ЛАБОРАТОРНА РОБОТА № 1. КЛАСИЧНИЙ ШИФР ПРОСТОЇ ЗАМІНИ ТА ЙОГО КРИПТОАНАЛІЗ. БІГРАМНИЙ ШИФР

Мета роботи: набути вміння із зашифрування та дешифрування повідомлень за допомогою шифру простої заміни, зокрема шифру Цезаря; використовуючи частотний криптоаналіз, навчитися зламувати шифротекст, зашифрований методом простої заміни; навчитися шифруванню біграмним шифром Плейфера.

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*.

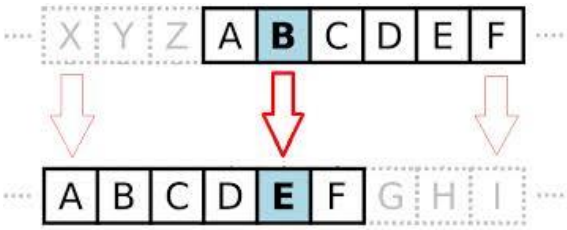


Рис. 1.1. Заміна символів повідомлення у шифрі Цезаря з ключем K=3

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:
ДАФИНЦШЕИЮЯЗЩШФЬИТЧИВЮЯШХСЯЯЗВИЇШЧШЮФЬСПЄСПИЇОЛ
РПЧИЦРЗФЬРІИЇЇШЛСЯИФСЦРЇЧЄШЦАСЇШЧШІСХЗЧИЮДАФИНЧИЮЮ
ИЦРВЧМЦИУШЙШЧСЛМЇСЛЯШЙШЕШЇШЧШЮФЬСПЄ

При зашифруванні відкритого тексту використовувався алфавіт АБВГҐДЕЄЖЗИІЇЙКЛМНОПРСТУФХЦЧШЩЬЮЯабвгґдеєжзиіїйклмнопрсту фхцчшщьюя. 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).

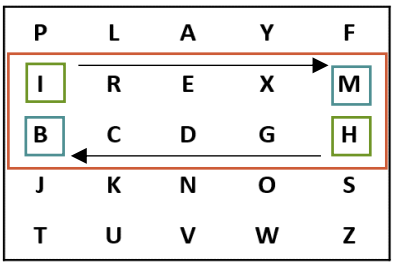


Рис. 1.3. Шифрування біграм

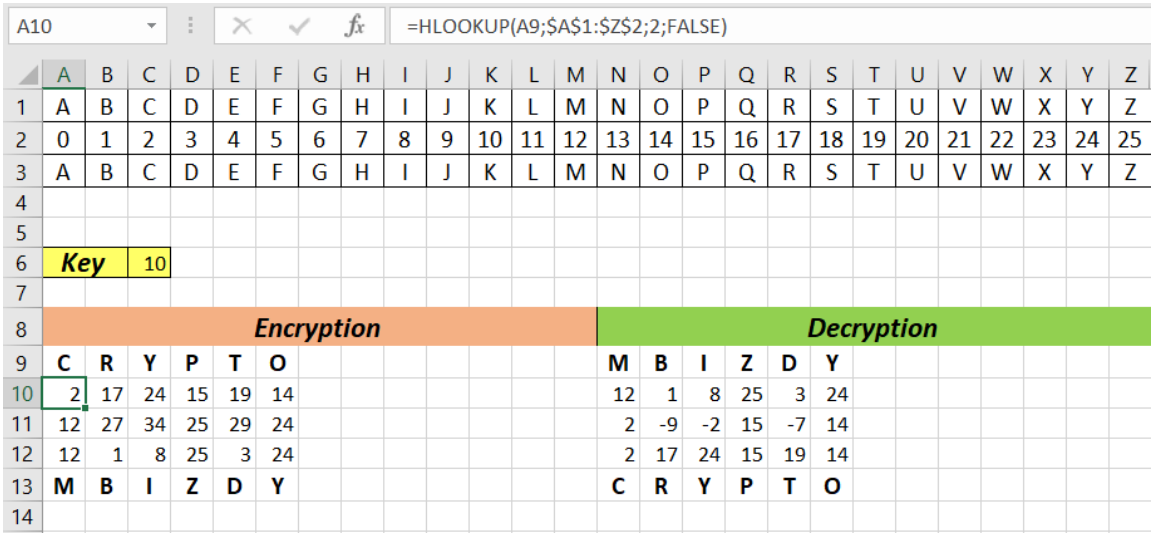
Далі, користуючись правилами шифрування біграм, отримаємо шифротекст: BM ND ZB XD KY BE JV DM UI XM MN UV IF.

Завдання до лабораторної роботи

Завдання 1

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

Створити програму в середовищі *MS Excel* або на будь-якій мові програмування для шифрування повідомлень 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).



A10 =HLOOKUP(A9;$A$1:$Z$2;2;FALSE)

	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
1	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
2	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
3	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
4																										
5																										
6	**Key**	10																								
7																										
8	**Encryption**													**Decryption**												
9	**C**	**R**	**Y**	**P**	**T**	**O**								**M**	**B**	**I**	**Z**	**D**	**Y**							
10	2	17	24	15	19	14								12	1	8	25	3	24							
11	12	27	34	25	29	24								2	-9	-2	15	-7	14							
12	12	1	8	25	3	24								2	17	24	15	19	14							
13	**M**	**B**	**I**	**Z**	**D**	**Y**								**C**	**R**	**Y**	**P**	**T**	**O**							
14																										

Рис. 1.4. Шифрування шифром Цезаря в середовищі MS Excel

Завдання 2

Студентам потрібно поділитися на ротаційні групи з трьох чоловік: СТУДЕНТ-ВІДПРАВНИК, СТУДЕНТ-ОТРИМУВАЧ, СТУДЕНТ-КРИПТОАНАЛІТИК. Обмін повідомленнями між учасниками відбуватиметься за схемою (рис. 1.5), в основі якої лежить секретна система зв'язку, описана Клодом Шеноном.

Рис. 1.5. Схема обміну повідомленнями між студентами

2.1. На сайті *CrypTool Online* – https://www.cryptool.org/en/cto/ з використанням шаблону *Caesar* виконати шифрування тексту шифром Цезаря згідно варіанту. Спочатку введіть відкритий текст до поля ***Input***, потім визначте алфавіт за допомогою опції ***Define own alphabet***, ключ шифрування оберіть самостійно.

Варіант №	Відкритий текст
1.	Єдино можливий порядок розташування знаків надає їм, знакам, ваги символів. Абетка є цілісною і до кінця заповненою даністю. Вона не зрадить і навіть не зміниться. Юрій АНДРУХОВИЧ
2.	Вікно відкрите дивиться у сад, де від дощу піднялись буйно трави. І день, що розпочатий так, навгад, приносить спокій тихий і ласкавий. Марта КАЛИТОВСЬКА
3.	Якщо не можна вітер змалювати, прозорий вітер на ясному тлі, змалюй дуби, могутні і крислаті, котрі од вітру гнуться до землі. Ліна КОСТЕНКО
4.	Блаженний муж, що серед ґвалту й гуку стоїть, як дуб посеред бур і грому, на згоду з підлістю не простягає руку, волить зламатися, ніж поклониться злому. Іван ФРАНКО
5.	Якщо маєш в душі бодай зернину віри в диво, воно приходить до тебе саме – рано чи пізно, в горі чи радості, в темряві чи у світлі. Бодай раз у житті воно виростає перед тобою, мов свіжий трояндовий кущ, і обдає своїм запаморочливим і справжнім ароматом. Ірен РОЗДОБУДЬКО
6.	Пори року існують для того, щоб ніколи не набриднути, тому їх так скоро забуваємо. Вже через певний час стираються риси попереднього сезону, і осінь наступного року буде такою ж вражаючою, як і минулого. Тарас ПРОХАСЬКО
7.	Найбільше і найдорожче добро в кожного народу – це його мова, ота жива схованка людського духу, його багата скарбниця, в яку народ складає і своє давнє життя, і свої сподівання, розум, досвід, почування. Панас МИРНИЙ
8.	І все то те, вся країна, повита красою, зеленіє, вмивається дрібною росою, споконвіку вмивається, сонце зустрічає... І нема тому починку, і краю немає! Тарас ШЕВЧЕНКО
9.	Боротьба захлинулася, але, хай там що, мусила мати продовження. З останніх сил, з останнього зубовного скреготу. Бо жодна катастрофа не ставить хрест на меті. Василь ШКЛЯР
10.	Я просто знаю, що все це варте зусиль і печалі. І що ми недаремно себе до цього привчали. І що всім, хто не відступиться, ще буде сходити радість тихими ранками, золотими ночами. Сергій ЖАДАН
11.	Це вже доля, а долю не обирають. Отож її приймають, яка вона вже є. А коли не приймають, тоді вона силоміць обирає нас. Василь СТУС
12.	Люди оточують нас, як повітря, що ми його вдихаємо, щоб жити. Звуки їхніх голосів лунають для нас вічною музикою життя. Рідні обличчя сяють для нас, як маленькі сонця. Павло ЗАГРЕБЕЛЬНИЙ
13.	Слово – найтонший дотик до серця; воно може стати і ніжною запашною квіткою, і живою водою, що повертає віру в добро, і гострим ножем, і розпеченим залізом, і брудом. Василь СУХОМЛИНСЬКИЙ
14.	А душа, це все на світі, що потрібно для життя. Роби свою справу чесно, з душею, – і твоє до тебе прийде. За будь-яких обставин головне – залишатися людиною. Богдан СТУПКА
15.	Мова – це не просто спосіб спілкування, а щось більш значуще. Мова – це всі глибинні пласти духовного життя народу, його історична пам'ять, найцінніше надбання віків. Олесь ГОНЧАР

2.2. Додати скріншот зашифрування до звіту (рис. 1.6).

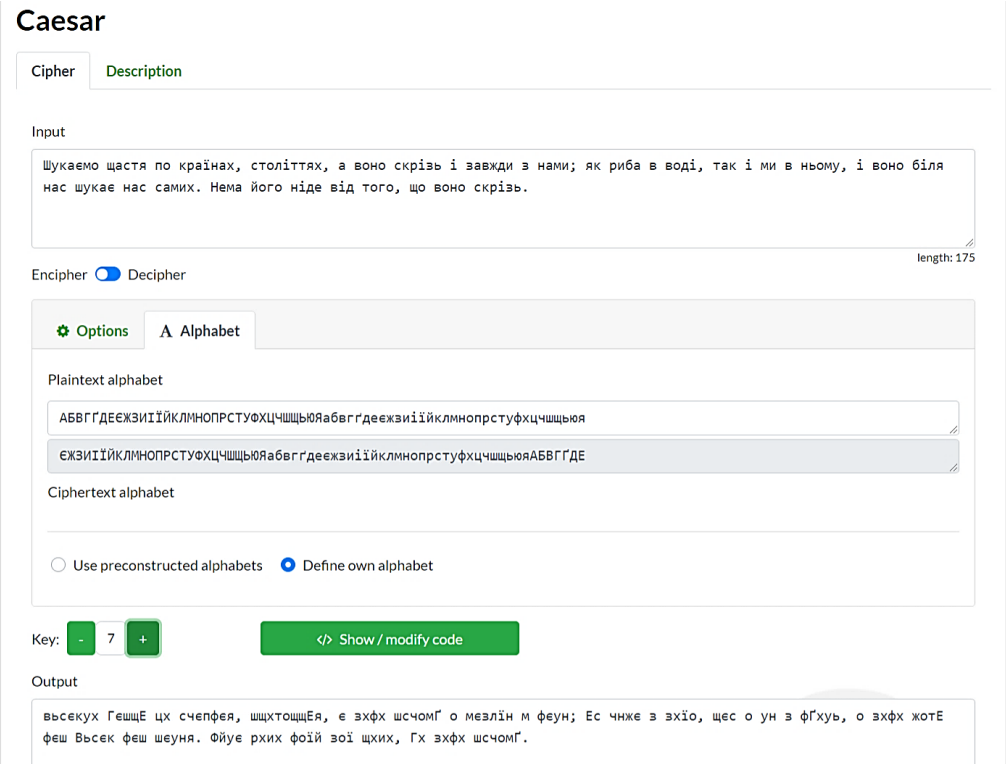


Рис. 1.6. Зашифрування шифром Цезаря

2.3. Зберегти отриманий шифротекст до текстового документу та обмінятися файлами із шифротекстом зі студентом своєї ротаційної групи. Заздалегідь таємно узгодити довжину ключа шифрування.

2.4. Аналогічно до п.2.1 виконати дешифрування повідомлення одногрупника із використанням шифру Цезаря, увівши шифротекст до відповідного текстового поля. При цьому потрібно встановити перемикач у положення ***Decipher***.

2.5. Додати до звіту скріншот дешифрування повідомлення.

2.6. Обмінятися повідомленнями із шифротекстом з іншим студентом своєї ротаційної групи. При чому, довжина ключа шифрування повинна триматися в таємниці.

2.7. Підрахувати частоти зустрічальності літер у шифротексті одногрупника, використовуючи шаблон *N-Gram Analysis* в розділі криптоаналізу на сайті https://www.cryptool.org/en/cto/ (рис. 1.7).

2.8. Додати до звіту таблицю частоти зустрічальності літер.

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

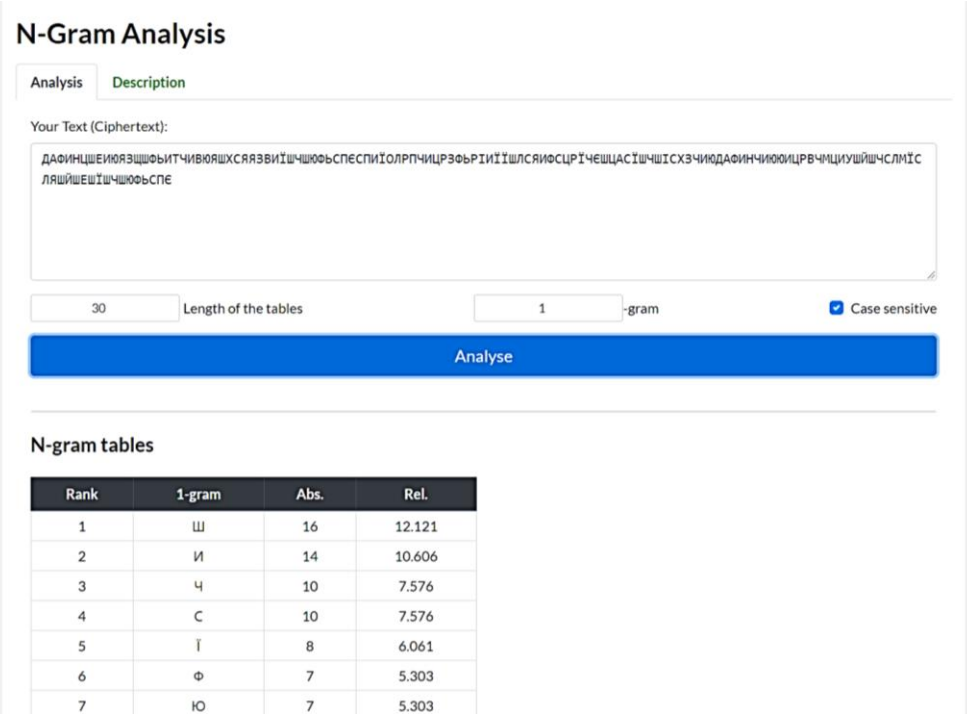


Рис. 1.7. Підрахунок частоти появи літер у тексті

2.10. Ввести шифротекст та значення підібраного ключа на сайті https://www.cryptool.org/en/cto/ з використанням шаблону *Caesar* та відновити повідомлення. Додати до звіту скріншот відновленого повідомлення.

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 вручну та описати їх 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.

Контрольні запитання:

1. Що таке криптографічний алгоритм та шифр?
2. Що таке криптографічний ключ?
3. Назвіть складові криптографічної системи.
4. У чому полягає криптостійкість криптографічної системи?
5. Опишіть алгоритм шифрування Цезаря.
6. У чому суть методу частотного криптоаналізу?
7. Опишіть алгоритм шифру Плейфера.
8. Що є ключем у шифрі Плейфера?