Лабораторна робота № 1

ШИФРУВАННЯ ДАНИХ МЕТОДАМИ ПІДСТАНОВКИ (ЗАМІНИ), ПЕРЕСТАНОВКИ І ПОЛІАБЕТНИМИ ШИФРАМИ

Мета роботи: придбання навичок шифрування інформації з використанням простих методів шифрування.

Основні теоретичні відомості

Проблемою захисту інформації шляхом її перетворення займається криптологія (kryptos – таємний, logos – наука). Криптологія розділяється на два напрями: криптографію і криптоаналіз.

Цілі цих напрямів прямо протилежні:

- криптографія займається пошуком і дослідженням математичних методів перетворення інформації.
- сфера інтересів криптоаналізу – дослідження можливості розшифрування інформації без знання ключів.

Термінологія. Криптографія дає можливість перетворити інформацію таким чином, що її прочитання (відновлення) можливе тільки при знанні ключа. В якості інформації, що підлягає шифруванню і дешифруванню, розглядаються тексти, побудовані на деякій абетці. Під цими термінами розуміється наступне:

Абетка – кінцева множина знаків, що використовується для кодування інформації.

Текст – впорядкований набір з елементів абетки. В якості прикладів абеток, що використовуються в сучасних інформаційних системах, можна навести наступні:

- абетка Z_{33} – 32 літери української абетки і пропуск;
- абетка Z_{256} – символи, що входять в стандартні коди ASCII і KOI-8;
- бінарна абетка – $Z_2=\{0,1\}$;
- вісімкова абетка або шістнадцяткова абетка.

Шифрування – процес перетворення: початковий текст, який носить також назву відкритого тексту, замінюється шифрованим текстом.

Дешифрування – зворотний шифруванню процес. На основі ключа шифрований текст перетвориться в початковий.

Ключ – інформація, необхідна для безперешкодного шифрування і дешифрування текстів.

Огляд використовуваних методів.

Метод підстановки (заміни)

Моноабеткова звичайна заміна Цезаря (шифр Цезаря). Як повідомляє історик Гай Светоній, римський імператор Гай Юлій Цезар користувався у своєму військовому та особистому листуванні шифром, сутність якого полягала у заміні кожної літери повідомлення на одну із інших літер 26-значного латинської абетки.

Щоб зрозуміти зашифроване повідомлення Цезаря, треба було кожну літеру в ній замінити третьою, що йде після неї в абетці. При досягненні кінця абетки виконувався циклічний перехід до його початку.

Такий метод шифрування можна відобразити шифрувальною таблицею, в якій вказано знаки заміни для кожного знаку криптограми. Використання таблиці очевидне: при шифруванні для кожного знаку відкритого тексту шукаємо відповідний знак криптограми, при дешифруванні – навпаки.

Отже, шифр Цезаря пов’язаний із використанням первинної абетки (для відкритого тексту) і вторинної абетки (для криптограми), циклічно зміщеної відносно

первинної на три знаки вперед.

Номер (код)	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
Знак Відкритого тексту	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Знак криптограми	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W

Зокрема, Цезар використовував свій шифр у листуванні з Цицероном (близько 50 р. до н.е.). А його відоме послання VENI VIDI VICI – «Прийшов, побачив, переміг» своєму другові Амінтію (після перемоги над понтійським царем Фарнаком, сином Мітрідата при Золе в 47 р. до н.е.) у зашифрованому вигляді мало такий вигляд: SBKF SFAF SFZF.

Загальний випадок шифру Цезаря для первинної абетки деякої величини m полягає в тому, що вторинна абетка циклічно зміщується відносно первинної на K знаків вперед ($0 \le K < m$). Значення K є ключем цього шифру.

Наприклад, для абетки «АБВГДЕЖЗИК» об'ємом m=10 шифрувальна таблиця для K=6 має наступний вигляд:

Номер(код)	0	1	2	3	4	5	6	7	8	9
Знак відкритого тексту	А	Б	В	Г	Д	Е	Ж	З	И	К
Знак криптограми	Д	Е	Ж	З	И	К	А	Б	В	Г

Таким чином, відкритому тексту «КВИДА» відповідає криптограма «ГЖВИД» і навпаки.

Недоліки моноабеткової звичайної заміни Цезаря:

- вона не маскує частот появи різних знаків відкритого тексту і тому її легко зламати на підставі аналізу частот появи знаків у криптограмі;
- у вторинній абетці зберігається той же самий абетковий порядок знаків, що і впервинній;
- мала кількість можливих ключів (рівна величині абетки).

Метод перестановки

Метод перестановки, також нескладний метод криптографічного перетворення. Використовується, як правило, у поєднанні з іншими методами. При шифруванні цим методом переставляються не літери абетки, а літери відкритого тексту. Наприклад, повідомлення розбите на 4 групи знаків, включаючи пропуски, і в кожній групі літери переставлені відповідно до правила:

[1 2 3 4]
[2 4 1 3]

В цьому випадку фраза:

ОСНОВИ ЗАХИСТУ ІНФОРМАЦІЇ

буде представлена в наступному виді:

СООНИЗВ ХСАИУІТ ФРНОАІМЦЇ.

У випадку перестановки, таблиці частот для двох і трьох літер, показують наявність стандартних літерних пар, дозволяючи реконструювати відкритий текст шляхом пошуку тих перестановок, які їх поєднують. Отже, ключ, що використовується для перетворення відкритого тексту, може бути відновлений за одною криптограмою.

Багатоабеткові шифри

Слабка криптостійкість моноабеткових підстановок (замін) долається з

застосуванням багатоабеткових підстановок (замін). Для захисту від частотного аналізу були розроблені багатоабеткові шифри, в яких для шифрування повідомлення періодично використовується декілька різних абеток підстановки. При шифруванні інформації, букви з номерами 4N+i шифруються i-ою абеткою (1,5,9,13, ... - 1 абеткою, 2,7,10,14, ... – 2 абеткою, і так далі).

Для отримання відкритого тексту виділяються групи знаків, що повторюються, і визначається період повторення. Передбачуваний період перевіряється складанням частотного розподілу для кожної n-ї літери зашифрованого тексту. Якщо кожен з n частотних розподілів має сильну неоднорідність, характерну для багатоабеткової підстановки, то передбачуваний період є правильним. Потім завдання вирішується як n різних простих підстановок.

Методика виконання роботи

1. Розробити алгоритм і скласти програму, що дозволяє закодувати будь-який текст одним з вищевикладених методів і виконати зворотне перетворення. Метод, яким необхідно зашифрувати початкову інформацію, вибирається відповідно до варіанту з таблиць 1,2,3. Мова програмування вибирається довільно.
2. Здійснити вивід на екран або принтер отриману криптограму.
3. Провести дешифрування цієї криптограми, в результаті має бути отриманий початковий текст.
4. Результати роботи оформити у вигляді звіту та захистити його.

Зміст звіту

1. Опис методу, що використовується. Опис початкових даних.
2. Алгоритм роботи програми (блок-схема), текст програми, результати роботи програми.
3. Аналіз результатів роботи, висновки.

Варіанти індивідуальних завдань

Таблиця 1. Методи шифрування

Номер вар.	Метод шифрування	Таблиця	Номер завдання в таблиці	Представлення початкового тексту
1	Підстановка	2	3	Англійська абетка
2	Перестановка	3	1	ASCII -код
3	Багатоабеткові шифри	2	1, 2, 5	Українська абетка
4	Перестановка	3	2	Українська абетка
5	Підстановка	2	4	ASCII -код
6	Багатоабеткові шифри	2	1, 3	Українська абетка
7	Підстановка	2	1	ASCII -код
8	Багатоабеткові шифри	2	2, 3, 4, 5	Англійська абетка
9	Перестановка	3	3	Англійська абетка
10	Підстановка	2	2	Українська абетка
11	Перестановка	3	4	Англійська абетка
12	Багатоабеткові шифри	2	1, 3, 4	Українська абетка
13	Підстановка	2	5	Англійська абетка
14	Багатоабеткові шифри	2	1, 5	Українська абетка
15	Перестановка	3	5	ASCII -код

Таблиця 2. Абетки підстановки

Номер з/п	Вихідна абетка		Абетка підстановки (вар.)									
			1		2		3		4		5	
1	А	A	Б	V	С	C	О	Z	Ю	C	М	V
2	Б	B	Ю	W	О	D	П		Я	D	Н	W
3	В	C	Г	X	У	A	М	.	И	A	О	X
4	Г	D	И	Y	М	B	Н	X	Е	B	П	Y
5	Ґ	E	Є	Z	К	H	Х	Y	Ь	H	Р	Z
6	Д	F	Ь		Х	I	Л	,	Ґ	I	С	
7	Е	G	З	.	Ч	J	И	!	Ш	J	Т	.
8	Є	H	Ш	,	I	E	I	S	Щ	E	У	,
9	Ж	I	И	!	Щ	F	Ж	T	Ц	F	Ф	!
10	З	J	Ц	:	Ж	G	З	:	Ч	G	Х	:
11	И	K	Л	;	Ґ	O	Д	;	Ф	O	Ц	;
12	І	L	Ф	?	Д	P	Е	Q	Х	P	Ч	?
13	Ї	M	Н	-	Э	Q	В	R	Т	Q	Ш	-
14	Й	N	Т	K	В	R	Г	?	У	R	Щ	K
15	К	O	П	L	Я	K	А	-	Р	K	Ґ	L
16	Л	P	Р	M	А	L	Б	N	С	L	Ь	M
17	М	Q	С	N	Б	M	Ю	O	О	M	И	N
18	Н	R	О	O	Ю	N	Я	P	П	N	Е	O
19	О	S	У	P	Г	U	Є	L	М	U	Ю	P
20	П	T	М	Q		V	Е	M	Н	V	Я	Q
21	Р	U	Х	R	Е	W	Ь	U	К	W		R
22	С	V	К	S	Ь	:		V	Л	:	А	S
23	Т	W	Ч	T	З	S	Ш	W		S	Б	T
24	У	X	І	U	Ш	T	Щ	A	Й	T	В	U
25	Ф	Y	Щ	A	І	Z	Ц	B	Ж	Z	Г	A
26	Х	Z	Ж	B	Ц		Ч	C	З		Д	B
27	Ц		Ґ	C	Ї	X	Ф	D	Д	X	Є	C
28	Ч	.	Д	D	Ф	Y	К	E	Є	Y	Ї	D
29	Ш	,	Е	E	Н	;	Т	F	В	;	Ж	E
30	Щ	!	В	F	Т	?	У	G	Г	?	З	F
31	Ь	:	Я	G	П	-	Р	H	А	-	І	G
32	Ю	;		H	Р	.	С	I	Б	.	Й	H
33	Я	?	А	I	И	,	Й	J	Ї	,	К	I
34		-	Ї	J	Л	!	Ї	K	І	!	Л	J

Таблиця 3. Групи перестановок.

Номер вар.	**Група перестановки**
1	$\begin{bmatrix}1 & 2 & 3 & 4 & 5 & 6\\3 & 5 & 2 & 6 & 1 & 4\end{bmatrix}$
2	$\begin{bmatrix}1 & 2 & 3 & 4 & 5\\5 & 4 & 1 & 2 & 3\end{bmatrix}$
3	$\begin{bmatrix}1 & 2 & 3 & 4 & 5 & 6\\2 & 5 & 3 & 4 & 1 & 6\end{bmatrix}$
4	$\begin{bmatrix}1 & 2 & 3 & 4 & 5 & 6\\2 & 6 & 3 & 5 & 1 & 4\end{bmatrix}$
5	$\begin{bmatrix}1 & 2 & 3 & 4 & 5\\2 & 5 & 4 & 3 & 1\end{bmatrix}$

Контрольні запитання

1. Чому метод підстановки має слабку надійність?
2. Що таке частотний аналіз?
3. Що є криптографічним ключем в методі перестановки?
4. Як пов'язані метод підстановки і багатоабеткові шифри?