволяющее сохранить на диске содержимое редактора текстов.

Выход из программы (Ctrl+X) — при выборе этого пункта появляется диалоговое окно, позволяющее выйти из программы.

Гистограмма. Вывод на экран двух гистограмм, отображающих частоту встречаемости символов в тексте.

Внимание! До выполнения шифрования и дешифрования вызывать гистограмму не имеет смысла, так как еще не сформированы тексты, для которых будет просматриваться гистограмма.

Имеется возможность просмотра следующих сочетаний гистограмм:

- исходного и зашифрованного файла;
- зашифрованного и расшифрованного файла;
- стандартного распределения и зашифрованного текста;
- стандартного распределения и расшифрованного текста.

С целью масштабирования в гистограммах используются левая и правая клавиши мыши. Например, после шифрования текста большого объема пользователь хочет посмотреть гистограммы исходного и зашифрованного файла. Поскольку размеры текста достаточно большие, то на экран будут выведены две гистограммы с большим количеством столбцов в каждой (столбец соответствует одному символу текста), однако трудно будет сказать, какой из этих столбцов соответствует тому или иному символу текста и какова частота встречаемости данного символа. Поэтому у пользователя есть возможность увеличить масштаб любой из двух гистограмм для более точного определения требуемого значения частоты встречаемости конкретного символа. Для этого необходимо навести указатель мыши на левую границу того участка гистограммы, который требуется увеличить, затем нажать левую клавишу мыши и, не отпуская ее, растянуть прямоугольник так,

чтобы его нижний правый угол совпал с правой границей увеличиваемого участка гистограммы. После этого следует отпустить левую клавишу мыши, и на экране появится увеличенное изображение нужного участка. Нажав и не отпуская правую клавишу мыши, можно перемещать гистограмму в любом направлении с целью изучения всего полученного распределения в увеличенном масштабе.

Для того чтобы от увеличенного масштаба вернуться к исходному виду, нужно навести указатель мыши на гистограмму, затем нажать левую клавишу мыши и, не отпуская ее, снизу вверх растянуть небольшой по размерам прямоугольник, после этого следует отпустить левую клавишу мыши, и на экране появится исходное изображение гистограммы.

Шифрование. Выполнение шифрования текстового файла осуществляется одним из семи методов, рассматриваемых в лабораторной работе:

1) одноалфавитный (с фиксированным смещением);
2) одноалфавитный с задаваемым смещением (от 2 до 20);
3) перестановка символов;
4) по дополнению до 255 (инверсный);
5) многоалфавитный (с фиксированным ключом);
6) многоалфавитный с ключом фиксированной длины;
7) многоалфавитный с ключом произвольной длины.

Выбор метода шифрования производится как мышкой, так и клавишами перемещения курсора и клавишей ENTER. Затем появляется окно, в котором в зависимости от метода шифрования требуется указать те или иные параметры и либо подтвердить процесс кодировки, либо отказаться от него. После этого в окне редактора будет выдан зашифрованный текст.

Расшифрование. Аналогично предыдущему пункту выбирается метод расшифрования (должен соответствовать методу, которым был зашифрован файл). Снова появляется окно, в котором в зависимости от метода расшифрования требуется указать те или иные параметры и либо подтвердить процесс расшифрования, либо отказаться от него. После этого в окно редактора будет выдан расшифрованный текст. При правильном расшифровании полученный текст совпадает с исходным.

Дополнительная информация. Программа предусматривает возможность посмотреть дополнительную информацию («Помощь Ctrl+F9»), справочную информацию об используемых методах шифрования («О методах Ctrl+F10»), сведения о программе («О программе Ctrl+F11»).

Пример работы с программой. Рассмотрим одноалфавитное шифрование с фиксированным ключом.

Нажав клавиши Ctrl+L либо выбрав в меню пункт ОТКРЫТЬ ФАЙЛ, загрузите в окно редактора исходный текст.

Затем вызовите пункт меню ШИФРОВАНИЕ, выберите одноалфавитный метод (с фиксированным смещением). В появившемся окне нажмите клавишу ЗАШИФРОВАТЬ. После того как шифрование выполнено, можно в редакторе просмотреть зашифрованный текст.

Перейдите к пункту меню ГИСТОГРАММА. Выберите тип гистограмм, отображающий гистограммы исходного и шифрованного файлов. Проанализируйте гистограммы. Они должны иметь примерно одинаковый вид.

Чтобы узнать ключ шифра (смещение второго алфавита относительно первого), необходимо по гистограммам найти символы, имеющие одинаковую частоту встречаемости. Например, самый частый символ в первой гистограмме при шифровании должен перейти в самый частый символ во второй гистограмме. Таким образом, найдя два самых часто встречаемых символа в обеих гистограммах, можно по стандартной таблице ASCII-кодов вычислить смещение. Зная смещение и таблицу кодировки символов, текст можно легко расшифровать. Вызвав пункт меню ДЕШИФРОВАНИЕ, можно провести те же действия в автоматическом режиме.

Примечание. При шифровании и расшифровании из таблицы кодировки не используются символы с кодами 176—223 и 240—255, т.е. при ручной расшифровке эти символы следует пропускать и считать, что, например, символ «Я» имеет код не 159, а 223, аналогично «п» не 175, а 239.

Иногда в гистограммах под столбцами, показывающими частоту встречаемости символов, изображены не сами символы, а их табличные коды в квадратных скобках.

Ниже провидено описание «горячих» клавиш и их использование при выполнении различных действий:

Shift+F10 — о программе;
Ctrl+X — выход из программы;
Ctrl+N — new — ФАЙЛ/СОЗДАТЬ;
Ctrl+L — load — ФАЙЛ/ОТКРЫТЬ;
Ctrl+S — save — ФАЙЛ/СОХРАНИТЬ.

Шифрование:

Ctrl+F1 — одноалфавитный метод (с фиксированным смещением);
Ctrl+F2 — одноалфавитный с задаваемым смещением (от 2 до 20);
Ctrl+F3 — перестановка символов;

Ctrl+F4 — по дополнению до 255 (инверсный метод);
Ctrl+F5 — многоалфавитный метод с фиксированным ключом;
Ctrl+F6 — многоалфавитный метод с ключом фиксированной длины;
Ctrl+F7 — многоалфавитный метод с ключом произвольной длины.

Расшифрование:

Shift+F1 — одноалфавитный метод (с фиксированным смещением);
Shift+F2 — одноалфавитный с задаваемым смещением (от 2 до 20);
Shift+F3 — перестановка символов;
Shift+F4 — по дополнению до 255 (инверсный метод);
Shift+F5 — многоалфавитный метод с фиксированным ключом;
Shift+F6 — многоалфавитный метод с ключом фиксированной длины;
Shift+F7 — многоалфавитный метод с ключом произвольной длины.

Гистограммы:

Shift+Ctrl+F1 — исходного и шифрованного файла;
Shift+Ctrl+F2 — шифрованного и расшифрованного файла;
Shift+Ctrl+F3 — стандартного распределения и шифрованного текста;
Shift+Ctrl+F4 — стандартного распределения и расшифрованного текста.

Помощь:

Ctrl+F9 — помощь;
Ctrl+F10 — о методах;
Ctrl+F11 — о программе.

Задание

Ознакомиться с описанием лабораторной работы и заданием.

1. Для одноалфавитного метода с фиксированным смещением определить установленное в программе смещение. Для этого следует:

- просмотреть предварительно созданный с помощью редактора свой текстовый файл; **(свой вариант)**
- выполнить для этого файла шифрование;
- просмотреть в редакторе зашифрованный файл;
- просмотреть гистограммы исходного и зашифрованного текстов;

- описать гистограммы (в чем похожи, чем отличаются) и определить, с каким смещением было выполнено шифрование;
- расшифровать зашифрованный текст:
  - с помощью программы, после чего проверить в редакторе правильность расшифрования,
  - вручную с помощью гистограмм; описать и объяснить процесс дешифрования.

В отчете для каждого метода шифрования описывается последовательность выполняемых действий, имена всех использованных файлов, полученные гистограммы, указывается найденное смещение, описывается процесс дешифрования.

Преподавателю предоставляется отчет о проделанной работе и все использованные и созданные файлы.

2. Для одноалфавитного метода с задаваемым смещением (шифр Цезаря) следует:

- выполнить шифрование с произвольным смещением для своего исходного текста;
- просмотреть и описать гистограммы исходного и зашифрованного текстов, определить смещение для нескольких символов;
- расшифровать текст с помощью программы;
- дешифровать зашифрованный шифром Цезаря текст с помощью программы методом подбора смещения; указать, с каким смещением был зашифрован файл.

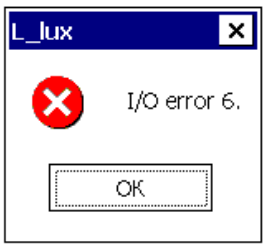
3. Для метода перестановки символов дешифровать зашифрованный файл. Для этого необходимо определить закон перестановки символов открытого текста. Создайте небольшой файл длиной в несколько слов с известным вам текстом, зашифруйте его, просмотрите гистограммы (опишите их; ответьте, можно ли извлечь из них полезную для дешифрации информацию). Сравните (с помощью редактора) ваш исходный и зашифрованный тексты и определите закон перестановки символов.

Дешифруйте файл:

- вручную (объясните ваши действия);
- с помощью программы.

4. Для инверсного кодирования (по дополнению до 255):

- выполните шифрование для своего произвольного файла;
- просмотрите гистограммы исходного и зашифрованного текстов, опишите гистограммы и определите смещение для нескольких символов;
- дешифруйте зашифрованный текст, проверьте в редакторе правильность дешифрования.



Для всех многоалфавитных методов обязательным условием является загрузка текстового файла (*.txt) с диска. В противном случае будет выдано сообщение "I/O error 6".

Если текстовый файл создается в самой программе L_Lux.exe, то необходимо набранный текст сначала сохранить на диск с указанием расширения (*.txt), затем открыть этот текстовый файл с диска.

Текстовый файл в кодировке ANSI (ср-1251, WIN) можно также создать в программе Блокнот.

5. Для многоалфавитного шифрования с фиксированным ключом определите, сколько одноалфавитных методов и с каким смещением используется в программе. Для этого нужно создать свой файл, состоящий из строки одинаковых символов, выполнить для него шифрование и по гистограмме определить способ шифрования и набор смещений.

6. Для многоалфавитного шифрования с ключом фиксированной длины:

- выполните шифрование и определите по гистограмме, какое смещение получает каждый символ для файла, состоящего из строки одинаковых символов;
- выполните шифрование и расшифрование для файла произвольного текста;
- просмотрите и опишите гистограммы исходного и зашифрованного текстов; ответьте, какую информацию можно получить из гистограмм.

7. Для многоалфавитного шифрования с произвольным паролем задание полностью аналогично п. 6.

Привести в отчете ответы на контрольные вопросы в соответствии с номером варианта, указанным преподавателем (табл. 1.1).

Таблица 1.1

Номер варианта	Контрольные вопросы
1, 5, 9, 13	Какие вы знаете методы криптографической защиты файлов?
2, 6, 10, 14	В чем преимущества и недостатки одноалфавитных методов?
3, 7, 11, 15	Если необходимо зашифровать текст, содержащий важную информацию, какой метод из рассмотренных вы выберете? Обоснуйте свой выбор
4, 8, 12, 16	Целесообразно ли повторно применять для уже зашифрованного текста: а) метод многоалфавитного шифрования; б) метод Цезаря?

Приложение. Таблица основных кодов ASCII (cp1251)

младшая тетрада

старшая тетрада

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0			*у*	*п*	*р*	*а*	*в*	*л*	*я*	*ю*	*щ*	*и*	*е*			
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1					*с*	*и*	*м*	*в*	*о*	*л*	*ы*					
	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
2		!	"	#	$	%	&	'	(	)	*	+	,	-	.	/
	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
3	0	1	2	3	4	5	6	7	8	9	:	;	<	=	>	?
	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
4	@	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79
5	P	Q	R	S	T	U	V	W	X	Y	Z	[	\	]	^	_
	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95
6	`	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
	96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111
7	p	q	r	s	t	u	v	w	x	y	z	{	|	}	~	
	112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127
8																
	128	129	130	131	132	133	134	135	136	137	138	139	140	141	142	143
9				*с*	*п*	*е*	*ц*	*и*	*а*	*л*	*ь*	*н*	*ы*	*е*		
	144	145	146	147	148	149	150	151	152	153	154	155	156	157	158	159
A					*с*	*и*	*м*	*в*	*о*	*л*	*ы*					
	160	161	162	163	164	165	166	167	168	169	170	171	172	173	174	175
B																
	176	177	178	179	180	181	182	183	184	185	186	187	188	189	190	191
C	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П
	192	193	194	195	196	197	198	199	200	201	202	203	204	205	206	207
D	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
	208	209	210	211	212	213	214	215	216	217	218	219	220	221	222	223
E	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п
	224	225	226	227	228	229	230	231	232	233	234	235	236	237	238	239
F	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я
	240	241	242	243	244	245	246	247	248	249	250	251	252	253	254	255