ЛАБОРАТОРНА РОБОТА № 1. КЛАСИЧНІ ШИФРИ ТА ЇХ КРИПТОАНАЛІЗ

Мета роботи: набути вміння із зашифрування та дешифрування повідомлень за допомогою шифрів Цезаря, Плейфера, Хілла, Віженера, використовуючи частотний криптоаналіз, навчитися зламувати шифротекст, зашифрований методом простої заміни.

Матеріально-технічне забезпечення: ПК зі встановленим програмним забезпеченням MS Excel та доступом до мережі Інтернет, текстові повідомлення для шифрування згідно варіанту.

Теоретичні відомості

ШИФР ЦЕЗАРЯ

Розглянемо один з найдавніших та найбільш поширених шифрів простої (моноалфавітної) заміни – шифр Цезаря, названий на честь римського імператора *Гая Юлія Цезаря*. У цьому шифрі кожна літера повідомлення зсувається в алфавіті на *K* позицій вперед від символу, що замінюється. При досягненні кінця алфавіту виконується циклічний перехід до його початку. При необхідності розділові знаки та пробіли ігноруються. Таким чином, наприклад, літерам алфавіту відповідатимуть числові позиції (табл. 1.1, табл. 1.2):

Таблиця. 1.1. Нумерація позицій літер англійського алфавіту

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
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

Таблиця. 1.2. Нумерація позицій літер українського алфавіту

А	Б	В	Г	Ґ	Д	Е	Є	Ж	З	И	І	Ї	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ю	Я
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	26	27	28	29	30	31	32

Ключем шифрування є деяке фіксоване секретне число *K* – від 1 до 25 для англійського (латинського) алфавіту та *K* – від 1 до 32 для українського. При дешифруванні літера зашифрованого тексту замінюється на літеру розташовану в алфавіті на *K* позицій назад.

Приклад 1.1:

Відомо, що Цезар для шифрування використовував ключ *K*=3, тобто відбувався зсув символів повідомлення на три позиції вперед у латинському алфавіті (рис. 1.1). Отже, повідомлення римського імператора *ALEA JACTA EST* (Жереб кинутий) після зашифрування буде мати вигляд *DOHDMDFWDHVW*.

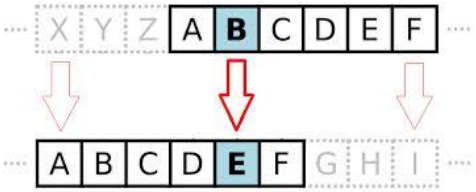

Рис. 1.1. Заміна символів повідомлення у шифрі Цезаря з ключем K=3

Зазначимо, що цей алгоритм шифрування, на сьогоднішній день, являється нестійким до зламу і не використовується на практиці, проте є важливим для вивчення. Оскільки відомо, що навіть дуже складні сучасні криптосистеми в якості типових складових використовують прості шифри заміни.

ЧАСТОТНИЙ КРИПТОАНАЛІЗ

Криптоаналіз шифру Цезаря ґрунтується на *частотному аналізі* появи окремих символів природньої мови у тексті. Частота символу у повідомленні дорівнює кількості його появи у тексті, поділеній на загальну кількість літер тексту. Для кожної мови справедливо наступне: у досить довгих текстах кожна літера зустрічається із приблизно однаковою частотою, залежно від самої літери і незалежно від конкретного тексту. Тобто імовірність появи окремих літер, а також їх порядок у словах і фразах природньої мови підпорядковуються статистичним закономірностям. Так, наприклад, відомо, що в українській та англійській мовах частоти появи літер розподілені наступним чином (табл. 1.3).

Таблиця. 1.3. Частоти появи літер в українській та англійській мовах

Українська мова						**Англійська мова**					
А	0,072	**Ї**	0,006	**У**	0,04	**A**	0,082	**J**	0,002	**S**	0,063
Б	0,017	**Й**	0,008	**Ф**	0,001	**B**	0,015	**K**	0,008	**T**	0,091
В	0,052	**К**	0,035	**Х**	0,012	**C**	0,028	**L**	0,040	**U**	0,028
Г, Ґ	0,016	**Л**	0,036	**Ц**	0,006	**D**	0,043	**M**	0,024	**V**	0,010
Д	0,035	**М**	0,031	**Ч**	0,018	**E**	**0,127**	**N**	0,067	**W**	0,023
Е	0,017	**Н**	0,065	**Ш**	0,012	**F**	0,022	**O**	0,075	**X**	0,001
Є	0,008	**О**	**0,094**	**Щ**	0,001	**G**	0,020	**P**	0,019	**Y**	0,020
Ж	0,009	**П**	0,029	**Ь**	0,029	**H**	0,061	**Q**	0,001	**Z**	0,001
З	0,023	**Р**	0,047	**Ю**	0,004	**I**	0,070	**R**	0,0060		
И	0,061	**С**	0,041	**Я**	0,029						
І	0,057	**Т**	0,055								

Отже, літера з найбільшою частотою в шифротексті буде замінюватися на літеру з найбільшою частотою у мові. А кількість позицій між ними буде визначати довжину ключа. Однак, якщо текст не дуже великий, то закономірності будь-якої природньої мови можуть проявлятися в ньому не обов’язково в строгій відповідності з таблицею частот. В такому випадку розглядається відношення наступної літери за частотою появи у зашифрованому тексті та найчастішою літерою мови.

Приклад 1.2:

Дано текст, зашифрований за допомогою шифру моноалфавітної заміни: ДАФИНЦШЕИЮЯЗЩШФЬИТЧИВЮЯШХСЯЯЗВИЇШЧШЮФЬСПЄСПИЇОЛРПЧИ ЦРЗФЬРІИЇЇШЛСЯИФСЦРЇЧЄШЦАСЇШЧШІСХЗЧИЮДАФИНЧИЮЮИЦРВЧМЦИ УШЙШЧСЛМЇСЛЯШЙШЕШЇШЧШЮФЬСПЄ

При зашифруванні відкритого тексту використовувався алфавіт АБВГҐДЕЄЖЗИІЇЙКЛМНОПРСТУФХЦЧШЩЬЮЯабвгґдеєжзиіїйклмнопрстуфхцчш щьюя. Припускаючи, що текст зашифрований за допомогою шифру Цезаря, складемо таблицю появи літер в даному шифротексті (табл. 1.4).

Таблиця. 1.4. Зустрічальності літер у шифротексті

А	**Б**	**В**	**Г, Ґ**	**Д**	**Е**	**Є**	**Ж**	**З**	**И**	**І**	**Ї**	**Й**	**К**	**Л**	**М**
3	0	3	0	2	2	3	0	4	14	2	8	2	0	4	2
Н	**О**	**П**	**Р**	**С**	**Т**	**У**	**Ф**	**Х**	**Ц**	**Ч**	**Ш**	**Щ**	**Ь**	**Ю**	**Я**
2	1	4	5	10	1	1	7	2	6	10	16	1	4	7	6

З табл. 1.4 видно, що найчастіше у тексті з’являється літера «Ш» – 16 разів. А з табл. 1.3 відомо, що найчастіше в текстах українською мовою зустрічається літера «О». Тому можемо припустити, що літері «Ш» в шифротексті, ймовірно, відповідає літера «О» у відкритому тексті. Якщо послідовності літер А, Б,…, О,…, Ш,…, Я ототожнити із послідовністю їх позицій в алфавіті 0, 1,…, 18,…, 28,…, 33, то можна обчислити ключ *K*: 28–18=10. Тепер ми можемо відновити початкове повідомлення, записавши його із розділовими знаками: *Шукаємо щастя по країнах, століттях, а воно скрізь і завжди з нами; як риба в воді, так і ми в ньому, і воно біля нас шукає нас самих. Нема його ніде від того, що воно скрізь.*

ШИФР ПЛЕЙФЕРА

Шифр Плейфера є біграмним, тобто текст повідомлення розбивається на біграми (групи з двох символів). Таким чином, шифр Плейфера є більш стійкий до зламу у порівнянні із шифром простої заміни, так як ускладнюється його частотний аналіз. Він може бути проведений, але не для 26 можливих символів (англійський алфавіт), а для 26x26 = 676 можливих біграм.

Для шифрування шифр Плейфера використовує матрицю 5x5 (для англійського алфавіту), яка містить ключове слово або фразу. Щоб скласти ключову матрицю, в першу чергу потрібно заповнити порожні клітинки матриці літерами ключового слова (виключаючи літери, що повторюються), потім заповнити клітинки, що лишилися символами алфавіту, що не зустрічаються в ключовому слові, по порядку (рис. 1.2). В

англійських текстах зазвичай пропускається символ «Q», щоб зменшити алфавіт, в інших версіях «I» і «J» об'єднуються в одну клітинку.

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

Рис. 1.2. Матриця шифру Плейфера

Ключове слово може бути записано у верхньому рядку матриці зліва направо, або по спіралі з лівого верхнього кута до центру.

Для того щоб зашифрувати повідомлення, необхідно розбити його на біграми (групи з двох символів) та відшукати ці біграми в матриці. Два символи біграми відповідають кутам прямокутника в ключовий матриці. Визначаємо положення кутів цього прямокутника відносно один одного. Потім, керуючись наступними 4 правилами, зашифровувати пари символів вихідного тексту.

Правила шифрування біграм

1. Якщо дві літери біграми однакові – додаємо після першого символу «X», зашифровуємо нову пару літер.
2. Якщо літери біграми знаходяться в різних стовпцях і різних рядках – замінюємо їх на літери, що знаходяться в тих самих рядках (стовпцях), але відповідно в інших кутах прямокутника.
3. Якщо літери біграми зустрічаються в одному рядку – замінюємо їх на літери, розташовані в найближчих стовпцях праворуч від відповідних літер. Якщо літера остання у рядку, то вона замінюється на перший символ цього ж рядка.
4. Якщо літери біграми зустрічаються в одному стовпці – перетворюємо їх в літери того ж стовпця, що знаходяться безпосередньо під ними. Якщо літера є нижньою в стовпці – вона замінюється на першу літеру цього ж стовпчика.

Приклад 1.3:

Зашифруємо повідомлення HIDE THE GOLD IN THE TREE STUMP із використанням ключової фрази PLAYFAIR EXAMPLE. Матрицею шифрування буде матриця описана вище (рис. 1.2).

Для шифрування розіб'ємо текст на біграми HI DE TH EG OL DI NT HE TR EX ES TU MP. Знайдемо літери першої біграми у матриці та замінимо їх на літери, що знаходяться у протилежних кутах прямокутника (рис. 1.3).

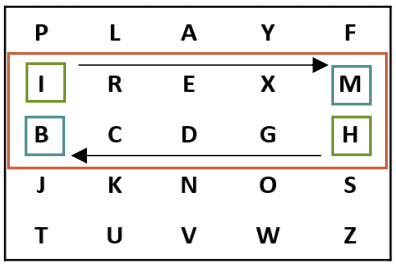

Рис. 1.3. Шифрування біграм

Далі, користуючись правилами шифрування біграм, отримаємо шифротекст: BM ND ZB XD KY BE JV DM UI XM MN UV IF.

ШИФР ВІЖЕНЕРА

На протязі століть використання простого моноалфавітного шифру заміни було достатнім, щоб забезпечити таємність. Подальший розвиток частотного криптоаналізу, спочатку арабами, а потім і в Європі, зруйнував його стійкість. Таким чином криптографи мали придумати новий, більш стійкий шифр. Вчений епохи Відродження *Леона Батіста Альберті* вперше запропонував замість одного секретного алфавіту, використовувати два або більше, послідовно або циклічно змінюючи їх за певним правилом. Ґрунтуючись на ідеях попередника, свій шифр створив французький посол в Римі *Блез де Віженер*.

Шифр Віженера складається з послідовності декількох шифрів Цезаря з різними значеннями зсуву, що визначаються літерами ключового слова. Кожна літера відкритого тексту зсувається вперед на позицію відповідної літери ключа. Якщо ключове слово менше за повідомлення, то воно циклічно повторюється.

Приклад 2.1:

Повідомлення *ATTACK AT DAWN* зашифруємо ключем *LEMON*. В результаті чого отримаємо шифротекст *LXFOPVEFRNHR*.

	A	T	T	A	C	K	A	T	D	A	W	N
	L	E	M	O	N	L	E	M	O	N	L	E
	0	19	19	0	2	10	0	19	3	0	22	13
+	11	4	12	14	13	11	4	12	14	13	11	4
	11	23	5	14	15	21	4	5	17	13	7	17
	L	X	F	O	P	V	E	F	R	N	H	R

Для зашифровування може використовуватися й таблиця, яка отримала назву таблиця Віженера (таб.2.1). У загальному випадку таблиця Віженера складається з

алфавіту, циклічно зміщеного на один символ ліворуч. Під час зашифрування кожна літера повідомлення замінюється на літеру, що знаходиться на перетині літер першого рядка (алфавіт повідомлення) і першого стовпчика (алфавіт ключа) в таблиці Віженера.

Таблиця. 2.1. Таблиця Віженера

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

Приклад 2.2:

Повідомлення *PURPLE*, зашифроване ключем *SMART* за допомогою таблиці Віженера (табл. 2.2), перетвориться у шифротекст *HGRGEW* .

Таблиця. 2.2. Шифрування повідомлення за таблицею Віженера

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

При дешифруванні потрібно відшукати у першому стовпчику літеру ключа і за літерами шифротексту визначити, в якому стовпчику зверху знаходиться літера відкритого тексту.

КРИПТОСИСТЕМА ХІЛЛА

У 1929 році американський математик *Лестер Хілл* придумав новий поліграмний шифр заміни, в якому використовувалися як модульна арифметика, так і лінійна алгебра.

Ключем шифру є квадратна матриця $K(n\times n)$, елементи якої числа від 0 до 25, $\det K \neq 0$, $n \geq 2$. Літери алфавіту нумеруються в порядку їхнього зростання від 0 до 25. При шифруванні відкритий текст розбивається на блоки з n літер, числові значення яких розглядаються як вектор розмірності n. Кожен вектор множиться на матрицю шифрування $K(n\times n)$ по модулю 26 (для англійського алфавіту).

Приклад 2.3:

Повідомлення *HELP* зашифруємо за допомогою ключової матриці:

$$K = \begin{pmatrix} 3 & 3 \\ 2 & 5 \end{pmatrix},\ det\, K = 15 - 6 = 9 \neq 0.$$

Розіб'ємо відкритий тест на вектори розмірністю 2, літерам поставимо у відповідність їх числові значення:

$$P_1 = \begin{pmatrix} H \\ E \end{pmatrix} = \begin{pmatrix} 7 \\ 4 \end{pmatrix} \qquad P_2 = \begin{pmatrix} L \\ P \end{pmatrix} = \begin{pmatrix} 11 \\ 15 \end{pmatrix}.$$

Помножимо ключову матрицю на кожен вектор відкритого тексту та отримаємо шифротекст *HIAT*:

$$K \cdot P_1 = \begin{pmatrix} 3 & 3 \\ 2 & 5 \end{pmatrix} \cdot \begin{pmatrix} 7 \\ 4 \end{pmatrix} = \begin{pmatrix} 33 \\ 34 \end{pmatrix} mod\ 26 = \begin{pmatrix} 7 \\ 8 \end{pmatrix} = HI;$$

$$K \cdot P_2 = \begin{pmatrix} 3 & 3 \\ 2 & 5 \end{pmatrix} \cdot \begin{pmatrix} 11 \\ 15 \end{pmatrix} = \begin{pmatrix} 78 \\ 97 \end{pmatrix} mod\ 26 = \begin{pmatrix} 0 \\ 19 \end{pmatrix} = AT.$$

Для того щоб дешифрувати повідомлення, кожен блок шифротексту з n літер множиться на обернену (за модулем 26) матрицю до матриці шифрування.

Шифротекст *HIAT* дешифруємо за допомогою матриці оберненої до ключової: $K^{-1} = \begin{pmatrix} 15 & 17 \\ 20 & 9 \end{pmatrix}$ та отримаємо повідомлення *HELP*.

$$K^{-1} \cdot P_1 = \begin{pmatrix} 15 & 17 \\ 20 & 9 \end{pmatrix} \cdot \begin{pmatrix} 7 \\ 8 \end{pmatrix} = \begin{pmatrix} 241 \\ 212 \end{pmatrix} mod\ 26 = \begin{pmatrix} 7 \\ 4 \end{pmatrix} = HE;$$

$$K^{-1} \cdot P_2 = \begin{pmatrix} 15 & 17 \\ 20 & 9 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 19 \end{pmatrix} = \begin{pmatrix} 323 \\ 171 \end{pmatrix} mod\ 26 = \begin{pmatrix} 11 \\ 15 \end{pmatrix} = LP.$$

Завдання до лабораторної роботи

Завдання 1

Завдання виконується індивідуально кожним студентом. Усі необхідні обчислення зі скріншотами описуються у звіті.

Створити програму для шифрування повідомлень в середовищі *MS Excel* із використанням шифру Цезаря (англійській алфавіт). Значення ключа шифрування визначається номером за алфавітним списком студента у журналі. Зашифрувати своє прізвище та дешифрувати отриманий шифротекст. Зразок виконання завдання наведено на рисунку нижче (рис. 1.4).

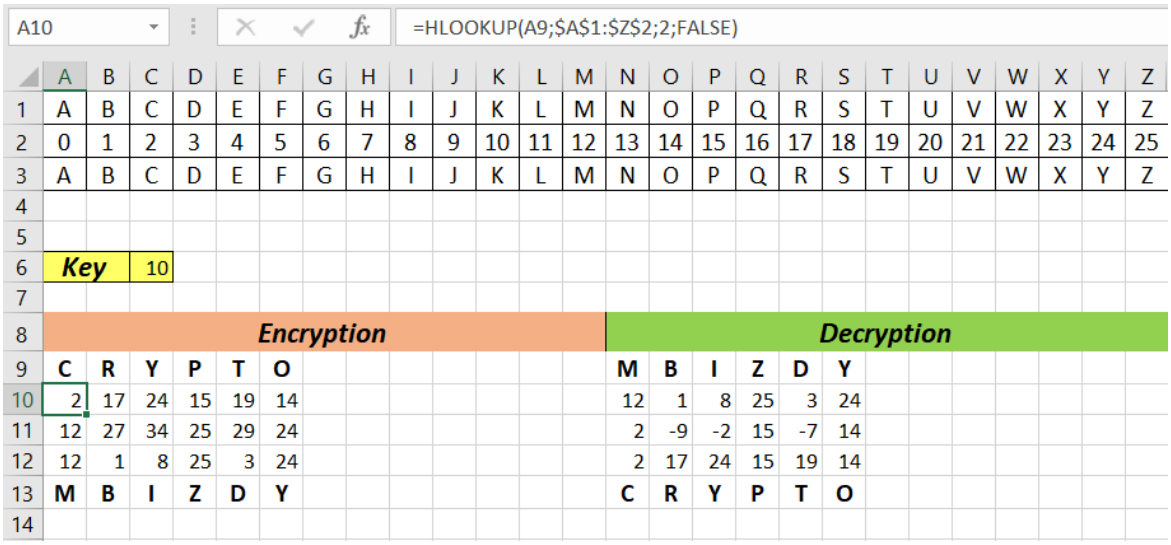

Рис. 1.4. Шифрування шифром Цезаря в середовищі MS Excel

Завдання 2

За допомогою частотного криптоаналізу відновити текст, зашифрований алгоритмом Цезаря згідно варіанту (мова українська, алфавіт АБВГҐДЕЄЖЗИІЇЙКЛМНОПРСТУФХЦЧШЩЬЮЯ*).*

Варіант №	**Шифротекст**
1.	ЄЧШЦЩЬЦНХЖЕҐЦИЩЦКБКИЖШЬКНЮЩОУДПЧКВЖУППҐЦФОХКЙЖШКФХЦЩКЗКЙЦБДЦІЦЧШОИВЖУОПҐЦИЩПФАЬЦХКИПЙЩЬЮЧОЬДЩЄҐКЗЮЙКЩАЦЙОЬОШЖЙПЩЬДЬОАОФОШЖХТЖФОНЦУЦЬОФОХЦВЖФОЩКШПСМЖЙЖХ
2.	ЮЬЯТЯЬЦВУАЩВИБЗНЧІБЬЛЬЖЬЙЩУЦЬЧТЩОЩЇЙЯТНЩВБТБЬШВФҐБЇЦАЦЬЯЬСЇЙВКЇПШЬКРОЕОЯОСЮОКЩТХЕЇААБТЯЇИБЗАІЯТАТЮЬЮООЯОНЩЗЬЛЬАОСЬЩВУЬАУЩЗЩЇАБВЮЩЬЛЬЯЬЦВЙВНОБЇЦЬИРКЯЇРЇИЕЬИЦУШТЩВЧЬЛЬБЇЯЇАЮЯЬҐЇАЗЦЬ
3.	ЕСГХУЄКВЗЇЬВОЖХЇЄРМЙЧФНФЬЗОЧНЗЇНЗХЗХФХЦЧНЯХЇНЩҐЇХЩЙЖЙШЄУЙЧЄФХБНЦОМФХЗИХЧОБНЧЄЇХШЩОЗЩЙУЧЕЗОБНЬШЗОЩТОЖХЇЄРЧЄМЬЛНЩЩОЗХФХЗНЧХШЩЄКЦЙЧЙЇЩХЖХДУХЗШЗОЛНРЩЧХЕФЇХЗНРСЬГОХЖЇЄКШЗХПУМЄЦЄУХЧХБТНЗНУОШЦЧЄЗЛФОУЄЧХУЄЩХУОЧЙФЧХМЇХЖЬЇҐСХ
4.	ЯЛШМЦЬЇИСЦЯЛШРАВАУЗСРАМВАНЩАУЯАОАЯЛВАРДЖСШАОАЮАНЛАҐЛУХНЛ

Варіант №	Шифротекст
	ГЄАНЛЯЩЛЬЙРГЇЩАОАРДЄДШАОАМЛОЛҐЛГЩЛВМЯХЖКНКЩДЯЛВАРГЩЬЛРЛТЦ ГНАТРЛНЯТУХГҐКЦГНАЧГБАРЦНЛЯЯКВАФДЮРАГНЦРБАЗДНЛЯЯКБЛЯЛГЮХВЯХ Ш
5.	ДХЦФЧШФЛУЕҐВФЖЧЇЯЇЖЕЦШЇЛЩЧМСГНХЇАЕСННВФТМУЇЕЦЇТУФЧЇЄЇІФЯГФЗФ ХЦМЖАЕСМНВФЖЧНТЮШФУЇЖНІЧШЩХМШГЧДВЇЄЩІЇЧЮФІМШМЦЕІНЧШГШМ ЮМТМЦЕУРЕТМЛФСФШМТМУФАЕТМЧЇЦЗНПКЕІЕУ
6.	ЦЗМСЩАЩДБЗАЖШІЯИХЬЩЙТАЮИЄЩЧСФЩКЩЙМСГІОЧЩЄЩЇПСАСРЙБХСУГШ ТГКЩЦЩЯТЙЦБШІЗАЖМЦИШІЯЙТДШЩЗЧБРСХЩЗПСААИЮТМШТЩЇЦСДДИЯИЗА ЖМЦИШІЯИХЧІЦНШЖХТЯЩШҐИЬЫЙЦЩРІКЮНЇНЦЖШСФ
7.	ЧЩЙІҐНШНЬЮЩЯАЩЯЬЩЯТЇЯЬТЦХБЙІШШИЄЩЯЖЇТЦЖЕРШІДБЄНЧЩЙІҐНЙЯТК ЦСЇСШШТЬЦІЯАСМБГЩЙШЩКЩПСААИШІЮЩМБФЩКЩТЯАЩЮСДШЬЫЧИАЖШІ ФҐТШШТЕНШІМЇІШШИЙТХТЙЩЦНЯЖКЩШДІЮ
8.	ЇНВЄЇДОКАОЩЇАКУБУЖЬЮЬБЯУЙЩЬНЧІРТББІЯЬЙТАКЬИАЮЯЇКВЕОАЩЬСНВЄОИ УБКЬПНЬБОЙОЮЯТХНОСЇЙВНЗІЦТҐЬЙАБЇКТЩЛЬЧЬКЩОСЇЧТЄЇБТАІЧИНТЩЬИЙЬЛ НЇЩАБВЮЦЇ
9.	ЩУЦИЦХЖСЬЦХГОСЙЦЬОТЙЦЩКШБЄИЦХЦФЦМКЩЬЖЬОПХПМХЦЕНЖЧЖГХЦЕТ ИПЬТЦЕПМОИЦЕИЦЙЦЕҐЦЧЦИКШЬЖЛИПШЮИЙЦЗШЦПІЦЩЬШОФХЦМКФПШЦНЧ КВКХОФНЖУПНЦФПЗШЮЙЦФИЖЩОУДЩЮАЦФУОХЩДТОС
10.	АЯБФБЯШҐХВЮҐЇГІПЩЙГЯНЯИЯЛЮХШЯЩФЮРЮКЛБФПЮҐГФГЯЬҐЦЕГКШВШЯБЯ УКЛҐМКСЬЯМТРЖРБРУАРМЮФЧЖКВВГФБКЇГІВЙБФВФАЯАРЬРПЮІЯНЯВРУЯЮҐХЯ ВХЮІЮКВГҐАЮЯНЯБЯШҐЛҐПРГКШЯЇТМБКТКЇЖЯЇЙШХЬФЮҐЩЯНЯГКБКВАБЯЕКВІ ШЯ
11.	ФТЧБВАВХЯЧПЧЫГВҐМТВЮҐВЦЕНЇЄПНББМЦБНЮШПБНТНФЩАЦБНЮНАПНРЧДЧА ПВЯШПНОУЕЮНФИШЯШДБВЛШТВЮШБИМЦНГВПБУБВЛТНБШДЕЛПВБНБУЦҐНТЧ ЕКШБНПШЕКБУЦАШБЧЕКДМЛҐШЬНБТҐЄЗВПЧІ
12.	УКАОБЬБОКАІЦЯЇФЩЇЮЬКТБЇЦЯЇАЬИСОЧОЩУПКШТКЇПБЗАІНЯУЙЩЬИЯЬАЬИАЮЬ ЦЬЩКУЦВКШТКЇПБЗАІАЬЩДОСВАБЯУЕЇПУЩОШЇБЬШВЮЬЕТЩВУЦЯЇИЩОШЇПБЇЯ ЇАЄОКЕОЩЦЬ

2.1. Підрахувати частоти зустрічальності літер у шифротексті, використовуючи https://www.cryptool.org/en/cto/n-gram-analysis (рис. 1.5).

2.2. Додати до звіту таблицю частоти зустрічальності літер.

2.3. На основі частоти зустрічальності літер у шифротексті підібрати значення ключа, обґрунтувавши свої дії у звіті.

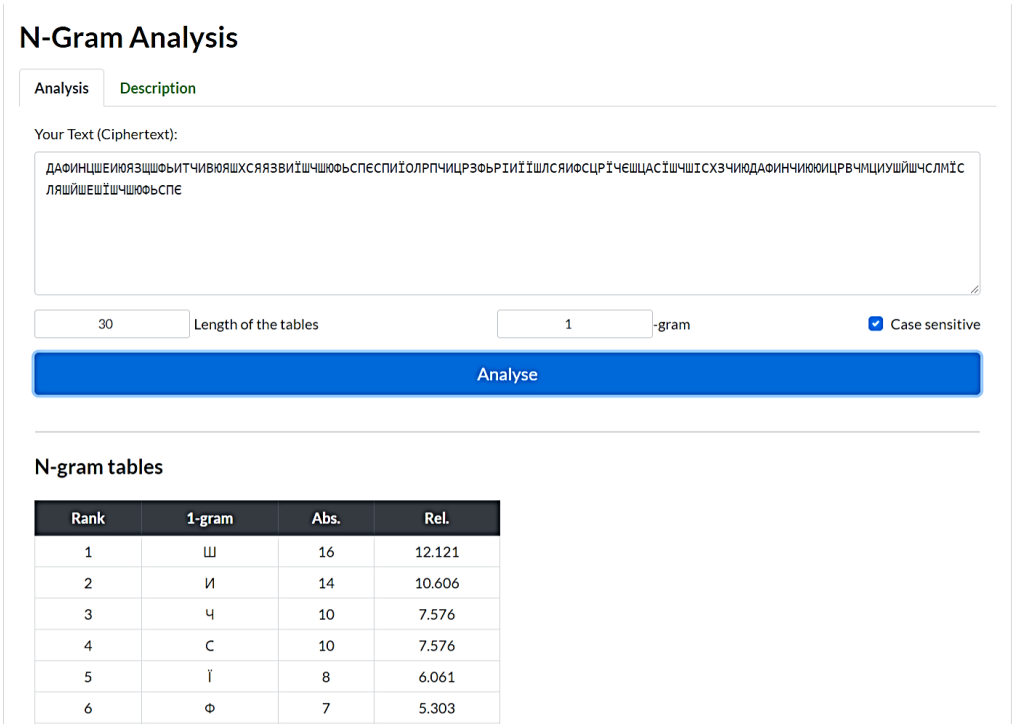

Рис. 1.5. Підрахунок частоти появи літер у тексті

2.4. Ввести шифротекст та значення підібраного ключа на сайті https://www.cryptool.org/en/cto/caesar та відновити повідомлення (рис. 1.6). Додати до звіту скріншот відновленого повідомлення.

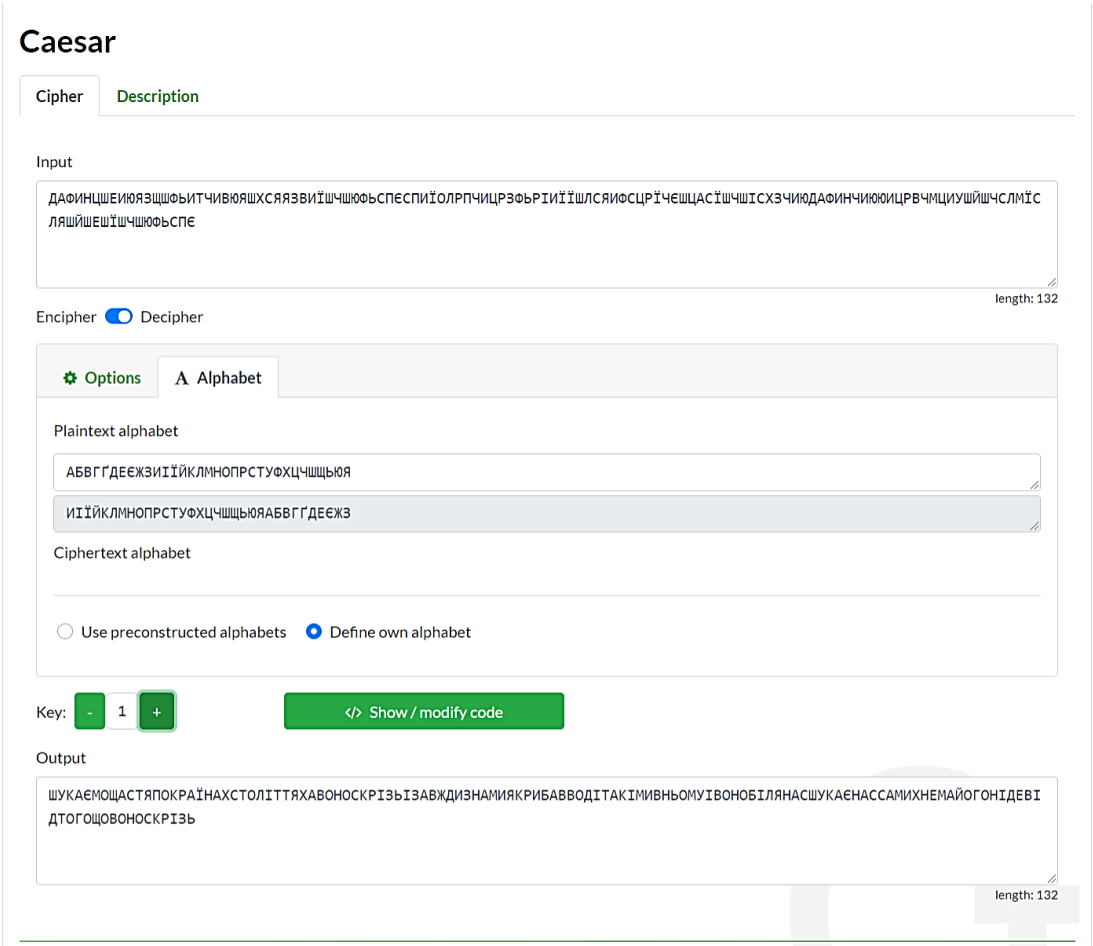

Рис. 1.6. Спроба відновлення повідомлення з підібраним ключем

Завдання 3

Виконати зашифрування повідомлення шифром Плейфера згідно варіанту (визначається номером студента у журналі: непарний – 1 варіант, парний – 2 варіант). Усі кроки алгоритму шифрування виконати описати у звіті.

1. Відкритий текст LITTLE STROKES FELL GREAT OAKS зашифруйте за допомогою шифру Плейфера, використовуючи ключ TRUTH.
2. Відкритий текст TILL FINAL VICTORY зашифруйте за допомогою шифру Плейфера, використовуючи ключ LIFE.

Завдання 4

Виконати зашифрування та дешифрування повідомлення шифром Віженера. Усі кроки алгоритму шифрування виконати вручну та описати їх у звіті.

4.1. Використовуючи шифр Віженера з ключовим словом TIME зашифруйте відкритий текст LIKE CURES LIKE.

4.2. Використовуючи шифр Віженера з ключовим словом WISDOM, дешифруйте зашифрований текст ADWUMFDQFJMAQKSQWYWOAQSUOZWDZ.

Завдання 5

Виконати зашифрування повідомлення згідно варіанту (визначається номером студента у журналі: непарний – 1 варіант, парний – 2 варіант). Усі кроки алгоритму шифрування описати у звіті. Обчислення можна виконувати в MS Excel.

1. У криптосистемі Хілла з матрицею $\begin{pmatrix} 11 & 2 & 19 \\ 5 & 23 & 25 \\ 20 & 7 & 1 \end{pmatrix}$ зашифруйте текст LOT TRY CAT.

2. У криптосистемі Хілла з матрицею $\begin{pmatrix} 11 & 14 & 19 \\ 19 & 17 & 24 \\ 2 & 0 & 18 \end{pmatrix}$ зашифруйте текст OUT OF DATE.

Контрольні запитання:

1. Дайте визначення поняттям: криптологія, криптографія та криптоаналіз.
2. У чому полягає забезпечення конфіденційності, цілісності, дійсності, доступності, інформаційних ресурсів?
3. Що таке криптографічний алгоритм та шифр?
4. Що таке криптографічний ключ?
5. Розкрийте поняття зашифрування та дешифрування даних.
6. Дайте визначення відкритого та закритого тексту.
7. Назвіть складові криптографічної системи.
8. У чому полягає криптостійкість криптографічної системи?
9. Дайте коротку класифікацію шифрів.
10. Опишіть алгоритм шифрування Цезаря.

11. У чому суть методу частотного криптоаналізу?
12.Опишіть алгоритм шифру Плейфера.
13. Поясніть відмінність між шифрами моноалфавітної та поліалфавітної заміни.
14. Опишіть алгоритм шифрування Віженера.
15. Що являє собою ключ у криптосистемі Хілла?
16. Опишіть алгоритм шифрування криптосистемою Хілла.