­­МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ “ЛЬВІВСЬКА ПОЛІТЕХНІКА”

­­­



Лабораторна робота №1-4

з курсу «Технології захисту інформації»

для студентів базового напрямку 6.08.04 "Комп’ютерні науки"

(заочна форма навчання)

Варіант 8

Виконав студент гр. КНз-3

Чалий Михайло

­­

Львів 2015

## Мета роботи

Дослідження статистичних властивостей відкритого тексту (ВТ) та шифрованого тексту (ШТ), вивчення простих методів шифрування та дешифрування інформації та їх властивостей.

## Теоретичні відомості

*2.1. Криптографічні системи*

Перетворення секретної інформації – це кодування даних, яке використовується для маскування інформації. Ці перетворення змінюють дані, представлені в явній формі, так, що вони стають нерозпізнаваними (з певною мірою надійності) неавторизованими людьми. Шифрування, тобто перетворення секретної інформації, є особливо ефективним засобом проти несанкціонованого доступу до повідомлень, які передаються по лініях зв'язку і неавторизованих доступів до даних, що зберігаються у віддалених файлах. Навіть просте перетворення секретної інформації є ефективним засобом, що дає можливість приховати її значення від більшості користувачів.

У загальній формі в криптографічній системі початкове повідомлення М і ключ К є входами в деякий перетворюючий пристрій. Процес відновлення повідомлення при невідомому ключі називається дещифруванням.

Статистичні властивості відкритого тексту (ВТ) та шифрованого тексту (ШТ) досліджуються в криптології. Криптологія – наука, яка займається методами шифрування і дешифрування. Криптологія складається з двох частин – криптографії і криптоаналізу. Криптографія займається розробкою методів шифрування інформації, а криптоаналіз займається оцінкою сильних і слабких властивостей методів шифрування і розробкою методів, на основі яких будуються розкриття криптосистем.

*2.2. Шифрування підстановкою*

2.2.1. Прямі підстановки

У прямих підстановках кожний знак початкового тексту замінюється одним або декількома знаками. Одним з важливих підкласів прямих підстановок є моноалфавітні підстановки, в яких встановлюється взаємно однозначна відповідність між кожним знаком аі алфавіту повідомлень А і відповідним знаком hj зашифрованого тексту.

Дуже простим прикладом перетворення секретної інформації є шифр Цезара, який, за переказами, був використаний ще Юлієм Цезарем . Рядок знаків YGBPCGFBOQTGBUPQYBHQTBDCVVGTBUMKKPI є зашифрованою формою наступного повідомлення: WE NEED MORE SNOW FOR BETTER SKIING (Для кращого катання на лижах треба більше снігу).

*Шифр Цезара* фактично являє собою окремий випадок методу моноалфавітної підстановки букв одного алфавіту. Кожний знак Р з початкового алфавіту замінюється відповідним числом Р(Р), [р(А)=1, р(В)==2,. ... р(Z)=26, пропуск = 0]. Потім формується еквівалентне зашифроване число у з рівняння

y(^)=p(Р) +2 (mod 27) (1)

Таким чином, у(Т)=р(Т)+2=20+2=22, у(1)=р(1)+2=9+2=11 і т. д.

Значення у потім заміняються відповідними їм буквами для отримання зашифрованого тексту.

Всі методи моноалфавітної підстановки можна представити як числові перетворення букв початкового тексту, що розглядаються як числа. Кожна буква в тексті множиться на деяке число (назване десятковим коефіцієнтом) і додається до деякого іншого числа (коефіцієнту зсуву)

с=(aP+s) mod K (2)

де: а - десятковий коефіцієнт; s - коефіцієнт зсуву. Результуюче число зменшується за правилом віднімання модуля K, де K - розмір алфавіту, і зашифрований текст формується із відповідних йому алфавітних еквівалентів. Неважко пересвідчитися, що рівняння (1) для шифру Цезара є фактично рівнянням (2) з а =1, s=2, і K=27.

2.2.2. Багатоалфавітні підстановки

Проста багатоалфавітна підстановка послідовно і циклічно міняє алфавіти, що використовуються. Ефект використання багатоалфавітної підстановки полягає в тому, що забезпечується маскування природної частотної статистики початкової мови L, оскільки конкретний знак з алфавіту А може бути перетворений в декілька різних знаків шифрувального алфавіту В. Рівень захисту, що забезпечується теоретично, пропорційний довжині періоду в послідовності алфавітів, що використовуються.

Багатоалфавітні (або поліалфавітні) шифри використовуються для підвищення стійкості шифру. Суть поліалфавітного шифру полягає в циклічному використанні декількох моноалфавітних шифрів.

*Шифр Віженера* - [поліалфавітний шифр](http://uk.wikipedia.org/wiki/%D0%9F%D0%BE%D0%BB%D1%96%D0%B0%D0%BB%D1%84%D0%B0%D0%B2%D1%96%D1%82%D0%BD%D0%B8%D0%B9_%D1%88%D0%B8%D1%84%D1%80), який у якості [ключа](http://uk.wikipedia.org/wiki/%D0%9A%D0%BB%D1%8E%D1%87) використовує слово. Якщо пронумерувати літери алфавіту від 0 до 32 (а → 0, б → 1, в → 2, ...), то шифрування і розшифрування Віженера можна представити формулами:

Ci = (Pi + Kj) mod 33,

Pi = (Ci - Kj + 33) mod 33, де

Ci - літера шифрованого тексту;

Kj - j-та літера [ключового](http://uk.wikipedia.org/wiki/%D0%9A%D0%BB%D1%8E%D1%87) слова;

Pi – літера відкритого тексту.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 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 |
|  |  | . | , | ; | - | ‘ | 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 | 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 | 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 | 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 | 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 | 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 |  | . | , | ; | - |

Таблиця Віженера

Ключове слово повторюється поки не отримано [гаму](http://uk.wikipedia.org/w/index.php?title=%D0%93%D0%B0%D0%BC%D0%B0%28%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%8F%29&action=edit&redlink=1), рівну довжині повідомлення

Для шифрування і розшифрування може використовуватися таблиця алфавітів, яка називається Tabula Recta або квадрат Віженера.

В цьому випадку використовується латинський алфавіт (26 символів) і 6 розділових знаки. Якщо використовується латинський алфавіт (без розділових знаків), в якому використовується 26 символів, формат таблиці Віженера буде 26х26.

2.2.3. Шифр підстановки

Шифр простої заміни, шифр простої підстановки, моноалфавітний шифр - клас методів шифрування, які зводиться до створення за певним алгоритмом таблиці шифрування, в якій для кожної букви відкритого тексту існує єдина зіставлена ​​їй буква шифр-тексту. Само шифрування полягає в заміні букв згідно з таблицею. Для розшифрування досить мати ту ж таблицю, або знати [алгоритм](http://znaimo.com.ua/%D0%90%D0%BB%D0%B3%D0%BE%D1%80%D0%B8%D1%82%D0%BC), за якою вона генерується.

# **Завдання**

*Варіант 8*

1. Ознайомитись з методами шифрування.

2. Написати програму для статистичного аналізу тексту. Статистичний аналіз повинен дати такі параметри аналізованого тексту:

- визначити використаний алфавіт;

- частоти повторень одного символу для всіх символів тексту, які представити двома способами – в алфавітному порядку і по спаданню частоти повторення у вигляді гістограм;

- частоти повторень для біграм (двох символів, які зустрічаються в тексті в кількості 10-15), які представити у вигляді гістограм;

- частоти повторень для триграм (трьох символів, які зустрічаються в тексті в кількості 10-15), які представити у вигляді гістограм;

- знайти повторення символів в тексті для 2, 3 і 4символів.

Отримати відкритий текст і виконати статистичний аналіз. Зробити висновки на основі отриманих статистичних характеристик відкритого тексту.

3. Отримати зашифрований текст з допомогою шифра Цезара. Виконати для цього ШТ статистичний аналіз і на основі отриманих результатів і висновків, які отримані в п.2 знайти ключ, прочитати і надрукувати ВТ і отриманий ключ шифрування. Зробити висновки які властивості відкритого і шифрованого текстів були використані при розшифруванні ШТ.

4. Отримати зашифрований текст з допомогою шифра прямої підстановки. Виконати для цього ШТ статистичний аналіз і на основі отриманих результатів і висновків, які отримані в п.2 знайти ключ, прочитати і надрукувати ВТ і отриманий ключ шифрування. Зробити висновки які властивості відкритого і шифрованого текстів були використані при розшифруванні ШТ.

5. Відкритий текст, який отриманий в п.3 (при розшифруванні шифра Цезара) зашифрувати з допомогою шифра Віженера (формат 33х33). При зашифруванні використати ключ, який складається з прізвища і імені студента латинськими символами. Виконати статистичний аналіз ШТ Віженера і ВТ і побудувати ці характеристики на одному графіку з одинаковим масштабом по спаданню частоти повторення для одного символа. Зробити висновки за результатами статистичного аналізу ШТ і ВТ.

6. Знайти в кожному тексті (ШТ і ВТ) повторення буквосполучень (2-3-4).

7. Зробити висновки по кожному розділі і по роботі вцілому.

8. Дайте оцінку методам шифрування, які використовані в циклі робіт 1-4.

# Статистичний аналіз

Статистичний аналіз відкритого тексту проводиться для того, щоб знайти та виділити частоти повторень одної літери, біграм та триграм. Це дає нам змогу виявити певні властивості та особливості мови. Виконавши статистичний аналіз шифрованого тексту ми можемо виявити певні закономірності, побачити які насправді слова можуть ховатися під шифрованим текстом. При співставленні отриманих даних після аналізу відкритого та шифрованого текстів робляться певні висновки та висуваються гіпотези щодо правильності розшифрування.

***Текст для статистичного аналізу***

IT INTRODUCED A RADICALLY NEW METHOD OF DISTRIBUTING CRYPTOGRAPHIC KEYS, WHICH WENT FAR TOWARD SOLVING ONE OF THE FUNDAMENTAL PROBLEMS OF CRYPTOGRAPHY, KEY DISTRIBUTI ON, AND HAS BECOME KNOWN AS DIFFIE-HELLMAN KEY EXCHANGE. THE ARTICLE ALSO STIMULATED THE ALMOST IMMEDIATE PUBLIC DEVELOPMENT OF A NEW CLASS OF ENCIPHERING ALGORITHMS, THE ASYMMETRIC KEY ALGORITHMS. PRIOR TO THAT TIME, ALL USEFUL MODERN ENCRYPTION ALGORITHMS HAD BEEN SYMMETRIC KEY ALGORITHMS, IN WHICH THE SAME CRYPTOGRAPHIC KEY IS USED WITH THE UNDERLYING ALGORITHM BY BOTH THE SENDER AND THE RECIPIENT, WHO MUST BOTH KEEP IT SECRET. ALL OF THE ELECTROMECHANICAL MACHINES USED IN WWII WERE OF THIS LOGICAL CLASS, AS WERE THE CAESAR AND ATBASH CIPHERS AND ESSENTIALLY ALL CIPHER SYSTEMS THROUGHOUT HISTORY. THE 'KEY' FOR A CODE IS, OF COURSE, THE CODEBOOK, WHICH MUST LIKEWISE BE DISTRIBUTED AND KEPT SECRET, AND SO SHARES MOST OF THE SAME PROBLEMS IN PRACTICE. OF NECESSITY, THE KEY IN EVERY SUCH SYSTEM HAD TO BE EXCHANGED BETWEEN THE COMMUNICATING PARTIES IN SOME SECURE WAY PRIOR TO ANY USE OF THE SYSTEM THE TERM USUALLY USED IS 'VIA A SECURE CHANNEL' SUCH AS A TRUSTWORTHY COURIER WITH A BRIEFCASE HANDCUFFED TO A WRIST, OR FACE-TO-FACE CONTACT, OR A LOYAL CARRIER PIGEON. THIS REQUIREMENT IS NEVER TRIVIAL AND VERY RAPIDLY BECOMES UNMANAGEABLE AS THE NUMBER OF PARTICIPANTS INCREASES, OR WHEN SECURE CHANNELS AREN'T AVAILABLE FOR KEY EXCHANGE, OR WHEN, AS IS SENSIBLE CRYPTOGRAPHIC PRACTICE, KEYS ARE FREQUENTLY CHANGED.THE AGING DES WAS OFFICIALLY REPLACED BY THE ADVANCED ENCRYPTION STANDARD AES IN - WHEN NIST ANNOUNCED FIPS. AFTER AN OPEN COMPETITION, NIST SELECTED RIJNDAEL, SUBMITTED BY TWO BELGIAN CRYPTOGRAPHERS, TO BE THE AES. DES, AND MORE SECURE VARIANTS OF IT SUCH AS TRIPLE DES, ARE STILL USED TODAY, HAVING BEEN INCORPORATED INTO MANY NATIONAL AND ORGANIZATIONAL STANDARDS. HOWEVER, ITS X-BIT KEY-SIZE HAS BEEN SHOWN TO BE INSUFFICIENT TO GUARD AGAINST BRUTE FORCE ATTACKS ONE SUCH ATTACK, UNDERTAKEN BY THE CYBER CIVIL-RIGHTS GROUP ELECTRONIC FRONTIER FOUNDATION IN-, SUCCEEDED IN- HOURS. AS A RESULT, USE OF STRAIGHT DES ENCRYPTION IS NOW WITHOUT DOUBT INSECURE FOR USE IN NEW CRYPTOSYSTEM DESIGNS, AND MESSAGES PROTECTED BY OLDER CRYPTOSYSTEMS USING DES, AND INDEED ALL MESSAGES SENT SINCE USING DES, ARE ALSO AT RISK. REGARDLESS OF DES' INHERENT QUALITY, THE DES KEY SIZE WAS THOUGHT TO BE TOO SMALL BY SOME EVEN IN-, PERHAPS MOST PUBLICLY BY WHITFIELD DIFFIE. THERE WAS SUSPICION THAT GOVERNMENT ORGANIZATIONS EVEN THEN HAD SUFFICIENT COMPUTING POWER TO BREAK DES MESSAGES; CLEARLY OTHERS HAVE ACHIEVED THIS CAPABILITY.THE SECOND DEVELOPMENT, IN-, WAS PERHAPS EVEN MORE IMPORTANT, FOR IT FUNDAMENTALLY CHANGED THE WAY CRYPTOSYSTEMS MIGHT WORK. THIS WAS THE PUBLICATION OF THE PAPER NEW DIRECTIONS IN CRYPTOGRAPHY BY WHITFIELD DIFFIE AND MARTIN HELLMAN. IT INTRODUCED A RADICALLY NEW METHOD OF DISTRIBUTING CRYPTOGRAPHIC KEYS, WHICH WENT FAR TOWARD SOLVING ONE OF THE FUNDAMENTAL PROBLEMS OF CRYPTOGRAPHY, KEY DISTRIBUTION, AND HAS BECOME KNOWN AS DIFFIE-HELLMAN KEY EXCHANGE. HE MID-S SAW TWO MAJOR PUBLIC ADVANCES. FIRST WAS THE PUBLICATION OF THE DRAFT DATA ENCRYPTION STANDARD IN THE U.S. FEDERAL REGISTER ON MARCH. THE PROPOSED DES CIPHER WAS SUBMITTED BY A RESEARCH GROUP AT IBM, AT THE INVITATION OF THE NATIONAL BUREAU OF STANDARDS NOW NIST, IN AN EFFORT TO DEVELOP SECURE ELECTRONIC COMMUNICATION FACILITIES FOR BUSINESSES SUCH AS BANKS AND OTHER LARGE FINANCIAL ORGANIZATIONS. AFTER 'ADVICE' AND MODIFICATION BY NSA, ACTING BEHIND THE SCENES, IT WAS ADOPTED AND PUBLISHED AS A FEDERAL INFORMATION PROCESSING STANDARD PUBLICATION IN-. DES WAS THE FIRST PUBLICLY ACCESSIBLE CIPHER TO BE 'BLESSED' BY A NATIONAL AGENCY SUCH AS NSA. THE RELEASE OF ITS SPECIFICATION BY NBS STIMULATED AN EXPLOSION OF PUBLIC AND ACADEMIC INTEREST IN CRYPTOGRAPHY. THE AGING DES WAS OFFICIALLY REPLACED BY THE ADVANCED ENCRYPTION STANDARD AES IN- WHEN NIST ANNOUNCED FIPS-. AFTER AN OPEN COMPETITION, NIST SELECTED RIJNDAEL, SUBMITTED BY TWO BELGIAN CRYPTOGRAPHERS, TO BE THE AES. DES, AND MORE SECURE VARIANTS OF IT, ARE STILL USED TODAY, HAVING BEEN INCORPORATED INTO MANY NATIONAL AND ORGANIZATIONAL STANDARDS. HOWEVER, ITS X-BIT KEY-SIZE HAS BEEN SHOWN TO BE INSUFFICIENT TO GUARD AGAINST BRUTE FORCE ATTACKS ONE SUCH ATTACK, UNDERTAKEN BY THE CYBER CIVIL-RIGHTS GROUP ELECTRONIC FRONTIER FOUNDATION IN-, SUCCEEDED IN- HOURS. AS A RESULT, USE OF STRAIGHT DES ENCRYPTION IS NOW WITHOUT DOUBT INSECURE FOR USE IN NEW CRYPTOSYSTEM DESIGNS, AND MESSAGES PROTECTED BY OLDER CRYPTOSYSTEMS USING DES, AND INDEED ALL MESSAGES SENT SINCE USING DES, ARE ALSO AT RISK. REGARDLESS OF DES' INHERENT

Проведемо аналіз англомовного відкритого тексту для того, щоб дослідити особливості англійської мови. Проведемо цей аналіз за допомогою розробленої програми.

***Алфавіт тексту:***

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 \_ . , ; - '

У відкритому тексті було використано всі літери англійського алфавіту (26 літер) та 6 розділових знаків ( \_ . , ; - ' ).

***Аналіз англомовного відкритого тексту***

Під час аналізу були отримані наступні графіки (Рис.4.1.1 – Рис.4.1.6).

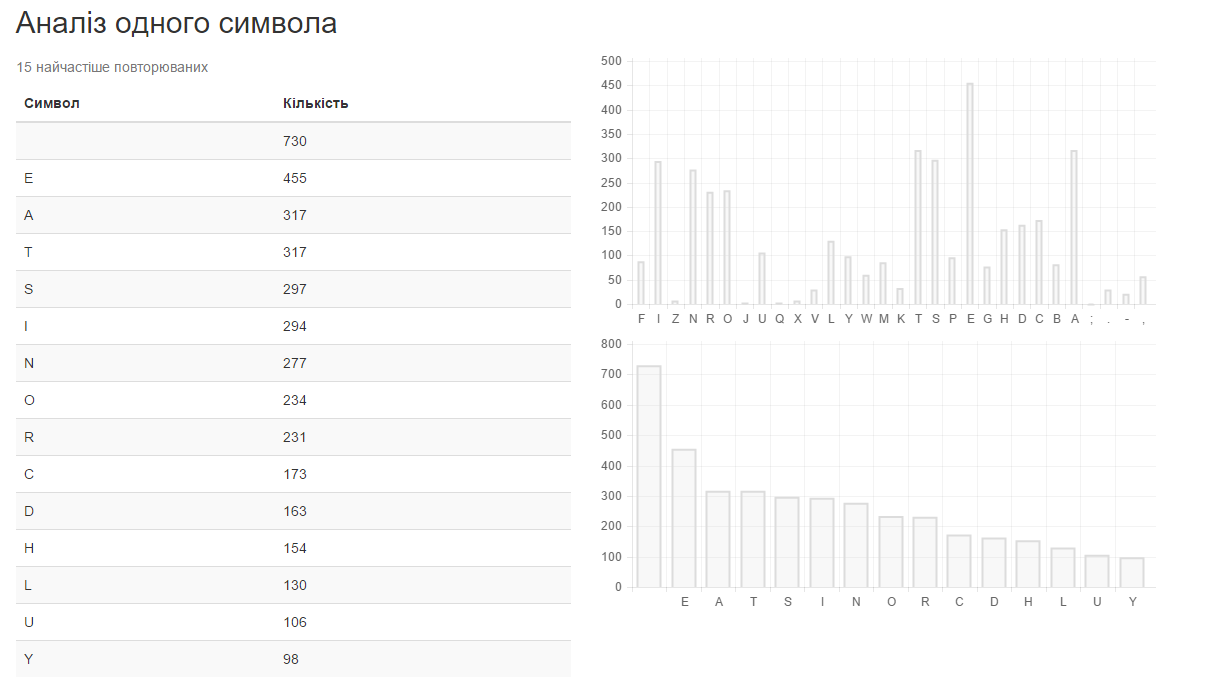


Рис. 1 Аналіз одного символу

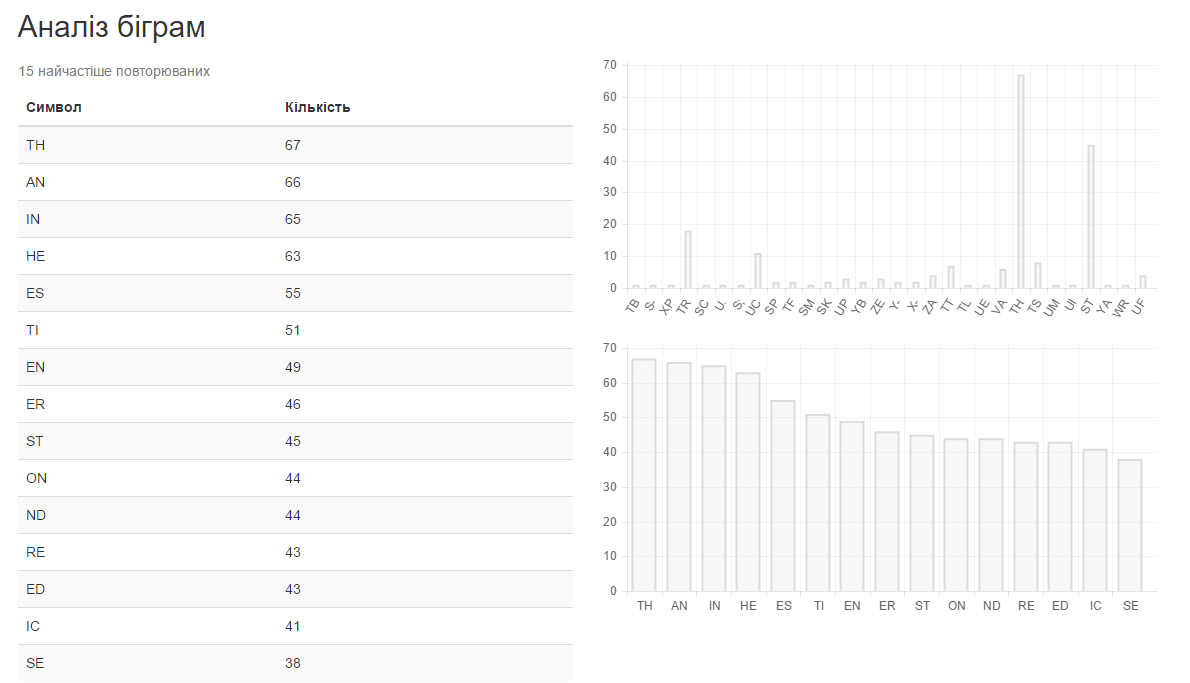


Рис. 2. Аналіз біграм

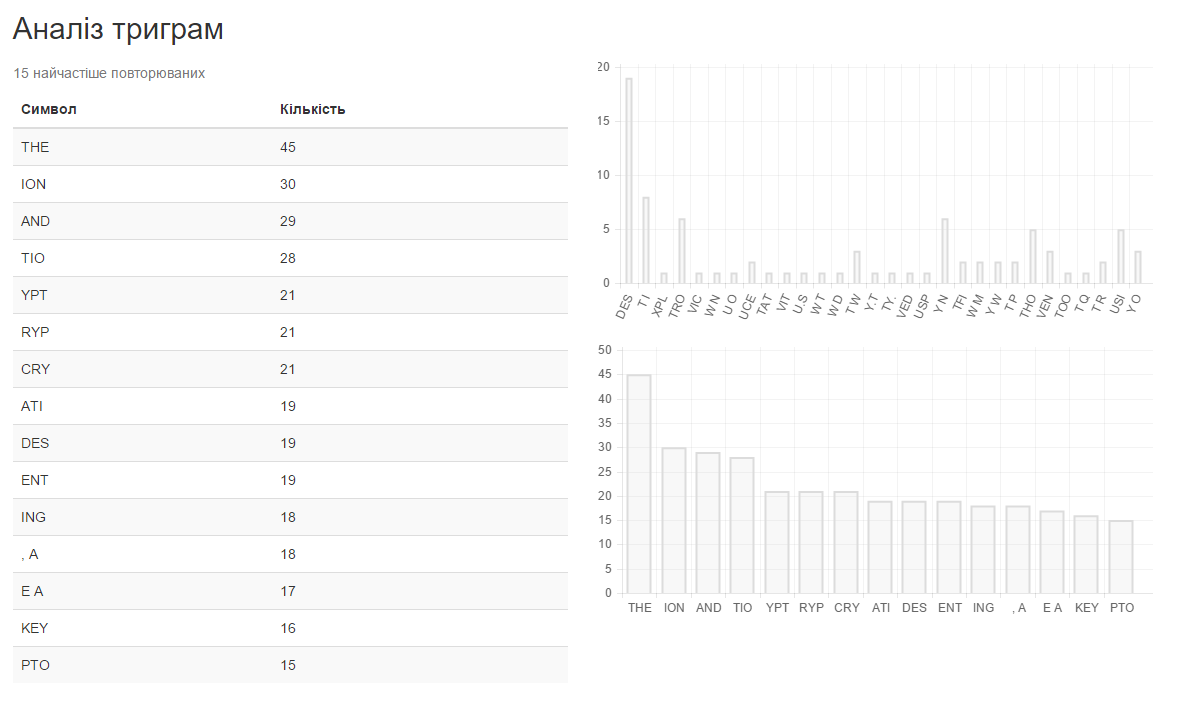


Рис. 3. Аналіз триграм

### Код програми для статистичного аналізу на мові JavaScript

Лістнг analysis-model.js

var EventEmitter = require('events').EventEmitter;

var assign = require('object-assign');

var CHANGE\_EVENT = 'change';

function calculateStats(t){

var onegram = {};

var bigram = {};

var trigram = {};

var fourgram = {};

for(var i = 0; i < t.length; i++){

var char = t.charAt(i);

onegram[char] = (onegram[char] || 0) + 1;

if (i < t.length - 1){

var char2 = char + t.charAt(i+1);

if (char2.trim().length == 2){

bigram[char2] = (bigram[char2] || 0) + 1;

}

if (i < t.length - 2){

var char3 = char2 + t.charAt(i+2);

if (char3.trim().length == 3){

trigram[char3] = (trigram[char3] || 0) + 1;

}

if (i < t.length - 3){

var char4 = char3 + t.charAt(i+3);

if (char4.trim().length == 4){

fourgram[char4] = (fourgram[char4] || 0) + 1;

}

}

}

}

}

var rows = function(hash){

return Object.keys(hash).map(function (key) {

return { name: key, val: hash[key] };

});

};

return {

onegram: rows(onegram),

bigram: rows(bigram),

trigram: rows(trigram),

fourgram: rows(fourgram)

};

}

var \_text = 'YGBPGGFBOQTGBUPQYBHQTBDGVVGTBUMKKPI';

var AnalysisModel = assign({}, EventEmitter.prototype, {

pushTextChanges: function(t){

\_text = t;

this.emitChange();

},

getState: function(){

return assign({

text: \_text

}, calculateStats(\_text));

},

emitChange: function() {

this.emit(CHANGE\_EVENT);

},

addChangeListener: function(callback) {

this.on(CHANGE\_EVENT, callback);

},

removeChangeListener: function(callback) {

this.removeListener(CHANGE\_EVENT, callback);

}

});

if (typeof exports == 'undefined') {

exports = {};

}

exports.calculateStats = calculateStats;

exports.AnalysisModel = AnalysisModel;

Лістінг analysis.js

var React = require('react');

var AnalysisModel = require('../models/analysis-model').AnalysisModel;

var Stats = require('./stats').Stats;

var Analysis = React.createClass({

getInitialState: function() {

return AnalysisModel.getState();

},

reloadState: function(){

this.setState(AnalysisModel.getState());

},

componentDidMount: function() {

AnalysisModel.addChangeListener(this.reloadState);

},

componentWillUnmount: function() {

AnalysisModel.removeChangeListener(this.reloadState);

},

render: function() {

return <form>

<div className='form-group'>

<label htmlFor='inputText'>Текст</label>

<textarea id='inputText'

className='form-control'

rows='10'

value={this.state.text}

onChange={this.\_handleTextChange}></textarea>

</div>

<h2>Аналіз одного символа</h2>

<Stats data={this.state.onegram} />

<h2>Аналіз біграм</h2>

<Stats data={this.state.bigram} />

<h2>Аналіз триграм</h2>

<Stats data={this.state.trigram} />

<h2>Аналіз чотирьох символів</h2>

<Stats data={this.state.fourgram} />

</form>;

},

\_handleTextChange: function(event) {

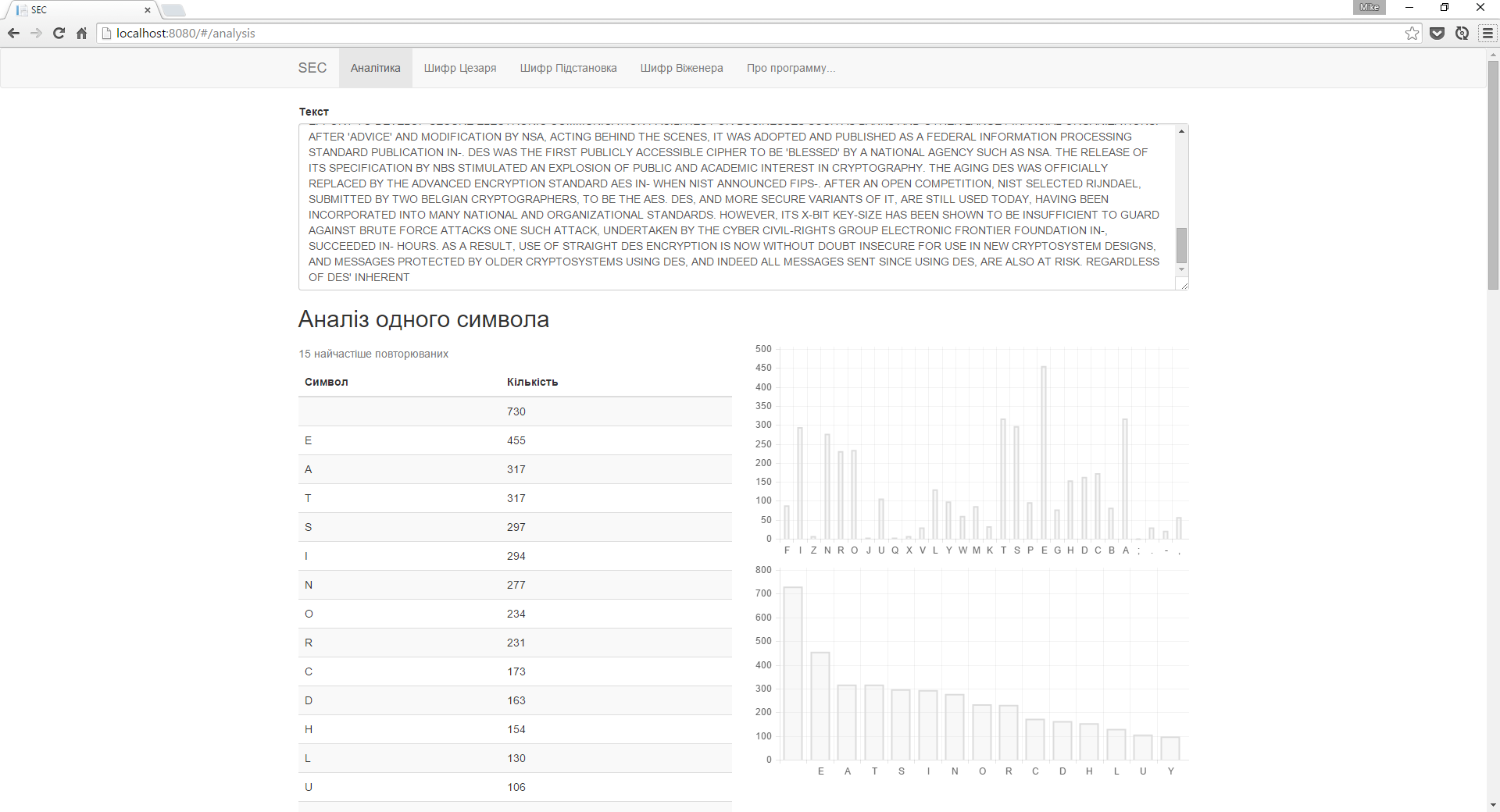
AnalysisModel.pushTextChanges(event.target.value);

}

});

exports.Analysis = Analysis;

## Результат



## Висновок

Виконавши статистичний аналіз ми визначили особливості англомовного тексту на тематику шифрування та дізнались про наступні особливості:

* Найчастіше зустрічається символ пробілу ( \_ , 730 разів), що зрозуміло, адже пробіл – розділяє слова одне від одного.
* Друга найчастіше повторювана літера – Е (455 раз), яка є частиною найчастіше повторюваних біграм Е\_, НЕ, ES та триграм THE, \_ED, \_DE.
* Треті найчастіше повторювані літери – А та Т. Літера А вживається мові на початку слова ( \_А), AN , AS та AND. Літера Т – на початку та вкінці слова, є частиною THE, TIO.
* Біграми зустрічаються досить часто: TH, AN, IN, HE, ES, ED, OF.
* Найчастіше повторювані триграми: TH\_, THE, AND, ION.

# Шифр Цезаря

*Шифр Цезара* являє собою окремий випадок методу моноалфавітної підстановки букв одного алфавіту. Для вдалого розшифрування потрібно спочатку провести статистичний аналіз отриманого зашифрованого тексту. На основі отриманих даних статистичного аналізу ШТ та ВТ, отриманого у пункті 4.1, можемо висунути певні гіпотези і знайти ключ зсуву алфавіту. Таким чином розшифрувавши текст.

***Шифрований текст***

WBJ;EK,;QYHOFJE,HWF;OQ;WIQWQBED,QWDZQYECFB NQ;-IJEHOSQ-JQMWIDVJQKDJ-BQJ; QY DJKHOQJ;WJQ-JQZ L BEF ZQWDOJ;-D,QCEH QJ;WDQWZQ;EYQWFFHEWY; IQJEQ -J; HQ DYHOFJ-EDQEHQYHOFJWDWBOI-IQJ; QIY- DY QE.Q.-DZ-D,QM WAD II IQ-DQYHOFJEQIOIJ CIRQ NWCFB IQE.QJ; QBWJJ HQ-DYBKZ QY;WHB IQXWXXW, VIQYH-C WDQMWHQ HWQMEHAQEDQCWJ; CWJ-YWBQYHOFJWDWBOI-IQE.QFEBOWBF;WX J-YQY-F; HISQH Z L BEF ZQWDZQFKXB-I; ZQIEC M;WJQBWJ HQXOQJ; QFHKII-WDQ.H- ZH-Y;QAWI-IA-RQKDZ HIJWDZ-D,QE.QYHOFJE,HWF;OQWJQJ;-IQJ-C QJOF-YWBBOQYEDI-IJ ZQE.Q;WHZUMEDQHKB IQE.QJ;KCXTQI SQ.EHQ NWCFB SQWK,KIJ QA HYA;E..IVYHOFJE,HWF;-YQMH-J-D,IQ-DQJ; QBWJJ HQY DJKHORQ Z,WHQWBBWDQFE QKI ZQIOIJ CWJQ-YQC

***Статистичний аналіз шифрованого тексту***

***Використаний алфавіт у ШТ***

\_' , . ; A B C D E G I J K L M N O P Q R S T U V W X Y Z

У шифрованому тексті було використано 24 літери англійського алфавіту (з 26 літер) та 5 розділових знаків (\_ ' , . ;).

***Аналіз шифрованого тексту***

Для розшифрування тексту зашифрованим шифром Цезаря, в нашому випадку, вистачить тільки аналізу першої гістограми, де наведена статистика повторення одного символу. З Рис.4.2.1 бачимо, що найбільше повторень має символ I. При аналізі ВТ у пункті 4.1 найбільше повторень мав символ пробілу. Тобто можемо припустити, що літера I у ШТ є пробілом у ВТ.

Наше припущення виявилось вірним, ми отримали розшифрований текст.

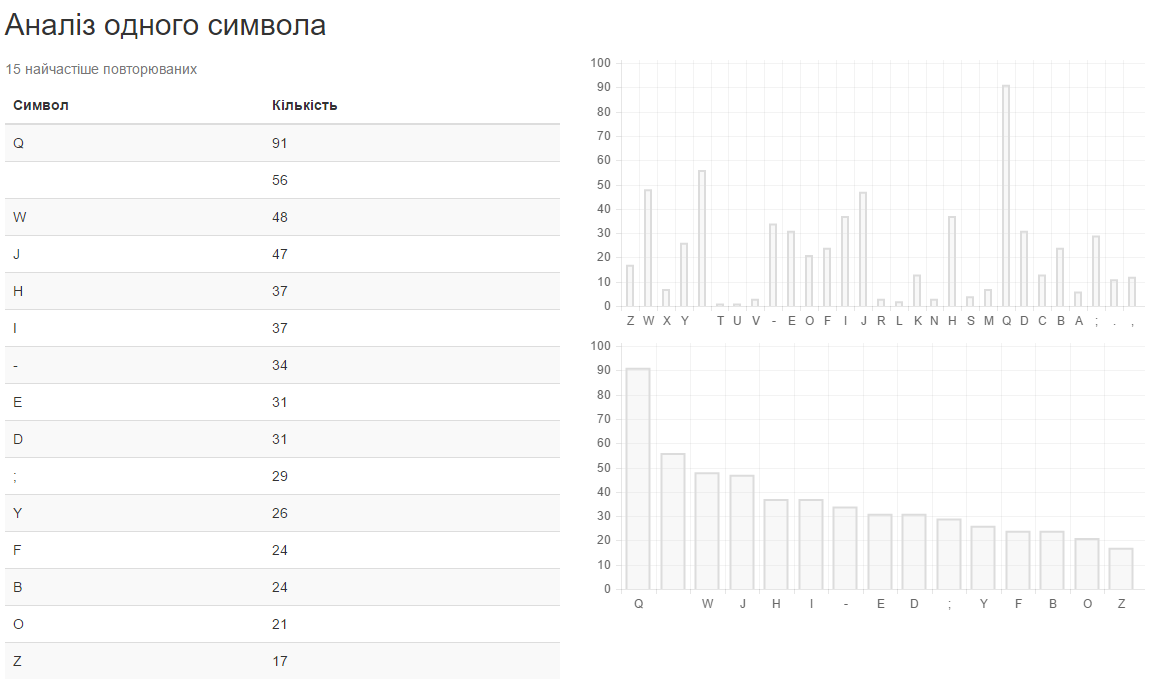


Рис. 4. Аналіз одного символа

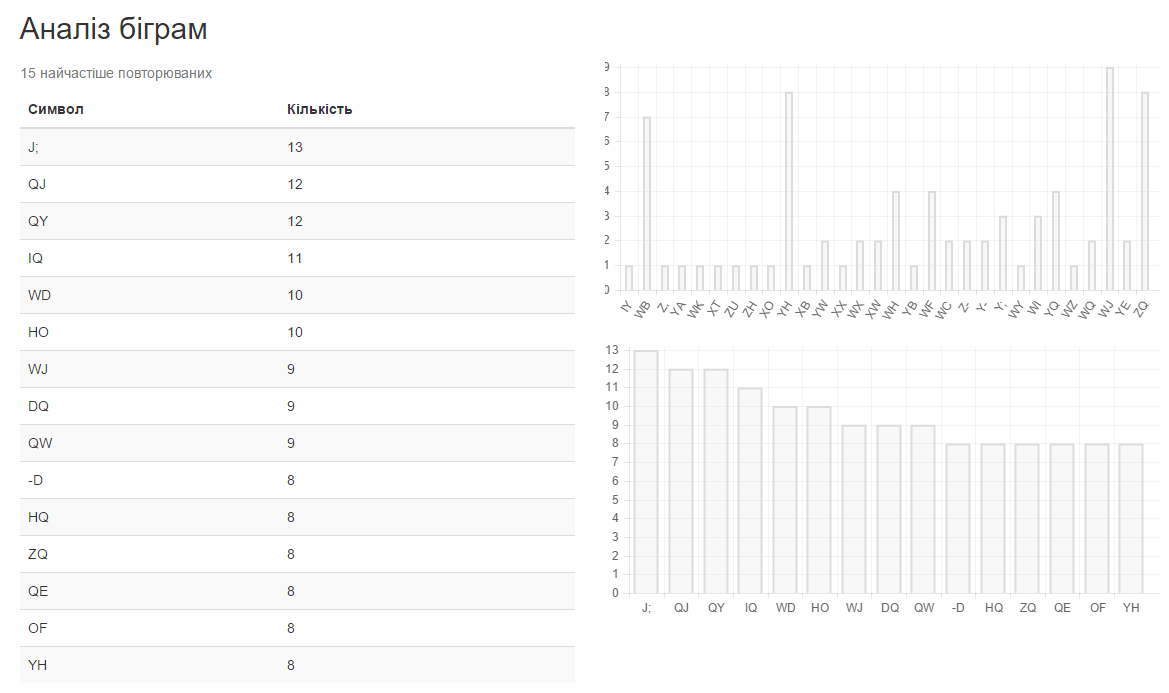


Рис. 5. Аналіз біграм

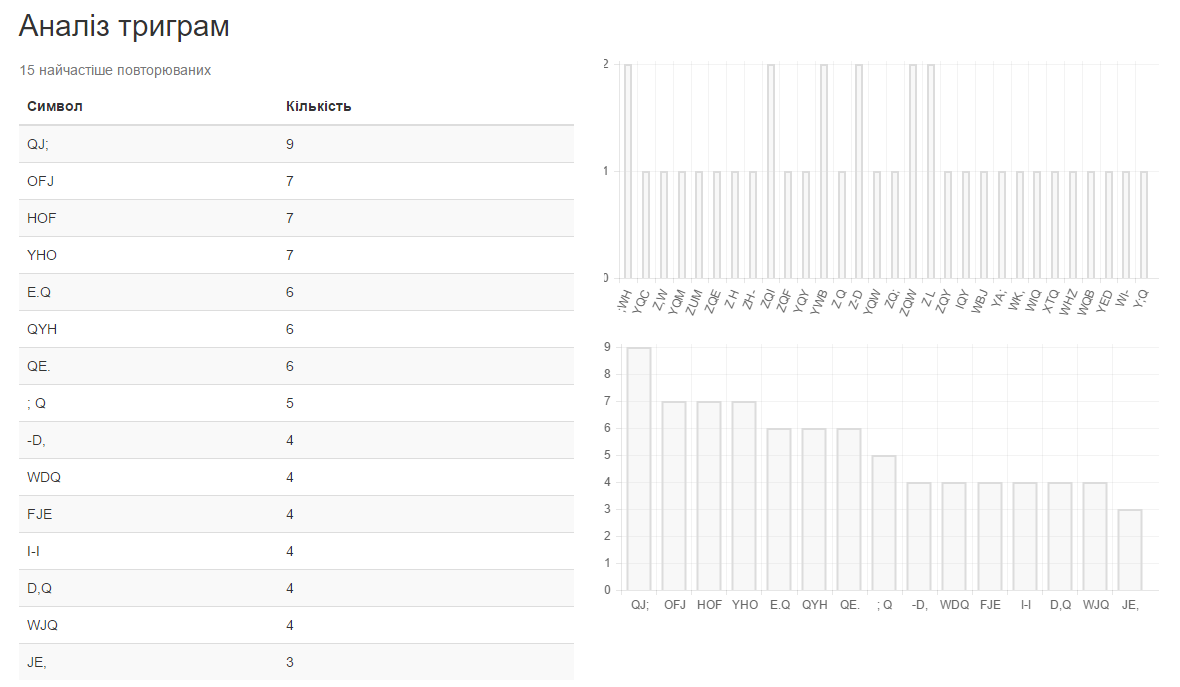


Рис. 6. Аналіз триграм

***Відкритий текст***

AT THE END OF THE WAR, ON APRIL, BRITAIN'S TOP MILITARY OFFICERS WERE TOLD THAT THEY COULD NEVER REVEAL THAT THE GERMAN ENIGMA CIPHER HAD BEEN BROKEN BECAUSE IT WOULD GIVE THE DEFEATED ENEMY THE CHANCE TO SAY THEY WERE NOT WELL AND FAIRLY BEATEN. US NAVY CRYPTOGRAPHERS WITH COOPERATION FROM BRITISH AND DUTCH CRYPTOGRAPHERS AFTER BROKE INTO SEVERAL JAPANESE NAVY CRYPTO SYSTEMS. THE BREAK INTO ONE OF THEM, JN-, FAMOUSLY LED TO THE US VICTORY IN THE BATTLE OF MIDWAY; AND TO THE PUBLICATION OF THAT FACT IN THE CHICAGO TRIBUNE SHORTLY AFTER THE BATTLE, THOUGH THE JAPANESE SEEM NOT TO HAVE NOTICED FOR THEY KEPT USING THE JN- SYSTEM. A US

***Ключ***

Ключ = *14*

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 |  | . | , | ; | - | ‘ |
| 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 |

Таблиця 1. Ключ до ШТ шифром Цезаря

***Використаний алфавіт відкритого тексту***

A B C D E F G H I K L M N O P R S U W Y \_ . , ; - `

У відкритому тексті було використано 20 літер англійського алфавіту (з 26 літер) та 6 розділових знаки (\_ . , ; - ` ).

***Код програми для розшифрування тексту шифром Цезаря на мові JavaScript***

Лістінг caesar-model.js

var ABC = ' ABCDEFGHIJKLMNOPQRSTUVWXYZ';

var decodeTextDictionary = function(text, abc, code){

var decoded = '';

for(var i = 0; i < text.length; i++){

var char = text.charAt(i);

var index = code.indexOf(char);

decoded += abc.charAt(index);

}

return decoded;

}

var decodeText = function(text, decode, abc){

text = text || '';

var size = abc.length;

var shift = 2;

if (decode){

shift = (size - shift) % size;

}

var decoded = '';

for(var i = 0; i < text.length; i++){

var char = text.charAt(i);

var abcCode = abc.indexOf(char);

if (abcCode >= 0){

var decodedCode = (abcCode + shift) % size;

decoded += abc.charAt(decodedCode);

} else {

decoded += char;

}

}

return decoded;

}

exports.ABC = ABC;

exports.decodeTextDictionary = decodeTextDictionary;

exports.decodeText = decodeText;

### Результат

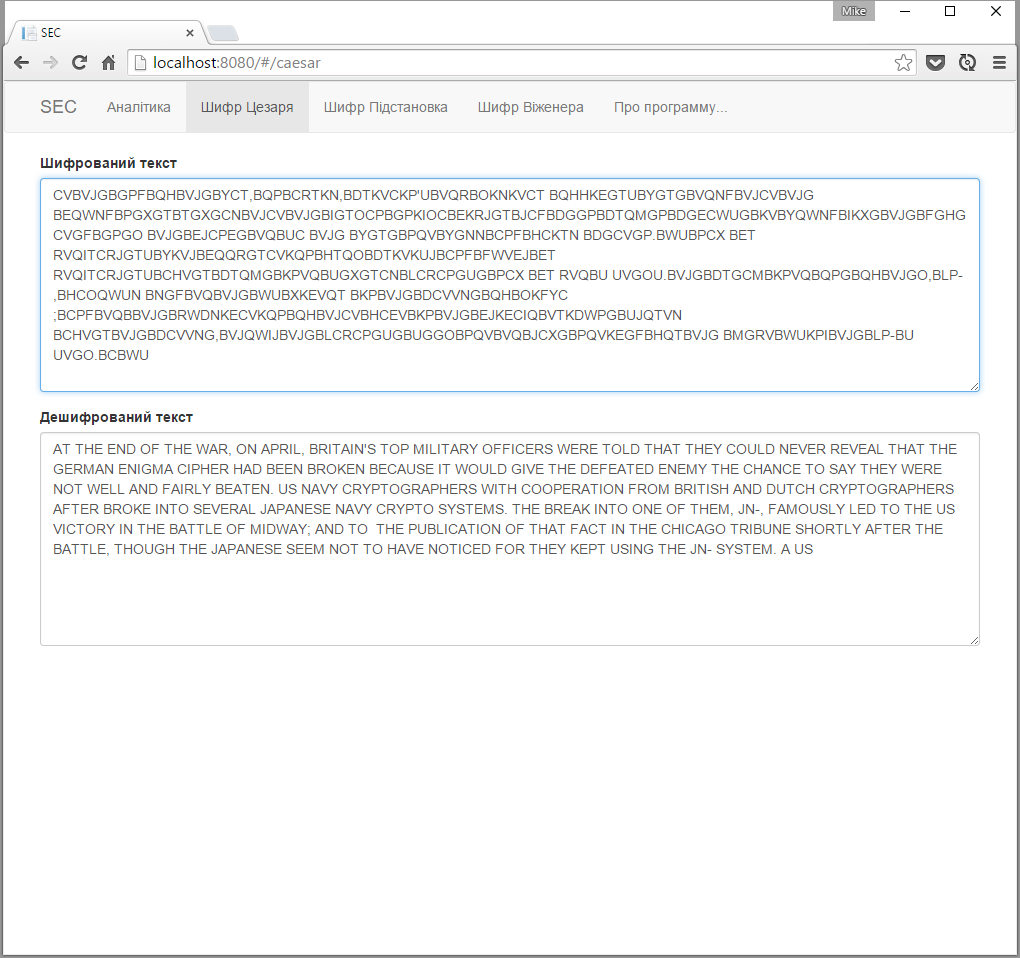


Рис. 7. Вигляд програми швифру Цезаря

### Висновок

У даному розділі ми докладно ознайомились з шифром Цезаря. Зробили статистичний аналіз ШТ, та на основі якого висунули певну гіпотезу, яка виявилось вірною.

# Шифр простої заміни

*Шифр простої заміни* – метод шифрування, який зводиться до створення за певним алгоритмом таблиці шифрування, в якій для кожної букви відкритого тексту існує єдина зіставлена ​​їй буква шифр-тексту. Для кожного ШТ потрібно проводити статистичний аналіз для того, щоб виявити закономірності, які допоможуть вдало розшифрувати текст. Для розшифрування більш складних текстів потрібен досвід.

Зробивши статистичний аналіз ШТ, ми можемо висунути певні гіпотези. Гіпотези ми будемо висувати до того моменту поки не розшифруємо текст. Відштовхуючись від основної гіпотези, розкриваємо наступні літери та намагаємось прочитати англомовні слова серед набору літер ШТ. Таким чином в результати отримуємо ВТ та ключ до нього.

***Шифрований текст***

JY,CE-Z,CAB.MZ-Z.,C-BFKBL,;BAC,C-DJYC;B,MCBYC.C;;J,RBFKB.FDLICSBZLL-FZ.MB,FBJ,;BJDL-FWCDCY,BZYABACWCIFLDCY,TBKF-BZIIB,MZ,BC.FIFEJ.ZIBACDZYA;BZYABMJ;,F-J.BZYAB.PI,P-ZIBDCDF-JZIB-C;C-WZ,JFYUBQMJICB;FIWJYEB.J,RV PJIAJYEB,Z;G;T;LC.JKJCABZLL-FZ.MB.FDLICSJ,RB-CNPJ-C;BACWCIFLDCY,BZYABJDLIJ.Z,JFYBFKB,MCBYCQUBDFCB.FDLICSBDFACI;BFKBL,;BZYABJ,O;B.FDLFYCY,;B Z;CABFYB,MCBP;ZECBFKB.FDLP,C-;BZYABDFAC-YBJYKF-DZ,JFYB,C.MYFIFEJC;TB,M-CCBICWCI;BFKBL,;B.FDLP,C-VZJACABAC;JEYB.FPIAB CBLFJY,CABFP,UBQMJ.MBZ-CBAJKKC-CY,JZ,CAB RBIJ;,BZYAB.MZ-Z.,C-BFKB;FIWJYEB,Z;G;TBJYBFP-BFLJYJFYB;R;,CDBZYABLZ-,J.PIZ-IRBKPY.,JFYZIVIFEJ.ZIBAC;JEYBICWCI;BZ-CB,MCBGCRBKF-BDZJYB

***Статистичний аналіз шифрованого тексту***

***Використаний алфавіт у ШТ***

A B D F G H I K L M N O P Q R S T U V W X Y Z \_ , - . `

У шифрованому тексті було використано 23 літери англійського алфавіту (з 26 літер) та 5 розділових знаків (\_ , - . `). Алфавіт представлений на Рис.4.3.1.

***Аналіз шифрованого тексту***

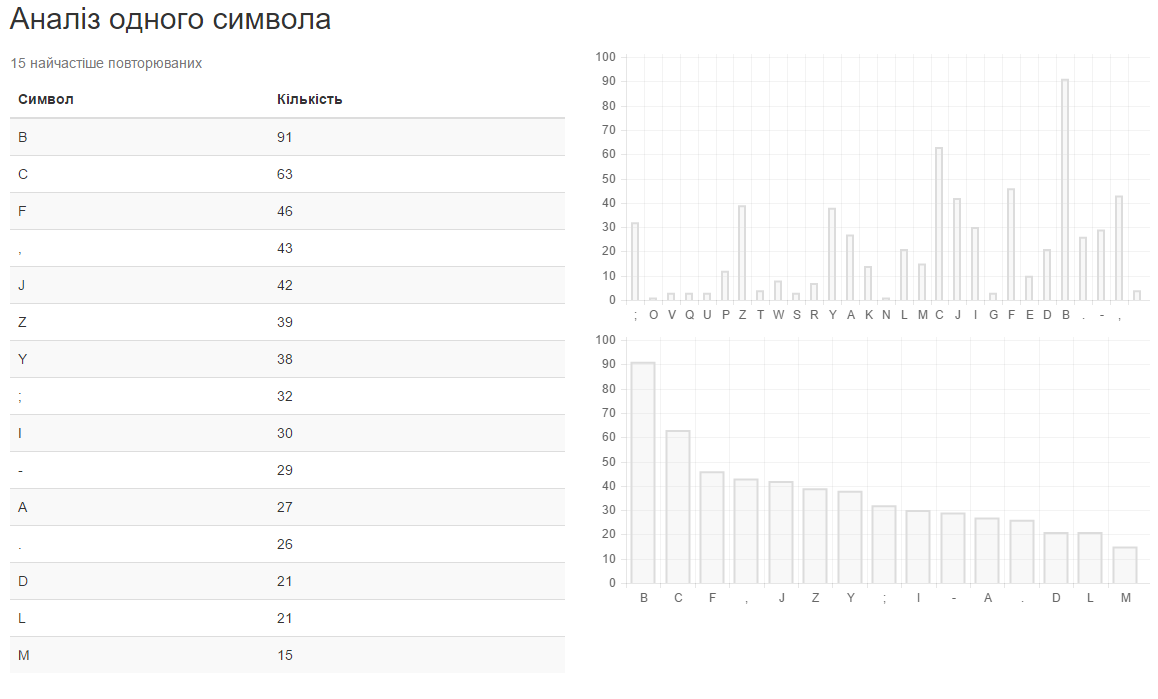


Рис. 8. Аналіз одного символа

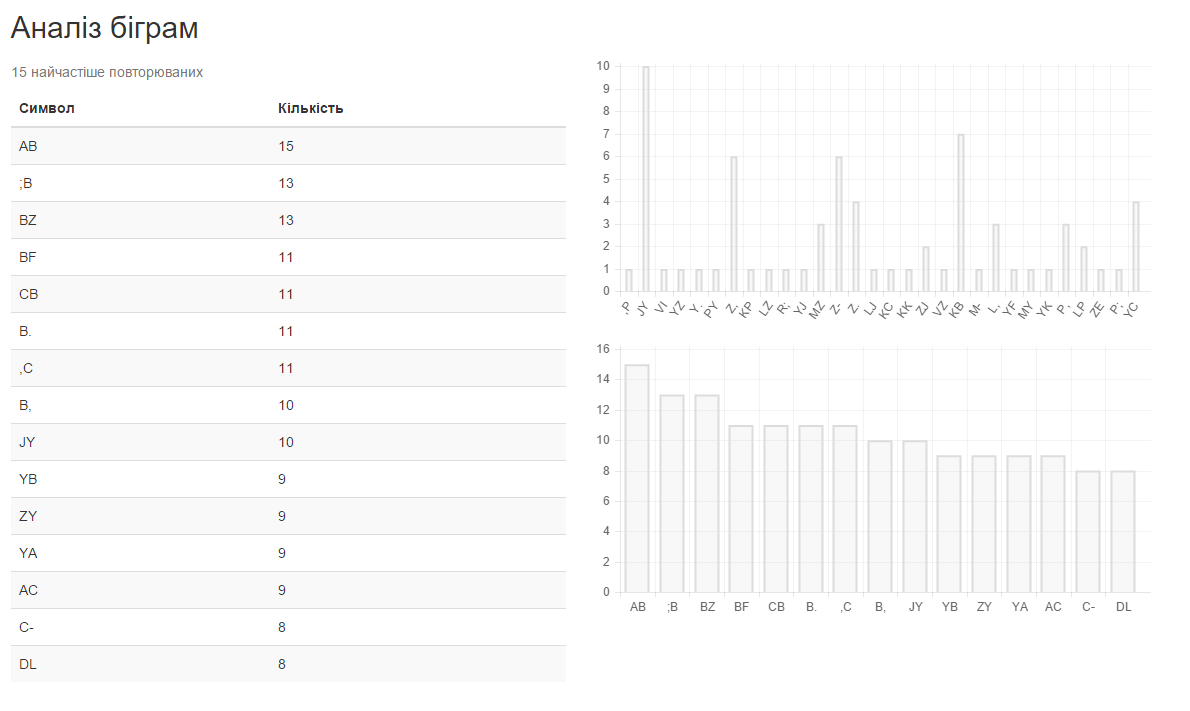


Рис. 9. Аналіз біграм

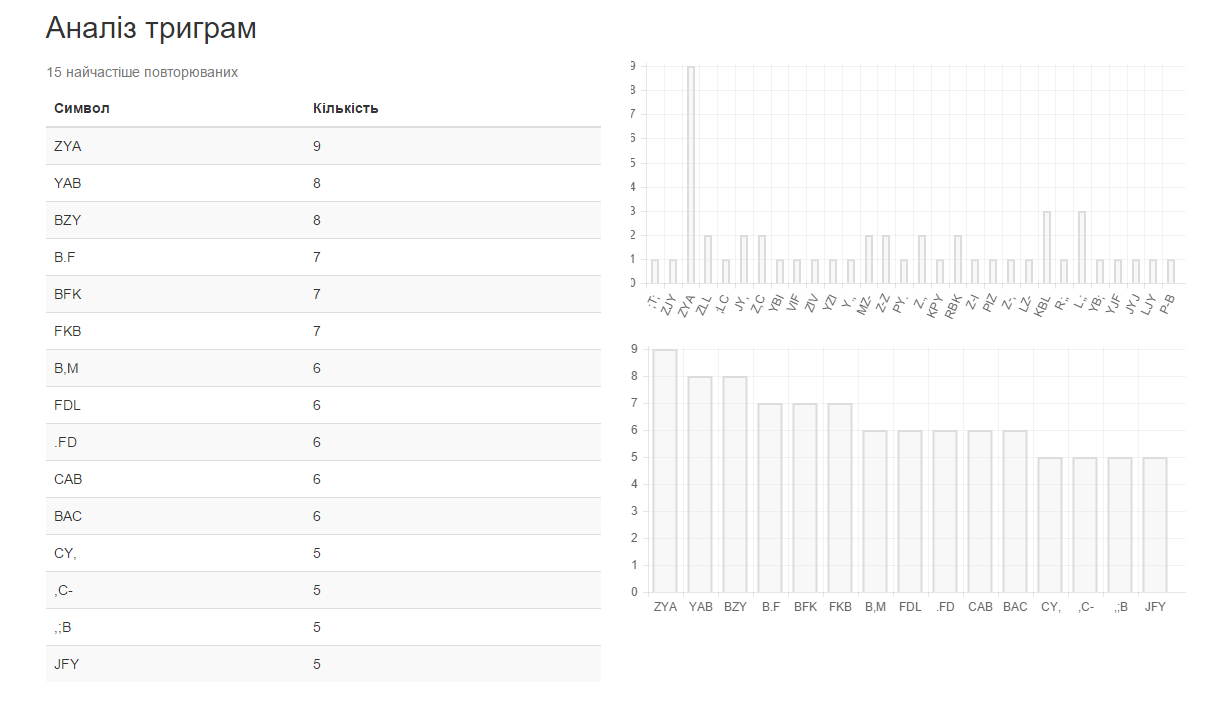


Рис. 10. Аналіз триграм

***Відкритий текст***

DESIGNING, PLANNING AND OPTIMIZATION OF CITY PASSENGER-TRANSPORT SYSTEM REQUIRES THE DEVELOPMENT AND ANALYSIS OF THE COMPLEX MATHEMATICAL MODELS, WHICH TAKE INTO ACCOUNT THE COMPLEX INTERACTION OF ITS COMPONENTS SPECIAL ATTENTION TO PTS MODEL PRESENTATION ON FUNCTIONAL-LOGICAL LEVEL IS CAUSED BY PROVIDING, ON THE ONE HAND, HIGH LEVEL OF ABSTRACTION, AND ON THE OTHER - IT IS ENOUGH CONCRETE FOR DETERMINATION AND DESCRIPTION OF THE BEHAVIOUR OF THE VEHICLES AND PEDESTRIANS IN DYNAMICS DEPENDING ON SITUATION SUCH CONNECTION IS REQUIRED FOR EFFICIENT SOLVING OF THE MANAGEMENT TASKS IN TRANSPORT, PASSENGER AND PEDESTRIAN FLOW, AS WELL

***Ключ***

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 | \_ | . | , | ; | - | ‘ |
| \_ | R |  | D |  | F | B | A | C |  | , | G | - | H | W | L | N | P | O | S | T | V | M | U | E | X | Y | Z | K |  | I | Q |

Таблиця 4.3.1. Ключ до ШТ шифром прямої заміни

Символи C, E, J, ; не розшифрувались, оскільки вони не входять до алфавіту ШТ.

***Використаний алфавіт відкритого тексту***

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

У відкритому тексті було використано 25 літер англійського алфавіту (з 26 літер) та 3 розділових знаки ( \_ , - ).

***Код програми для шифру простої заміни на мові JavaScript***

*Лістінг substitute-model.js*

var ABC = ' ABCDEFGHIJKLMNOPQRSTUVWXYZ';

var CAESAR\_CODE = 'VZHLANQRCWDXFOUSPBTIELGM KY';

var decodeText = function(text, abc, code){

text = text || '';

var decoded = '';

for(var i = 0; i < text.length; i++){

var char = text.charAt(i);

var index = code.indexOf(char);

decoded += abc.charAt(index);

}

return decoded;

};

exports.ABC = ABC;

exports.CAESAR\_CODE = CAESAR\_CODE;

exports.decodeText = decodeText;

### Результат

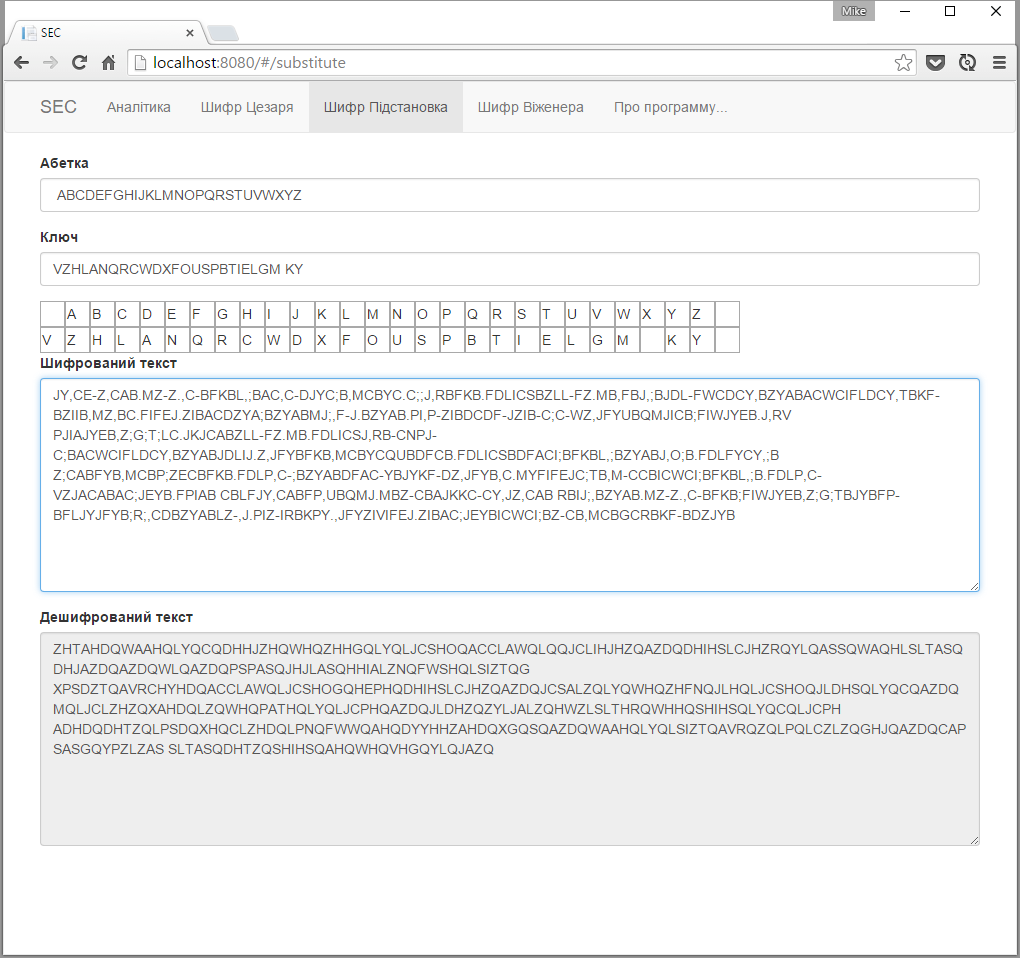


Рис. 11. Вигляд програми шифру простої підстановки

### Висновок

У цьому розділі ми докладно ознайомились з шифром простої заміни. Зробили статистичний аналіз ШТ та висунили 3 гіпотези щодо розшифрування тексту. Одна з гіпотез виявилась хибною, адже, по-перше, замінивши літери, ми не побачили прогрес розшифрування в інших словах, по-друге, використовуючи статистику триграм ми не знайшли жодних потрібних комбінацій символів.

Врешті-решт дві гіпотези виявились вірними і ми змогли розшифрувати текст.

Використовуючи статистичні дані, ми можемо виділити такі особливості даного тексту:

* Найчастіше зустрічається символ пробілу, що зрозуміло, адже пробіл – розділяє слова одне від одного.
* Другим символом, що найчастіше повторюється, є символ A.
* Одним з найчастіше повторюваних слів є триграма ТНЕ.

Для того, щоб розшифрувати ШТ потрібно мати певні базові знання мови та мати опрацьований статистичний матеріал.

# Шифр Віженера

*Шифр Віженера* - [поліалфавітний шифр](http://uk.wikipedia.org/wiki/%D0%9F%D0%BE%D0%BB%D1%96%D0%B0%D0%BB%D1%84%D0%B0%D0%B2%D1%96%D1%82%D0%BD%D0%B8%D0%B9_%D1%88%D0%B8%D1%84%D1%80), який у якості [ключа](http://uk.wikipedia.org/wiki/%D0%9A%D0%BB%D1%8E%D1%87) використовує слово. Ключ дає можливість як зашифрувати, так і розшифрувати текст. Кожна буква ключа визначає свій алфавіт, що зміщений на n позицій відносно нормального алфавіту. Шифрування і розшифрування Віженера можна представити формулами:

Ci = (Pi + Kj) mod 33,

Pi = (Ci - Kj + 33) mod 33, де

Ci - літера шифрованого тексту;

Kj - j-та літера [ключового](http://uk.wikipedia.org/wiki/%D0%9A%D0%BB%D1%8E%D1%87) слова;

Pi – літера відкритого тексту.

***Відкритий текст***

AT THE END OF THE WAR, ON APRIL, BRITAIN'S TOP MILITARY OFFICERS WERE TOLD THAT THEY COULD NEVER REVEAL THAT THE GERMAN ENIGMA CIPHER HAD BEEN BROKEN BECAUSE IT WOULD GIVE THE DEFEATED ENEMY THE CHANCE TO SAY THEY WERE NOT WELL AND FAIRLY BEATEN. US NAVY CRYPTOGRAPHERS WITH COOPERATION FROM BRITISH AND DUTCH CRYPTOGRAPHERS AFTER BROKE INTO SEVERAL JAPANESE NAVY CRYPTO SYSTEMS. THE BREAK INTO ONE OF THEM, JN-, FAMOUSLY LED TO THE US VICTORY IN THE BATTLE OF MIDWAY; AND TO THE PUBLICATION OF THAT FACT IN THE CHICAGO TRIBUNE SHORTLY AFTER THE BATTLE, THOUGH THE JAPANESE SEEM NOT TO HAVE NOTICED FOR THEY KEPT USING THE JN- SYSTEM. A US

***Статистичний аналіз відкритого тексту***

***Використаний алфавіт у ВТ***

' , - . ; A B C D E F G H I J K L M N O P R S T U V W Y

У відкритому тексті було використано 23 літери англійського алфавіту (з 26 літер) та 6 розділових знаків ( \_ . , - ; `). Алфавіт представлений на Рис.4.4.1.

Для шифрування шифром Віженера відкритого тексту використовуємо **ключ CHALYIMYKHAILO**. У результаті отримуємо ШТ.

***Шифрований текст***

YLZHJWNGCWZFULQ DOYSE,BDFZSDCFD,ZQT GCYF'RRH MSLXN GCGQZFURFVDFURJGGXZKCXASSWCKNVXXXRR RDCOPWIGGSQWJQYDZHJSGBI DRVQOE BBWAKWE RRUM DFBZOFPUDWBLZJNZGENDUV LGQXASOYFHNTSF JQXLGTBVSHUTSWSLBFDA RGJUSBZPZ XZHQRFCNSSZTJXODFGRAQISVW XXTMSBXOKGDXRQQYLDB.BLFBCTUPOOOQOHQYECE DIGLTASWBUBQEXQSHULFZUTF BRJHKXDES BFRRWIVGRRCVHSCIIORXXQJOMCLDFBTEQ XZ BELSRTXWECASISDMKXRTBEOXNSBIMAQGZG JGGBK.ZKWQXUQTCBNKCLNRCZBSNUBKVGB,SIE-,ORYENIUCLBAXCRH XLGTBLFBKABKCCVSHBBKVGPU KHXBSNUBDWFLTX;RPZASSCBRGJUSOLQXFV HKFABDYZKWMQSEPEKNKCSSZTL HRCYBBIJHTIZBSRWQIGNNS XHQOSSWGRPCILKW,OEEGTVJRGJUSISDMKXRTBJSGBSMFHLQGZWCMSBCGS RQASECTRGJUQZBTAQSTGKEUBI DRYZ-XKXGVW .BQSTJ

***Статистичний аналіз шифрованого тексту***

***Використаний алфавіт у ШТ***

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 \_ . , ; - '

У відкритому тексті було використано 26 літери англійського алфавіту (з 26 літер) та 6 розділових знаків ( \_ . , ; - ‘ ). Алфавіт представлений на Рис.4.4.4.

***Аналіз шифрованого тексту***

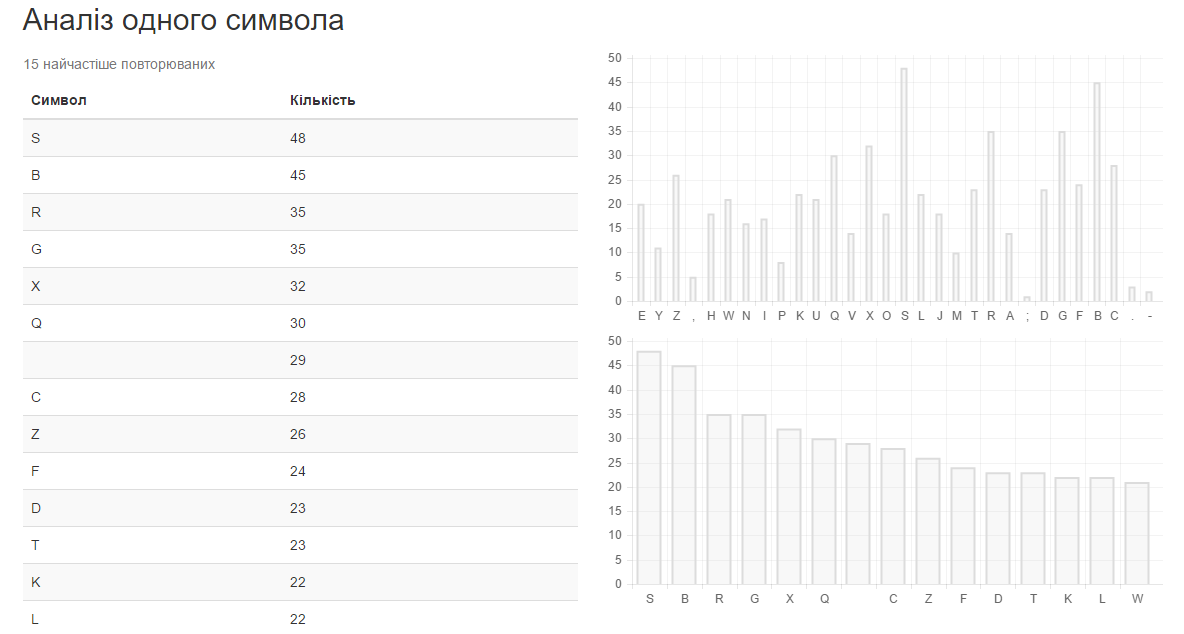


Рис. 12. Аналіз одного символа

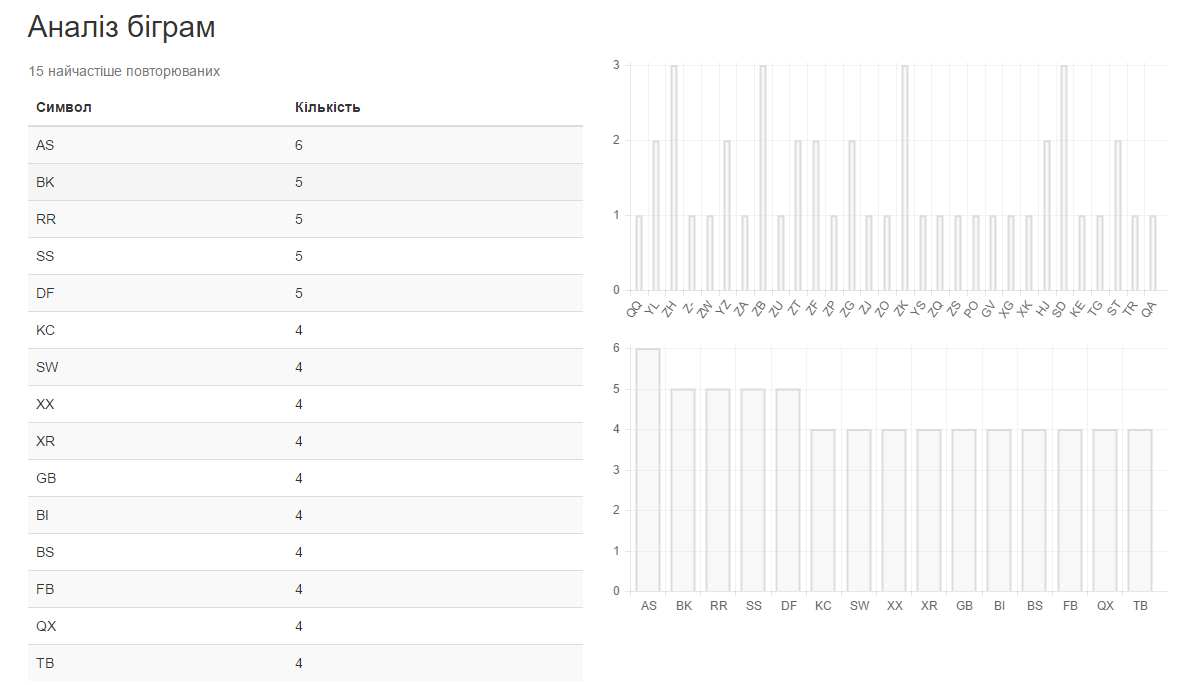


Рис. 13. Аналіз біграм

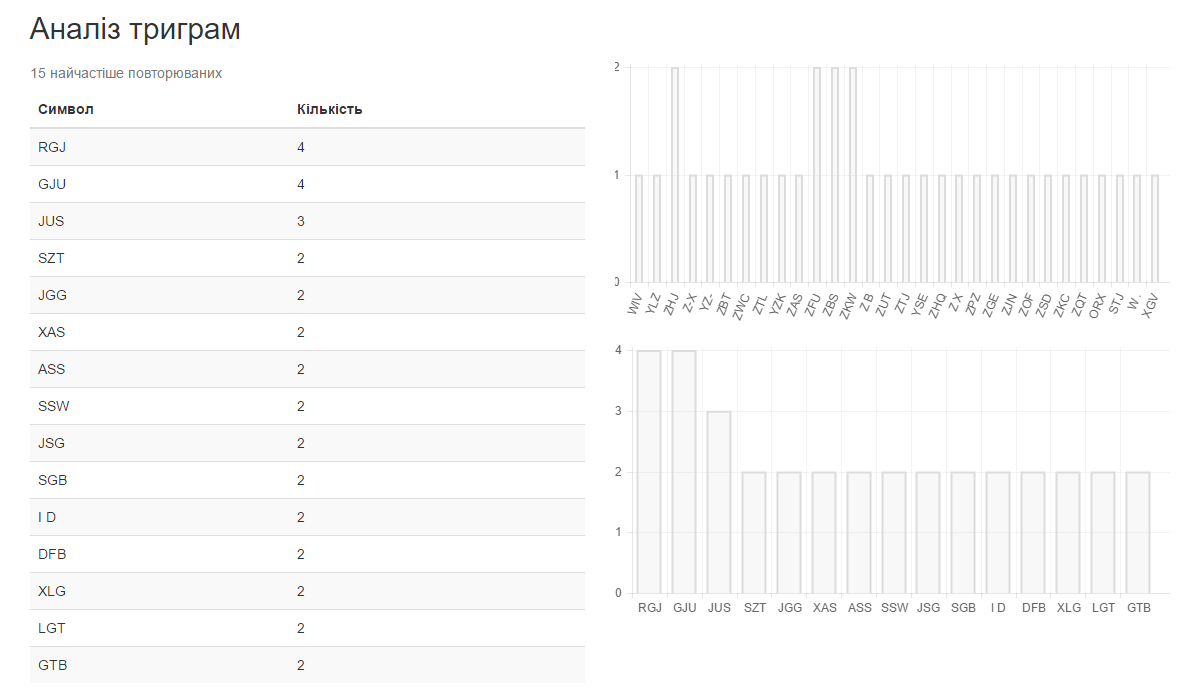


Рис. 14. Аналіз триграм

З графіка видно, що у ШТ частота літер вирівнюється і тому даний шифр є досить непростим для розшифрування.

***Код програми для шифрування Віженера тексту на мові JavaScript***

Лістінг vigenere-model.js

var ABC = ' ABCDEFGHIJKLMNOPQRSTUVWXYZ';

var decodeText = function(text, key, decode, abc){

text = text || '';

key = key || '';

var size = abc.length;

var keySize = key.length;

var codeKey = key.split('').map(function(x){

return abc.indexOf(x);

});

if (decode){

for (var i = 0; i < keySize; i++) {

codeKey[i] = (size - codeKey[i]) % size;

}

}

var decoded = '';

for (var i = 0, j = 0; i < text.length; i++) {

var char = text.charAt(i);

var abcCode = abc.indexOf(char);

if (abcCode >= 0){

var decodedCode = (abcCode + codeKey[j % keySize]) % size;

decoded += abc.charAt(decodedCode);

j++;

} else {

decoded += char;

}

}

return decoded;

}

exports.ABC = ABC;

exports.decodeText = decodeText;

### Результат

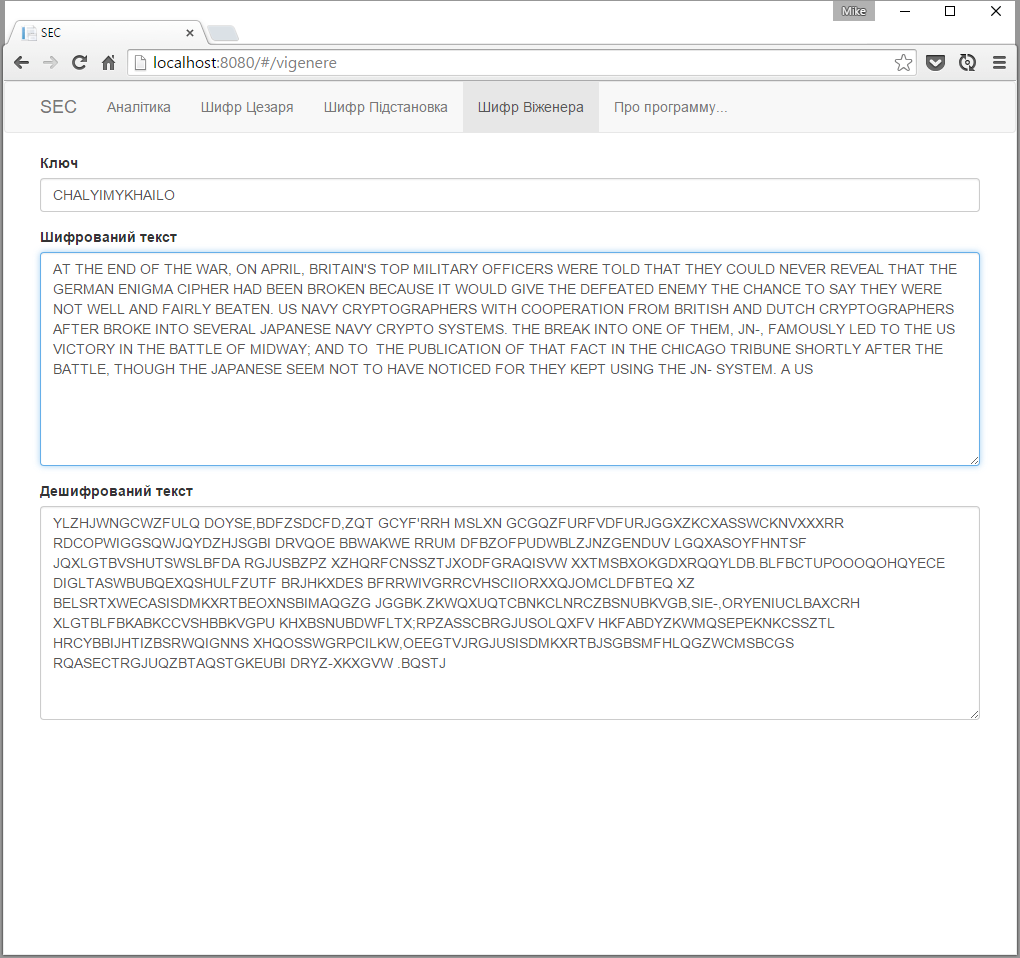


Рис. 15. Вигаляд програми для шифру Віжнера

### Висновок

У цьому розділі ми докладно ознайомились з шифром Віженера. Розшифрували та зашифрували текст даним методом, а також провели статистичний аналіз ВТ та ШТ.

У результаті визначили, що ВТ має досить помітний перепад частоти появи літер, тим самим легко можна визначити яка це літера. Аналогічна ситуація з біграмами та триграмами.

# Висновок

Виконавши дані лабораторні роботи ми здобули практичні навички роботи з шифрами заміни та перестановки, навчились розшифровувати та зашифровувати тексти шифрами Цезаря, Віженера та простої заміни, а також виконувати статистичний аналіз (частота входжень літер, біграм, триграм). А також на основі аналізу розшифровувати тексти.

У першій частині роботи ми виконували статистичний аналіз англомовного відкритого тексту. Це допомогло нам отримати загальні статистичні дані, які допомагали нам в подальшому розшифровувати тексти. Статистичний аналіз є важливою та невід’ємною складовою процесу розшифрування. Знаходження повторень у криптографії – це ті залежності в тексті, які дозволяють розшифрувати текст навіть без заданого ключа.

Шифри Цезаря та простої заміни вважаються недостатньо стійкими, адже піддаються розшифрування за допомогою частотного аналізу. Шифр Цезаря навіть можливо розшифрувати за допомогою перебору, причому для цього навіть не потрібно мати відомий повний алфавіт.

При розшифруванні даних шифрів використовували наступні особливості англійської мови:

* Найчастіше зустрічається символ пробілу, що зрозуміло, адже пробіл розділяє слова одне від одного.
* Другим символом, що найчастіше повторюється, є символ Е.
* Одна з найчастіше повторюваних біграм є триграма ТНЕ.

Шифр Віженера на відміну від шифрів Цезаря та простої заміни згладжує частоту літер. Головний недолік шифру Віженера полягає в тому, що його ключ повторюється. Тому криптоаналіз розділяється на два етапи: пошук довжини ключа та сам криптоаналіз.

Криптоаналіз після знаходження довжини ключа перетворюється в просте розшифрування ШТ шифром Цезаря.

Отже, в результаті виконання лабораторної роботи ми можеш сказати, що найстійкішим серед розглянутих методів шифрування є шифр Віженера.