ЛАБОРАТОРНА РОБОТА № 2. КЛАСИЧНИЙ ШИФР ПОЛІАЛФАВІТНОЇ ЗАМІНИ ТА ЙОГО КРИПТОАНАЛІЗ. КРИПТОСИСТЕМА ХІЛЛА

Мета роботи: набути вміння із шифрування повідомлень за допомогою шифру поліалфавітної заміни, зокрема шифру Віженера; використовуючи методи Казіскі та Фрідмана, навчитися зламувати шифротекст, зашифрований методом поліалфавітної заміни; навчитися шифрувати повідомлення у криптосистемі Хілла.

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

Теоретичні відомості

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.

МЕТОД КАЗІСКІ та МЕТОД ФРІДМАНА (індекс збігу)

У 1863 році офіцер прусської армії, майор *Фрідріх Казіскі* запропонував метод зламу поліалфавітного шифру на прикладі шифру Віженера. Метод Казіскі заснований на наступній ідеї: повторення літер в ключі разом з повторенням літер у відкритому тексті дає повторення літер в зашифрованому тексті. Автор прийшов до висновку, що відстань між повтореннями в шифротексту будуть рівні або кратні довжині (періоду) ключа. Щоб знайти довжину ключа виконаємо наступні дії:

1) знайдемо у шифротексті однакові відрізки довжиною не менше трьох символів (зауважмо, що такі однакові відрізки можуть з'явитися в тексті з досить малою ймовірністю);
2) визначимо відстань між стартовими позиціями відрізків у шифротексті;
3) візьмемо один із спільних дільників цих відстаней в якості довжини ключа.

Для уточнення довжини ключа будемо використовувати метод Фрідмана, що був винайдений американським криптологом *Вільямом Фрідманом* у 1920 році. Цей метод базується на обчислені індексу збігу (ІЗ), який дозволяє визначити для деякої послідовності $x = (x_1 x_2 \dots x_n)$ з літер алфавіту $A = \{a_1, a_2, \dots, a_m\}$ ймовірність того, що два випадкових елемента цієї послідовності збігаються. Значення ІЗ обчислюються за формулою:

$$I_c(x) = \frac{\sum_{i=0}^{m-1} n_i(n_i-1)}{n(n-1)}, \qquad (2.1)$$

де n_i – кількість появи літери *i* в послідовності *x, n* – загальна кількість літер в x.

Довжину ключа можна визначити за формулою:

$$l \approx \frac{k_p - k_r}{I_c(x) - k_r + \frac{k_p - I_c(x)}{n}}, \qquad (2.2)$$

де $k_r = \frac{1}{m}, k_p = \sum_{i=0}^{m-1} p_i^2$, де p_i – частота появи літери *i* в природній мові.

Відомо, що ІЗ рядків осмисленого тексту для різних природніх мов такий:

$I_c(x) = 0{,}058$ – українська мова;

$I_c(x) = 0{,}065$ – англійська мова

Нехай криптограма $c = (c_1 c_2 \dots c_n)$, отримана за допомогою шифру Віженера з ключем рівним *l*. Запишемо її літери в *l* стовпців.

Таблиця. 2.3. Запис шифротексту за довжиною ключа

C_1	C_2	…	C_l
c_1	c_2	…	c_l
c_{l+1}	c_{l+2}	…	c_{2l}
c_{2l+1}	c_{2l+2}	…	c_{3l}
…	…	…	…

Якщо довжину ключа визначено правильно, то кожний стовпець C_i – це відрізок відкритого тексту, зашифрованого простою заміною. Тоді ІЗ кожного стовпця буде близьким до ІЗ осмислених текстів цією мовою. Наприклад, для осмислених текстів англійською мовою ІЗ лежатиме в межах $0{,}038 < I_c(x) < 0{,}065$. Якщо довжину ключа визначено неправильно, то стовпці C_i будуть випадковими, а ІЗ таких стовпців буде близьким до 0,038.

Для текстів англійською мовою довжину ключа можна визначити за таблицею 2.4.

Таблиця. 2.4. Визначення довжини ключа за значенням ІЗ

l	***1***	***2***	***3***	***4***	***5***	***6***	***7***	***8***	***9***	***10***	∞
$I_c(x)$	0,0667	0,0525	0,0478	0,0445	0,0441	0,0431	0,0424	0,0414	0,0410	0,0407	0,0384

Припустимо, що на першому етапі ми знайшли довжину ключа *l*. Тепер для кожного стовпчика C_i визначимо літери, що найчастіше повторюються та за допомогою частотного аналізу знайдемо літери ключа.

Приклад 2.3:

Дано текст, зашифрований шифром Віженера:

MRGFNIATXZQVFFNUXFFYBTCETYXIIXGZKACJLRGKQYEIXOYYAUAPX
YIJLHPRGVTSFPAYNNYURZOPHXWYXLFRNUTZBRFKAHFWFZESYUWZ
MOLLBSBZBJHFPLXKHVIVMZTZHUIWAETIUEDFGLXDIEXIYJIUXPNNEI
XABVCINTVCIEZYYDAZGZIWTYXJIKTRZLMFFKALGZNVKZXIIMXUUNA
PGVXFUSMISKHVYVOCRVXRIWTYXZOIRFNUXZNXLDUDPZGVHVOWM
OYJERLAUGLVTUXTHRBUQZTYTXORNKBASFFXGHQVDSHUYJSYHDYU
WYXYYKHVTUCDACAHXSEVGJIEFZGLXRSBXSYKOEPPNYAKTUACEFYI
LFWEAHCIAUALLZNXMVCKLRRHGFNXMOYUESKPM

Потрібно визначити ключ та прочитати текст.

Використаємо спочатку метод Казіскі для знаходження довжини ключа. У шифротексті триграма TYX зустрічається 3 рази. Відстань між першою і другою появою становить 156 символів, між першою і третьою – 210. НСД (156, 210) = 6, тому можна припустити, що довжина ключового слова рівна 6.

Для підтвердження гіпотези скористаємося методом Фрідмана. Обчислимо ІЗ за формулою (2.1) для всього шифротексту $I_c(\text{с}) = 0{,}043$. Обчислимо довжину ключа за формулою (2.2): $l \approx 6{,}64$. За отриманими даними та за таблицею 2.4 можна зробити висновок, що довжина ключового слова обрана правильно і дорівнює 6.

Запишемо шифротекст у таблицю із 6 стовпчиків (табл. 2.5).

Таблиця. 2.5. Запис шифротексту за довжиною ключа 6

C_1	C_2	C_3	C_4	C_5	C_6
M	R	G	F	N	I
A	T	X	Z	Q	V
F	F	N	U	X	F
F	Y	B	T	C	E
T	Y	X	I	I	X
G	Z	K	A	C	J
L	R	G	K	Q	Y
E	I	X	O	Y	Y
A	U	A	P	X	Y
I	J	L	H	P	R
G	V	T	S	F	P
A	Y	N	N	Y	U
R	Z	O	P	H	X
W	Y	X	L	F	R
N	U	T	Z	B	R
F	K	A	H	F	W
F	Z	E	S	Y	U
W	Z	M	O	L	L
B	S	B	Z	B	J
H	F	P	L	X	K
H	V	I	V	M	Z
T	Z	H	U	I	W
A	E	T	I	U	E
D	F	G	L	X	D
I	E	X	I	Y	J
I	U	X	P	N	N
E	I	X	A	B	V
C	I	N	T	V	C
I	E	Z	Y	Y	D
A	Z	G	Z	I	W
T	Y	X	J	I	K
T	R	Z	L	M	F
F	K	A	L	G	Z
N	V	K	Z	X	I
I	M	X	U	U	N
A	P	G	V	X	F
U	S	M	I	S	K

C_1	C_2	C_3	C_4	C_5	C_6
H	V	Y	V	O	C
R	V	X	R	I	W
T	Y	X	Z	O	I
R	F	N	U	X	Z
N	X	L	D	U	D
P	Z	G	V	H	V
O	W	M	O	Y	J
E	R	L	A	U	G
L	V	T	U	X	T
H	R	B	U	Q	Z
T	Y	T	X	O	R
N	K	B	A	S	F
F	X	G	H	Q	V
D	S	H	U	Y	J
S	Y	H	D	Y	U
W	Y	X	Y	Y	K
H	V	T	U	C	D
A	C	A	H	X	S
E	V	G	J	I	E
F	Z	G	L	X	R
S	B	X	S	Y	K
O	E	P	P	N	Y
A	K	T	U	A	C
E	F	Y	I	L	F
W	E	A	H	C	I
A	U	A	L	L	Z
N	X	M	V	C	K
L	R	R	H	G	F
N	X	M	O	Y	U
E	S	K	P	M	

Підрахуємо кількість появи кожної літери алфавіту по стовпцях. Занесемо дані в таблицю 2.6 (комірки, що позначені кольором відповідають літерам, що зустрічаються найчастіше).

Таблиця. 2.6. Кількості появи літер по стовпцям шифротексту

	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**
C_1	9	1	1	2	6	7	2	5	5	0	0	3	1	6	2	1	0	3	2	6	1	0	4	0	0	0
C_2	0	1	1	0	5	5	0	0	3	1	4	0	1	0	0	1	0	6	4	1	4	8	1	4	9	8
C_3	6	4	0	0	1	0	9	3	1	0	3	3	5	4	1	2	0	1	0	7	0	0	0	13	2	2
C_4	4	0	0	2	0	1	0	6	5	2	1	7	0	1	4	5	0	1	3	2	9	5	0	1	2	6
C_5	1	3	5	0	0	3	2	2	6	0	0	3	3	3	3	1	4	0	2	0	4	1	0	10	11	0
C_6	0	0	3	4	3	6	1	0	4	5	6	1	0	2	0	1	0	5	1	1	4	4	4	2	4	5

Знайдемо тепер саме ключове слово. Так як кожен з стовпців таблиці є результатом зашифрування фрагменту відкритого тексту простою заміною, то спробуємо застосувати частотний аналіз, тобто виконаємо зсув відносно літери, що найчастіше зустрічається у кожному стовпці (табл. 2.7).

Таблиця. 2.7. Визначення літер ключового слова із застосуванням частотного аналізу

Стовпець шифротексту	Літера, що найчастіше зустрічається	Зсув відносно E	Можлива літера ключового слова
C_1	A	0 – 4 mod 26 = 22	W
	E	4 – 4 mod 26 = 0	A
	F	5 – 4 mod 26 = 1	B
	N	13 – 4 mod 26 = 9	J
	T	19 – 4 mod 26 = 15	P
C_2	Y	24 – 4 mod 26 = 20	U
	V	21 – 4 mod 26 = 17	R
	Z	25 – 4 mod 26 = 21	V
	R	17 – 4 mod 26 = 13	N
C_3	X	23 – 4 mod 26 = 19	T
	G	6 – 4 mod 26 = 2	C
	T	19 – 4 mod 26 = 15	P
	A	0 – 4 mod 26 = 22	W
C_4	U	20 – 4 mod 26 = 16	Q
	L	11 – 4 mod 26 = 7	H
	H	7 – 4 mod 26 = 3	D
	Z	25 – 4 mod 26 = 21	V
C_5	C	2 – 4 mod 26 = 24	Y
	I	8 – 4 mod 26 = 4	E
	X	23 – 4 mod 26 = 19	T
	Y	24 – 4 mod 26 = 20	U
	U	20 – 4 mod 26 = 16	Q
C_6	F	5 – 4 mod 26 = 1	B
	K	10 – 4 mod 26 = 6	G
	J	9 – 4 mod 26 = 5	F
	R	17 – 4 mod 26 = 13	N
	Z	25 – 4 mod 26 = 21	V
	V	21 – 4 mod 26 = 17	R

Отже, ключове слово: ARTHUR. Тепер можемо дешифрувати текст, розділяючи слова пропусками: Many traces we found of him in the bog girt island where he had hid his savage ally a huge driving wheel and a shaft half filled with rubbish showed the position of an abandoned mine beside it were the crumbling remains of the cottages of the miners driven away no doubt by the foul reek of the surrounding swamp in one of these a staple and chain with a quantity of gnawed bones showed where the animal had been confined a skeleton with a tangle of brown hair adhering to it lay among the debris.

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 2.4:

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

Виконати зашифрування, дешифрування та криптоаналіз повідомлення, зашифрованого шифром Віженера згідно варіанту (визначається номером студента у журналі). Усі кроки алгоритму шифрування описати у звіті.

1. Виконати зашифрування тексту шифром Віженера на сайті *CrypTool Online* – *https://www.cryptool.org/en/cto/* з використанням шаблону *Vigenère* згідно варіанту (ключове слово обрати самостійно):

Варіант №	**Відкритий текст**
1.	Two things are infinite: the universe and human stupidity; and I am not sure about the universe. Albert Einstein
2.	Live as if you were to die tomorrow. Learn as if you were to live forever. Mahatma Gandhi
3.	Darkness cannot drive out darkness: only light can do that. Hate cannot drive out hate: only love can do that. Martin Luther King
4.	Happiness is when what you think, what you say, and what you do are in harmony. Mahatma Gandhi
5.	Peace cannot be achieved through violence, it can only be attained through understanding. Ralph Waldo Emerson
6.	It has become appallingly obvious that our technology has exceeded our humanity. Albert Einstein
7.	Far and away the best prize that life has to offer is the chance to work hard at work worth doing. Theodore Roosevelt
8.	When you are enthusiastic about what you do, you feel this positive energy. It’s very simple. Paulo Coelho
9.	It is fine to celebrate success, but it is more important to heed the lessons of failure. Bill Gates
10.	Between the great things we cannot do and the small things we will not do, the danger is that we shall do nothing. Adolph Monod
11.	Courage is what it takes to stand up and speak; courage is also what it takes to sit down and listen. Winston S. Churchill
12.	A cat has absolute emotional honesty: human beings, for one reason or another, may hide their feelings, but a cat does not. Ernest Hemingway
13.	Tell me and I forget. Teach me and I remember. Involve me and I learn. Benjamin Franklin
14.	When something is important enough, you do it even if the odds are not in your favor. Elon Musk
15.	Even if I knew that tomorrow the world would go to pieces, I would still plant my apple tree. Martin Luther King

2. Додати скріншот зашифрування до звіту. Описати алгоритм шифрування у звіті на прикладі перших 2-3 слів відкритого тексту.
3. Обмінятися шифротекстом та ключами із іншим студентом своєї групи.
4. Виконати дешифрування шифротексту одногрупника на сайті на сайті *CrypTool Online* – *https://www.cryptool.org/en/cto/* з використанням шаблону *Vigenère*.
5. Додати скріншот дешифрування до звіту. Описати алгоритм дешифрування у звіті на прикладі перших 2-3 слів шифротексту.
6. Виконати криптоаналіз шифротексту, зашифрованого шифром Віженера згідно варіанту:
    a) Обчислити довжину ключа за методом Казіскі. Здійснити пошук триграм, що повторюються можна, використовуючи шаблон *N-Gram Analysis* в розділі криптоаналізу на сайті *https://www.cryptool.org/en/cto/*;
    b) Обґрунтувати довжину ключа, використовуючи метод Фрідмана. Обчислити індекс збігу можна за допомогою MS Excel. Додати скріншот обчислення індексу збігу та описати хід обчислень у звіті;
    c) Знайти літери ключового слова, використовуючи частотний аналіз;
    d) Відновити початкове повідомлення із знайденим ключем та додати скріншот до звіту.

Варіант №	**Шифротекст**
1.	MFXIVVBYIXXHJGAYFJTZVKVQQZNIJHMFXIJHBZTPOHXKZSAJBVPSCHBVEMYOURAWNWJJB ARKTGMARZNCTQNNJEMASUNVVHFZJYWTRZJNQPYQJMMVYRXVBLRRQUEIURUVASZHTEM PBYJJCWJHMFXIGKFKTSIHBZTPSLSUCWJHMFXIJKJEIPYVJVUWYRXKEIURUVELRQBVIVRKZI BARKTGMAUHSNMTYDDXIQRVBVPSCHBYMRJHHIGRRYJITSFHDFCVURUVVIIHWXQZRXUNPI AVTDMSAHLZDIFXUFVCBXYYMCZDDJBMYOMFXINVDFCHB
2.	PVVCHWGFYLPVLCWOGFXXYVKZVADRCDPSZDEAQRFVACLCVKICDDNSTZQJSTEHZARJEAH YPBWZNLBOVRGHXSVYDJRNTOHPVXDUPVHHRSCTYARREKKIJLQZZZGHOPVQRNSKSLOCEP DJRZYHWQYZIPVVXZAJVQRQBUPDYVFEKAFRYGIOPMHAOTSWEAVHHRSSPHJTFCFARRADN HWZUPVVDDISIPDOCEDWDOKXHWBJEKWHKSLOUFZGXMVTVXCKSDCCFOEUSWZUPVVADO HKPQPVFFVWBUJHWFJLQZOGCHHIUPWKKYLWSWCWFKAV
3.	BTESSAFISTWDTGRBFHOROEAXIBTENEZPEYXBASGCBTEEEZQTNIBTITKAKOAKMFAYLIYEJS NNEIECEECSZPSJMUUNOWPFHKQEARJWATRORSFHOROETNEBEEKQMPLOQQFLKWAIHKRBT EEAMDEORGAUXLMMDZSVAMUVMFHGRTUVOROEIFIETETXPQYXIJDOAKPFOAXJGTOXAYOX IBTATXPMTOWVFIZXPQMUWBUMVSZFATXBTITKAXIKXWACRSAQTUAPQRKZMDYUYZEEIV MFHKEZFIYFCDIKHTUKKPIZDSEZWSZSIFRKEAGRKCWGRKRMYIKWEAURHTAVKXWETKETM WGC

Варіант №	Шифротекст
4.	VOEZUWVTEEIMHBLGNMPNIAZLGDOERHKAHVTOKZTUKMPHBVRMVFOSZLGOUZGROPNQZS EVREKPCAENRPKASPURVLNGYAGSIIKSPHPYGGKKIFREPKOSOKPVRNTGGPNGNIOPDFZSHILN IOULAFUJKUFVTMVFAAJMVDAFTSVTENTXVOAGCIUOOHRHXVYNMIHHRGNIUJIRTGGZENILU ARNORKUGVTMVZOJTHKYEPZMQUHNBIJPTUKVVVHNXQGKUFRMVALRHYVZOZKHCFTUKTK LCVTKVVGRZLGYOSJMUZOPOEVLDXTSYSEQMIYPLYUTGUUCYYEOTRXVKMYVTKXPSGGWQ MRRGPKAYNTHQMOHXJTPGUZJWSPBYMVPOAZLGYEVTXJHTJKWJHLYKMVOEEMSOHDSXSO AHRXIXLLNZMQUOELPGLFEUQVOEYOKJAIAZSVOECKEELAAJWCMEGESHHNRCHCYKNMI
5.	WEVGCDYEXIGLECVSXHGADRDGVUYLUMAINEIYYSVFTJOTIILEFELROTXWIQWMTXAPHREL ONJWTCWPWTQVBINFWDVPGVWEPUCDYKPSLXHGWXPEPGTAHGRNSUJEKINVXWIAPWLIRV SPUUGWIMOPCDYVGFTINCWZIDQVILEJYHLOHERSUPXGCRQESETPMVLTQVILEGBEICVECXP CYHIOHEGSOOJJPLQJEIORPTAHGRHSMGSCIIUNJWTCFDYTVSHTECODVMQWIFECYIMFWPDJA NPILEOSBINVEUXETXWIDQSGGLQWTWAPHNSUTIPPOPIXRTJILLONIWSUUITECJSCIIUHXJFGV TRTASJONQAPRDCPAZETCQIAWXXJUNMUCOWPXWTGRRERGJJPLA
6.	ZJYGIGYMNCCACCOXMBLVSWZSZJYGISFVGWHGYIRAUUKWAFRJVPLTSVEKOXCGYIRKCENS RKSFKMLDWSPSUWLCCSILCGYIRKIYKMMSHRCCYGIJZPLDCFVCOMKVCPHSJRESFJWREHSOV BNMLDGUFACGBPVVNXCEPSUJKRCPBWWAXQOJSBMIRATNKVAYSQPFEXOYCWYGIVEWTW OQFJFWSYZRGUCATIRFSQFXHWFFDMGZHRMINKSPIITDMEVNOAQRSCCGBGIESLWSRRIFRVM MDMOYZWCGACRWSACARXESBQRPTJIVJXIUOAULAKHUVMNLSEVWTKCSFXHWFFZRMABQ KLEFWEIISHSPKMVWCSNLELVRIXHSHCVVSGBXESWKOYFXOXDRFTLWKUVVENSEKLALDRI WOFABMISZSBIWHWKVCPIEARUMALSYPQACSSIMEFRFRRDOVREXHSHCVVSGBSRGEKOGIEG WRLKLEJSJZPLTSCCINLMBWTEGDYVAHGKVCPCGARKSHWZC
7.	ZMWSWZPPWPSMZWOXBPAZLKSIETDRKMXMVRTSNIKVOEKNLJFQAVHLZXKEDDMPKEFBCG NPWDRMJLUOCEAGGXFEHMWSMQUMKDBPSPWQOSWQFWVQUWHHBFDMKXBIETDUWEAPW DFUPAKDTQDMJHWFOESUATAIJWVQZIAVWQOOMDFPUWMIFAIMNHFKDIJPVQWZQRIDZZWD AEWZWVKQABSQRFKUGUFASJJLBSOBZHAFNCWKSMNQKWVQLTSFSIDMJHWXKDWBCGZMW SWZPPWPSMZWOKWPZMFIODWESBOOHWUNCRHMSYSEWUGRBNAIEUOKBWJJSFUWMUKAA ASQRXABQRIDPZGXPXAADDMMJLOKSZWOSLBUPAERFZEVYWVQUTDZOEDIODMTAIJLHEOI XHVQWZKLHESIJPVQWZLKSPWQKHGSQIJGMAQNJRAQRMJBVMNUZHODUWMURDAIEVODAA OHSFWVVWCYKZJRKNNQFJHTAULUIQDMSUWEPPWSZMYMOKSDAQDRJQUWM
8.	HCIISXFZWRGSJSKBSWRKICXITPUAHKWOPWRAZPLVXFBIRIVAVJPFAXFDPNMXWHPLVXFOS EVGPSFHKAIKPBZAZAROSPDIHIKIVAQXDCNAYTBUSLDDARKWSYEXTHKJVTRPLVBHDIPHCII YDKBPPDIPTRHHUSLPBZXYTDWVKDTUSLIVWXBCCSWZIKWWNGCJKKDWITIXGKRKWSIMEI VAJZGGPTCPQAVVYCEGVHPQXJIWHPKWSLPRRSSLVGSUSLAWRIZHHDEKBIYLDDFAHIPPWR UTALXPUCNXYTWNHVEONXLGS
9.	MFWVVOLDIYRTZYTOLPKRIIGPTJEYEYWKHZGWHLDNHCBWTZHLPRYNSEARTOLPLBYREDL TAOXPKVDJRNXDOMIHBKHOLPBECMIOBSLZPLFGSJJDMRRNXSXETCIMKVEUIOBVDOSZTEDO LPKVWVWYHEODWPLRVZXSXURDTLGUTDGVEVOAALMVROLLMIAISFMFFXPPYKSVROLGIG PPWUORRWXRFWCWXRFOSEAVBMSHGVAMXSHWTCITLCAIHEAVADVHTJCJSWFFINXLGUCGI LKRNYTCXJEIXWRVVZREAVSJYYWFFOLPPRTZVHTJSOMWEKHZFPTJTGEJALDYPPWFNOLPIR LZFPTTHVROMYENXLBESNTCXRDDRNASYDRNA
10.	WHMCCZGULRTQQYKGZBSIXMKPSXFPPISDBSLSEIDXWQTAPSFMTRZUASISPJFXARGZYDUM OSOZVZASZLELWZIYHYQBDXAXTLWQACNEFUBHMDXAWMVQWAIFXQVIWXMGELAZOSGD AWILFQYKAZIWPLTMDIUDMEXZACRLLEBSELTIGITQMYWLMVOMFSICSMZLDSHMBTIFFTJTM EPTRYFPPFMFBZRXAZLVAPMESLTMESHFPPVWMTEVGGJWIKUVWMXQPLTHQVHLWZBSSKQP THVQVOSGDADXSKKWSKQLQSJFWZPGZO
11.	LWOUIOWOFVWPMDCVPYCVWROIRAOAPXGUMCRQIHKRYHWJMUWEUGSEEVLGHEYLGSRG EEDNNCTNNKKZIIPXZTITKJPYXMKXOPWLWEASTIAKRYAIOTKTSQJWIETRAIYCRVIHTMDAIP ASZIPKLDFKRVIHCXLWEALSKEDIWCURSFIHGZWGGGSXIHGKJTAVWWRRGXACSPELRHGWL WEAPWPRPWGBEVLACGQJLWEYMKSOOAZXCJMKDFISGSAPHEDRGSXIHGQWGEMRGLLGHYT WJMUWIUSXTVKP
12.	PRSKMGLSFZZRYCTCMANMSOMYSFEGMRCITCEGWIOKPRHVEMINSPYBSBKETCINYXINMZW PYXEAAFUDPQBTMTLBWISJRNMSUIHNAMOIGBUWINXVUKOAGBUJUNMBUQINIEFENYHRHX HDWRLXHZABYPDBVNKYAGPLIIIIKGBVNZHVUXOVAVSHEMRRZWICINYXHZIILVAKTEVECC MANXHPRQLVWCMPOAIGPQLWTMSLBWTJSVJENAIRSXHZWHMJEMMANWOAQVSPIJRFHRDTI GPJIGSBRYPDRGVXHZLRHZEIWVALIIOGOETDXJPPLVPYJSMZVVNLTOLNAXHDWPYYEGXLAS ORMYSINYEAKXHVXCLECZEAKXRVRDBMLDXLDMLGVRAYRIETHMN

Варіант №	Шифротекст
13.	KAYQWWNSGVOMZBFMOJDOZMZDYHQUZQYIYXZPYAZBTLKLGMYAJSUVZSWLUDPQBERWC KTUDNTPXTDMWYYIAVDFNPEETRMOGZAYWEZBDYSDIMOCUEZLZLYHQUEMURABPAYUEIY BURADTBJFAZZSWNQMOQTUDNLKNLUMDENVQCDSSCAVOGYIAVLJQOHMLLISGXAMWTMV OKFKQCDPJAXQKCNTEBCSJIYXZPYAZKPMZRBICCSTEICCTUDNTPXTFMLAMEDARSNDQALLI RATPKTDQTDDFMUTTCXSFMPPTUDTTTJSQDPLBHQVHCFRQIOSQTEIDYQLACCTFLGMDYSDN MWGJFEICCROEBWWNNRTFCSCQLMWTUDXLPJNFADGGLUVRQFNPKWMXEDMWYYIHMDUM EZMGCWWQMYATUZBPPFDQDLQYAFQYEXEFJLAPFQMWBTWZCYQFFQWCGSSQKFPJWQBFPS TAWFPKAYQWGJSRWCCROFQZLFLMVOKJNFIWQZPBWCR
14.	LOEUSWJLTZCXSZIFAKLPVDHEFNFRFYWZFHONSUDOCRWDHHBSWHRHOBJHIGKAHBLOPWU RFUCIDPFHKDWUWHONWPNOCRWDERDAFAODZHLOAWZEXLHDGPGVFISNOPTKDWKZIRBAP JIWSIWUTDBZSJCHDPSUCHKAFLEGHKDLAUBPGSOYSKMYSHZRWZFLFOLPNDZHGBRJZKJFAQ RKMYIPDAJMEFHEGUSLTSWJAQBKLSOYSKMYSHZRWZWHQWFUOWTQDSYRDAFAORINSIIO WPQAOOCRWVTKSNKVRRINHVTHBPAHLWCYJLAWSANVLXHEGUAQRWDSHRDAKMOUOXW ATHFSGYLGFAKAIQHDWMEDFHWZSQSOKHNGCLWUHHONLLDYWOAVNRTLWVPOSSZVEPPN SJEOWBW
15.	TFECVPZEKULXWVYPEREOJTRRPEMCVJSITYRCMTDRLRSKBWIAIAESDRANIBPCCECKVNMNX QLRCZARSRKBWIAIAESLZIPFYGELGTZPTRGCVGMNXGSIPIVYGIGYPWAIRELEJNXIIERLGHZG TWTYRAIRWBCQAEPPSFRQPHITNEIDGEPGIJRDITFSLGTJCSCSZPLPOIVYXECYPGTLNWJRFZHL ITUNSMVFDLAGRZJATUTIVVZPRTRFPRSVBQSNVFMIIETLWAKVDJATGTSNFSDTIIVESNVOPGO DRDMNJBXIAIRLENRGSPEKRZJGFQAVATGTGEDRLRSKBAIRWBCQOMRCENUBGIRRTLMNZAE LEWNNIOWNWPOSFEECCRDWODRLGTFSGMSZBYSFWNTXHFSOISZEPTRRPEMCVVDEMVNYW OWVYZIKVYKTYRAIRWRNXIFAOISZEPH

Завдання 2

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. Поясніть відмінність між шифрами моноалфавітної та поліалфавітної заміни.
2. Опишіть алгоритм шифрування Віженера.
3. У чому полягає метод Казіскі?
4. Як уточнити довжину ключа методом Фрідмана?
5. Що таке індекс збігу?
6. Що являє собою ключ у криптосистемі Хілла?
7. Опишіть алгоритм шифрування криптосистемою Хілла.