Лабораторна робота № 3.

Вивчення афінної системи шифрування Цезаря.

У системі шифрування Цезаря (лаб. работа № 2) використовувалися лише адитивні властивості множини цілих Z. Однак символи множини Z_n можна також множити за модулем n. Застосовуючи одночасно операції додавання та множення за модулем n над елементами множини Z_n, можна отримати систему підстановок, яку називають ***афінною системою підстановок Цезаря:***

$$E_{a,b}(t) = at + b \pmod n,$$

де a, b – цілі числа, $0 < a$, $b < n$, $НСД(a, n) = 1$.

Зауважимо, що перетворення $E_{a,b}(t)$ є взаємно однозначним відображенням на множині Z_n тільки в тому випадку, якщо найбільший спільний дільник ($НСД(a, n)$), дорівнює одиниці, тобто a і n повинні бути взаємно простими числами.

Наприклад, для англійського алфавіту, нехай $n = 26$, $a = 3$, $b = 5$. Тоді, очевидно, $НСД(3, 26) = 1$, і ми отримуємо співвідношення між числовими кодами літер, яке наведено у табл. 5.

Таблиця 5

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 в літери англійської мови, отримаємо представлені у табл. 6 співвідношення між літерами відкритого тексту та шифротексту.

Таблиця 6

Співвідношення між літерами відкритого тексту та шифротексту

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

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

Перевагою афінної системи, крім вищої порівняно зі звичайною системою Цезаря крипостійкістю, є зручне керування ключами – ключі подаються в компактній формі у вигляді пари чисел (a, b).

Тепер розглянемо шифрування українською мовою. Вважаємо, що потужність алфавіту $n = 32$. Будемо використовувати відкритий текст “Лабораторна робота з криптографії”.

Використаємо такі числа: $n = 32$, $a = 3$, $b = 5$. Оскільки $НСД(3, 32) = 1$, то ми можемо використати їх для створення афінної системи Цезаря.

Отже, отримаємо таблицю заміни (табл. 7).

Таблиця 7

Співвідношення між числовими кодами літер української мови

t	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	16
$3t+5$	5	8	11	14	17	20	23	26	29	0	3	6	9	12	15	21

t	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
$3t+5$	24	27	30	1	4	7	10	13	16	19	22	25	28	31	2

На основі цієї таблиці отримаємо таблицю відповідності літер української мови (табл. 8).

Таблиця 8

Співвідношення між літерами відкритого тексту та шифротексту українською мовою

А	Б	В	Г	Д	Е	Є	Ж	З	И	І	Ї	Й	К	Л	М
Е	З	Ї	Л	О	С	Ф	Ч	Ь	А	Г	Є	И	Й	М	П
Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ю	Я
Т	Х	Ш	Ю	Б	Д	Ж	І	К	Н	Р	У	Ц	Щ	Я	В

Отже маємо таку шифрограму для нашого відкритого тексту: “МЕЗХЮЕДХЮТЕЮХЗХДЕЬЙЮАШДХЛЮЕІГЄ”.

Для криптоаналізу підрахуємо частоти появи літер: Ю, Х та Е зустрічаються по 5 разів. Ототожнивши Ю з О, не отримаємо зв'язного тексту, а якщо ототожнимо Х з О, тоді отримаємо рівняння $24 = (a \times 17 + b) \bmod 32$, яке треба розв'язати відносно a та b. Для розв'язку замало даних: потрібне друге рівняння. Другим рівнянням може бути $НСД(a, n) = 1$. Тоді маємо $a = 1, 3, 5, 7, \ldots$. Одиницю навряд чи використовували б, пробуємо 3. Тоді маємо рівняння $24 = (3 \times 17 + b) \bmod 32$. Звідки $b = 5$. Тепер отримуємо таблицю заміни (табл. 8). Застосовуючи таблицю, одержимо розшифроване повідомлення.

Завдання роботи.

1. Народне прислів’я українською мовою, обране для лаб. работи № 1, зашифрувати методом афінної системи підстановок Цезаря. Величина параметру a дорівнює номеру студента у списку підгрупи дорівнює, а b – номеру комп’ютера, за яким працює студент.
2. Розшифрувати повідомлення, використовуючи частоту появи літер у шифротексті.