ЛАБОРАТОРНАЯ РАБОТА 2
Шифрование с использованием систем Цезаря и системы Трисемуса

Цель работы: формирование умений шифрования с использованием систем Цезаря и системы Трисемуса.

Теоретические сведения

При шифровании *заменой* (подстановкой) символы шифруемого текста заменяются символами того же или другого алфавита с заранее установленным правилом замены. В шифрах простой замены (одноалфавитной подстановки) каждый символ исходного текста заменяется символами того же алфавита одинаково на всем протяжении текста.

Система шифрования Цезаря

Шифр Цезаря является частным случаем шифра простой замены (одноалфавитной подстановки).

Ключом шифрования является целое число 1 … N, где N – количество букв алфавита шифруемого слова, уменьшенное на 1. Ключ будет обозначаться символом K. При шифровании исходного текста каждая буква заменяется на другую букву того же алфавита. Заменяющая буква определяется путем смещения от исходной буквы алфавита на K букв. При достижении конца алфавита выполняется циклический переход к его началу.

Рассмотрим пример шифрования сообщения «ПРИЛЕТАЮ ЗАВТРА» с использованием системы Цезаря. Ключ шифрования K примем равным 3.

Сначала сформируем таблицу подстановок, содержащую соответствующие пары букв исходного текста и шифртекста (табл. 2.1).

Таблица 2.1

↓	а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о
	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с

↓	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я
	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в

При шифровании каждая буква исходного текста (из верхней строки таблицы) заменяется на соответствующую букву из нижней строки.

Таким образом, в результате шифрования сообщения «ПРИЛЕТАЮ ЗАВТРА» будет получен шифртекст «ТУЛОЗХГБКГЕХУГ».

Аффинная система подстановок Цезаря

При шифровании с использованием аффинной системы подстановок Цезаря буква с порядковым номером t в соответствующем алфавите заменяется на букву, порядковый номер которой в этом же алфавите рассчитывается по формуле $(at + b) \bmod m$, где a, b – числовые ключи, а m – количество букв в алфавите.

При выборе ключа a необходимо учитывать следующее требование: a и m должны быть взаимно простыми числами, то есть наибольший общий делитель a и m должен быть равен 1.

Рассмотрим пример шифрования сообщения «ПРИЛЕТАЮ ЗАВТРА» с использованием аффинной системы подстановок Цезаря. Ключи шифрования примем следующими: $a = 4$, $b = 2$. Так как количество букв в алфавите $m = 33$, то требование к выбору ключа a соблюдается.

В первую очередь построим таблицу соответствия порядковых номеров букв исходного текста и шифртекста в соответствии с формулой (табл. 2.2). Нумерация букв начинается с 0.

Таблица 2.2

t	*4t + 2*	*t*	*4t + 2*	*t*	*4t + 2*	*t*	*4t + 2*
0	2	9	5	18	8	27	11
1	6	10	9	19	12	28	15
2	10	11	13	20	16	29	19
3	14	12	17	21	20	30	23
4	18	13	21	22	24	31	27
5	22	14	25	23	28	32	31
6	26	15	29	24	32		
7	30	16	0	25	3		
8	1	17	4	26	7		

Затем на основании табл. 2.2 построим таблицу соответствия конкретной букве исходного текста буквы шифртекста для заданных ключей шифрования (табл. 2.3).

Таблица 2.3

→		→		→		→	
а	в	и	е	с	з	ъ	к
б	ё	й	и	т	л	ы	о
в	й	к	м	у	п	ь	т
г	н	л	р	ф	у	э	ц
д	с	м	ф	х	ч	ю	ъ
е	х	н	ш	ц	ы	я	ю
ё	щ	о	ь	ч	я		
ж	э	п	а	ш	г		
з	б	р	д	щ	ж		

Соответствующим образом заменив буквы исходного текста «ПРИЛЕТАЮ ЗАВТРА», получим шифртекст «АДЕРХЛВЪБВЙЛДВ».

Система шифрования Цезаря с ключевым словом

Особенность системы шифрования Цезаря с ключевым словом – использование ключевого слова для смещения и изменения порядка символов в алфавите подстановки. Для этой системы ключ должен быть составным и содержать некоторое число (например, k) и ключевое слово. Для числа k должно соблюдаться требование

$0 \le k < m - 1$,

где m – количество букв в алфавите.

Рассмотрим пример шифрования сообщения «ПРИЛЕТАЮ ЗАВТРА» с использованием системы шифрования Цезаря с ключевым словом. Примем $k = 5$, в качестве ключевого слова будем использовать слово «РАБОТА».

Первым этапом шифрования является запись ключевого слова в таблицу подстановок, начиная с буквы исходного алфавита с номером k. Если ключевое слово имеет повторяющиеся буквы, в таблицу подстановок повторно они не записываются (табл. 2.4).

Таблица 2.4

№	→		№	→		№	→		№	→	
0	а		9	и	т	18	с		27	ъ	
1	б		10	й		19	т		28	ы	
2	в		11	к		20	у		29	ь	
3	г		12	л		21	ф		30	э	
4	д		13	м		22	х		31	ю	
5	е	р	14	н		23	ц		32	я	
6	ё	а	15	о		24	ч				
7	ж	б	16	п		25	ш				
8	з	о	17	р		26	щ				

Оставшиеся буквы алфавита подстановки записываются после ключевого слова в алфавитном порядке (табл. 2.5).

Таблица 2.5

№	→		№	→		№	→		№	→	
0	а	ы	9	и	т	18	с	й	27	ъ	х
1	б	ь	10	й	в	19	т	к	28	ы	ц
2	в	э	11	к	г	20	у	л	29	ь	ч
3	г	ю	12	л	д	21	ф	м	30	э	ш
4	д	я	13	м	е	22	х	н	31	ю	щ
5	е	р	14	н	ё	23	ц	п	32	я	ъ
6	ё	а	15	о	ж	24	ч	с			
7	ж	б	16	п	з	25	ш	у			
8	з	о	17	р	и	26	щ	ф			

Таким образом, в результате шифрования исходного сообщения «ПРИЛЕТАЮ ЗАВТРА» с использованием данной системы шифрования получим шифртекст: «ЗИТДРКЫЩ ОЫЭКИЫ».

Система шифрования Трисемуса

Составной ключ шифрования в данной системе включает ключевое слово и размер таблицы подстановок.

Рассмотрим пример шифрования сообщения «ПРИЛЕТАЮ ЗАВТРА» с использованием системы шифрования Трисемуса. В качестве ключевого слова будем использовать слово «РАБОТА», размер таблицы подстановки – 4 × 8.

Примечание – Так как при размере таблицы 4 × 8 в нее может быть записано только 32 буквы, из исходного алфавита будет исключена буква «ё».

В таблицу сначала по строкам вписывается ключевое слово, причем повторно встречающиеся в нем буквы не записываются. Затем эта таблица дополняется не вошедшими в нее буквами алфавита по порядку (табл. 2.6).

Таблица 2.6

р	а	б	о	т	в	г	д
е	ж	з	и	й	к	л	м
н	п	с	у	ф	х	ц	ч
ш	щ	ъ	ы	ь	э	ю	я

При шифровании в этой таблице находим очередную букву открытого текста и записываем в шифртекст букву, расположенную ниже ее в том же столбце. Если буква текста оказывается в нижней строке таблицы, тогда для шифртекста берут самую верхнюю букву из того же столбца.

Таким образом, при шифровании с помощью этой таблицы исходного сообщения «ПРИЛЕТАЮ ЗАВТРА» будет получен шифртекст «ЩЕУЦНЙЖГ СЖКЙЕЖ».

Содержание заданий

Задание 1

Зашифруйте сообщение «МЫ ДОЛЖНЫ ПРИЗНАТЬ ОЧЕВИДНОЕ: ПОНИМАЮТ ЛИШЬ ТЕ, КТО ХОЧЕТ ПОНЯТЬ», используя систему Цезаря со значением ключа соответствующим номеру варианта (например, для варианта 10 – ключ $K = 10$).

Задание 2

Зашифруйте сообщение «СМЫСЛ ЖИЗНИ НАШЕЙ – НЕПРЕРЫВНОЕ ДВИЖЕНИЕ», используя аффинную систему подстановок Цезаря с ключами, согласно своему варианту (табл. 2.7).

Таблица 2.7

Вариант	Ключ	Вариант	Ключ	Вариант	Ключ
1	$a = 5, b = 1$	10	$a = 7, b = 2$	19	$a = 5, b = 4$
2	$a = 2, b = 5$	11	$a = 8, b = 2$	20	$a = 7, b = 4$
3	$a = 4, b = 7$	12	$a = 2, b = 3$	21	$a = 8, b = 3$
4	$a = 2, b = 10$	13	$a = 4, b = 2$	22	$a = 4, b = 6$
5	$a = 7, b = 1$	14	$a = 5, b = 3$	23	$a = 5, b = 6$
6	$a = 8, b = 1$	15	$a = 7, b = 3$	24	$a = 7, b = 5$
7	$a = 2, b = 4$	16	$a = 8, b = 4$	25	$a = 8, b = 6$
8	$a = 4, b = 10$	17	$a = 2, b = 2$		
9	$a = 5, b = 2$	18	$a = 4, b = 5$		

Задание 3

Выполните шифрование сообщения «РАЗУМА ЛИШАЕТ НЕ СОМНЕНИЕ, А УВЕРЕННОСТЬ», используя систему шифрования Цезаря с ключами, соответствующими варианту.

1. $k = 1$, ключевое слово «РАДОСТЬ».
2. $k = 2$, ключевое слово «УСПЕХ».
3. $k = 3$, ключевое слово «УДАЧА».
4. $k = 4$, ключевое слово «ЛЕТО».

5. $k = 5$, ключевое слово «ВЕСНА».
6. $k = 6$, ключевое слово «ЗИМА».
7. $k = 7$, ключевое слово «ОСЕНЬ».
8. $k = 8$, ключевое слово «АЛГОРИТМ».
9. $k = 9$, ключевое слово «ПРОГРАММИРОВАНИЕ».
10. $k = 10$, ключевое слово «КРИПТОГРАФИЯ».
11. $k = 11$, ключевое слово «КРИПТОАНАЛИЗ».
12. $k = 12$, ключевое слово «ШИФРТЕКСТ».
13. $k = 13$, ключевое слово «ОРЕХИ».
14. $k = 14$, ключевое слово «ТЕЛЕФОН».
15. $k = 15$, ключевое слово «КОМПЬЮТЕР».
16. $k = 16$, ключевое слово «ЧАСЫ».
17. $k = 17$, ключевое слово «МУЗЫКА».
18. $k = 18$, ключевое слово «РУЧКА».
19. $k = 19$, ключевое слово «ИНФОРМАЦИЯ».
20. $k = 20$, ключевое слово «РАБОТА».
21. $k = 21$, ключевое слово «СОЛНЦЕ».
22. $k = 22$, ключевое слово «ПЕРЕМЕНЫ».
23. $k = 23$, ключевое слово «ЖИЗНЬ».
24. $k = 24$, ключевое слово «ЛАБОРАТОРНАЯ».
25. $k = 25$, ключевое слово «СПРАВОЧНИК».

Задание 4

Выполните шифрование сообщения «УСПЕХ – ЭТО КОГДА ТЫ ДЕВЯТЬ РАЗ УПАЛ, НО ДЕСЯТЬ РАЗ ПОДНЯЛСЯ», используя систему Трисемуса с ключевым словом из задания 3. Размер таблицы подстановок 4 × 8.

Контрольные вопросы

1. В чем особенность шифров простой замены?
2. Чем отличаются система шифрования Цезаря и аффинная система подстановок Цезаря?
3. Какие требования предъявляются к выбору ключей для аффинной системы подстановок Цезаря?
4. Для каких шифров простой замены используется составной ключ?
5. Каким образом заполняется таблица подстановок для шифрования с использованием системы Трисемуса?

Отчетность по лабораторной работе

Выполните задания согласно своему варианту. Оформите отчет в виде документа Word с описанием хода решения и отправьте на проверку .