ЛАБОРАТОРНА РОБОТА № 3

Дослідження афінної системи шифрування Цезаря

Мета роботи:
Ознайомитися з різними шрифтами простої замни (шифрами підстановки) та методами їх криптоаналізу.

Теоретичні відомості

При шифруванні заміною (підстановкою) символи відкритого тексту замінюються символами того ж або іншого алфавіту за завчасно встановленим равилом заміни. У шифрах простої заміни кожен символ вихідного тексту замінюється символами того ж алфавіту однаково на протязі усього тексту. Часто шифри простої заміни називають шифрами одноалфавітної підстановки.

Афінна система підстановок Цезаря

У системі шифрування Цезаря використувалися лише адитивні вастивості множини цілих Z_m. Однак символи множини Z_m можна також множити за модулем m. Застосовуючи одночасно операції додавання та множення за модулем m над елементами множини Z_m, можна отримати систему підстановок, яку називають ***афінною системою підстановок Цезаря***.

$$E_{a,b}(t) = at + b \ (mod\ m),$$

де a,b - цілі числа, $0 < a,b < m$, НСД $(a,m) = 1$.

Необхідно відмітити, що перетворення $E_{ab}(t)$ є взаємно однозначним відображенням на множині Z_m тільки в тому випадку, якщо найбільший спільний дільник (НСД(a,m)), рівний одиниці, тобто a і m повинні бути взаємно простими числами.

Наприклад, нехай $m = 26$, $a = 3$, $b = 5$. Тоді, очевидно, НСД (3,26) = 1, і ми отримуємо таке співвідношення між числовими кодами літер:

Таблиця 1 – Співвідношення між числовими кодами літер

t	0	1	2	3	4	5	6	7	8	9	10	11	12
$3t + 5$	5	8	11	14	17	20	23	0	3	6	9	12	15

t	13	14	15	16	17	18	19	20	21	22	23	24	25
$3t + 5$	18	21	24	1	4	7	10	13	16	19	22	25	2

Перетворюючи числа у літери англійської мови, отримаємо наступні співвідношення між літерами відкритого тексту та шифротексту:

Таблиця 2 – Відповідність між літерами відкритого тексту та шифротексту

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	Q	P	R	S	T	U	V	W	X	Y	Z
F	I	L	O	R	U	X	A	D	G	J	M	P	S	V	Y	B	E	H	K	N	Q	T	W	Z	C

Відкрите повідомлення **NIGHT** перетворюється у шифротекст **SDXAK.**

Перевагою афінної системи є зручне керування ключами – ключи шифрування і розшифровуання подаються у компактній формі у вигляді пари чисел (*a, b*).

Недоліки афінної системи аналогічні недолікам всіх шифрів підстановки.

Афінна система використовувалася на практиці кілька століть тому, а сьогодні її застосування обмежується більшою мірою ілюстрацією основних положень криптографії.

Система Цезаря з ключовим словом

Система шифрування Цезаря ***з ключовим словом*** – це також одноалфавітна система підстановки. Особливостю цієї системи є можливість використання ключового слова для зміщення та зміни порядку символів у алфавіті підстановки.

Виберемо деяке число k, $0 < k < 25$, і слово або коротку фразу в якості ***ключового слова***. Бажано, щови всі літери ключового слова були різними. Ехай вибрано слово **DIPLOMAT** у якості ключового слова та число $k = 5$.

Ключове слово записується під літерами абетки, починаючи з літери, числовий код якої співпадає з вибраним числом k:

Таблиця 3 – Підписування ключового слова

0	1	2	3	4	5					10					15					20					25
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	Q	P	R	S	T	U	V	W	X	Y	Z
					D	**I**	**P**	**L**	**O**	**M**	**A**	**T**													

Решту літер абетки підстановки записуються після ключового слова у алфавітному порядку:

Таблиця 4 – Записування решти літер алфавіту підстановки

0	1	2	3	4	5					10					15					20					25
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	Q	P	R	S	T	U	V	W	X	Y	Z
V	W	X	Y	Z	**D**	**I**	**P**	**L**	**O**	**M**	**A**	**T**	B	C	E	F	G	H	J	K	N	Q	R	S	U

Тепер ми маємо підстановку для кожної літери довільного повідомлення.

Відкрите повідомлення **SEND MORE MONEY**
шифруеться як **HZBY TCGZ TCBZS**.

Треба відмітити, що вимога про відмінність усіх літер ключового слова необов'язкова. Можна просто записати ключове слово (або фразу) без повторення однакових літер. Наприклад, ключова фраза

КАК ДЫМ ОТЕЧЕСТВА НАМ СЛАДОК И ПРИЯТЕН

і число k = 3 породують таку таблицю підстановок:

Таблиця 5 – Таблица подстановок

0			3												
А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П
Ь	Э	Ю	**К**	**А**	**Д**	**Ы**	**М**	**О**	**Т**	**Е**	**Ч**	**С**	**В**	**Н**	**Л**

Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
И	**П**	**Р**	**Я**	Б	Г	Ж	З	Й	У	Ф	Х	Ц	Ш	Щ	Ъ

Перевагою сисеми Цезаря з ключовим словом є той факт, що кількість можливих ключових слів практично невичерпна.

Недоліком цієї системи є можливість розкриття шифротексту на основі аналізу частот появи літер.

Підготовка до роботи

1. Підгрупа розбивається на пари за бажанням.
2. Один з пари пише програму шифрування за афінною системою Цезаря для текстових файлів.
3. Програма повинна задовільняти наступним умовам: читати файл з відкритим текстом з диску; шифрувати його за допомогою афінної системи Цезаря з ключем, що вводиться з клавіатури; зберігати шифрограму у текстовому файлі. Приклад зовнішнього вигляду форми введення даних такої програми зображено на рис.1.
4. Другий з учасників пари пише програму розшифрування. Програма повинна задовільняти наступним умовам: читати з файлу отриману шифрограму зі значеннями ключа; обчислювати таблицю заміни та виводити розшифрований текст на екран.

Виконання роботи

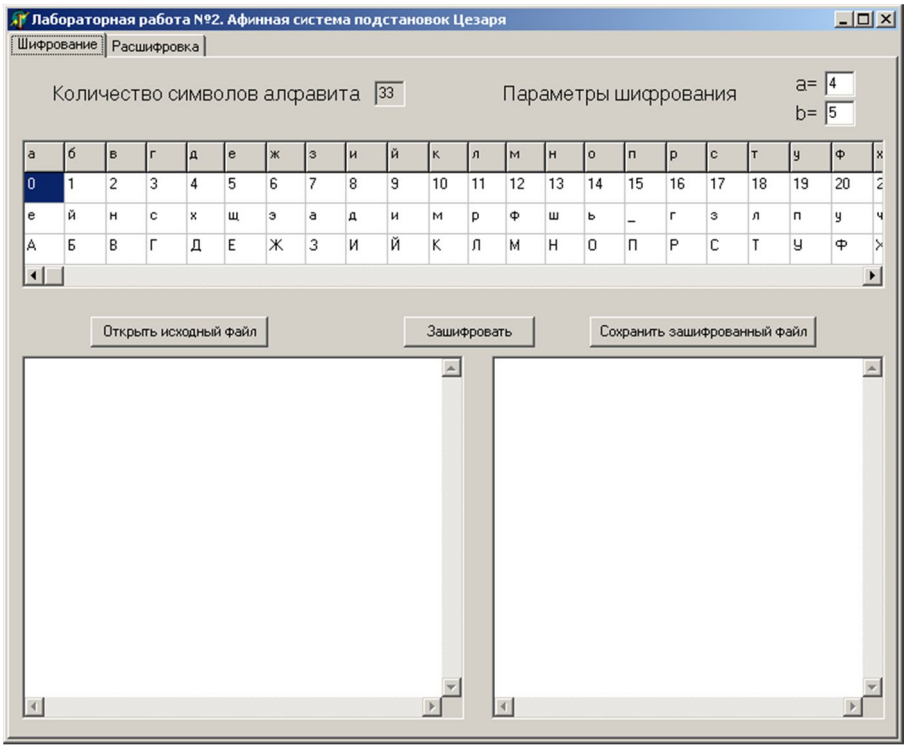
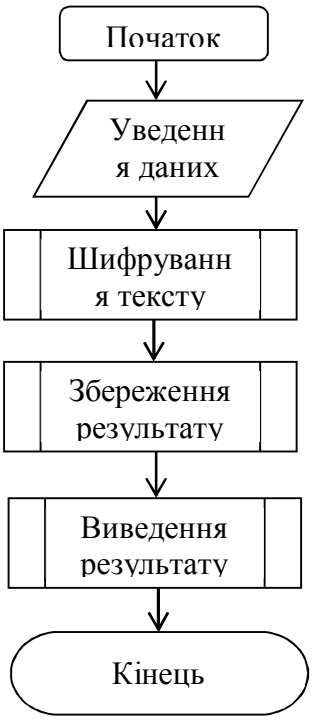


Рис.1. Приклад програми шифрування афінним методом Цезаря.

1. Зашифровані першим учасником пари файли передаються для криптоаналізу другому учаснику.

1 Блок-схема алгоритму

Шифрування



2. По результатах лабораторної роботи напишіть звіт.
3. Звіт повинен містити:
    1. Протоколи дій учасників пари.
    2. Розшифрований текст.
    3. Ключ афінної системи Цезаря, при якому отримано результат.