Міністерство освіти і науки України

Національний університет «Львівська політехніка»

Кафедра: САПР



**ЗВІТ**

про виконання лабораторних робіт №1 – 4

з курсу: Технології захисту інформації

на тему:

Методи шифрування та дешифрування текстових повідомлень

Прізвище: Горик

Ім'я: Данило

Група: КН-306

Перевірив: Томюк В.В.

Львів – 2019

Зміст

[КОРОТКІ ТЕОРЕТИЧНІ ВІДОМОСТІ 3](#_Toc21504112)

[ЛАБОРАТОРНЕ ЗАВДАННЯ 5](#_Toc21504113)

[Лабораторна робота№1 6](#_Toc21504114)

[Лабароторна робота №2 10](#_Toc21504115)

[Лабараторна робота №3 12](#_Toc21504116)

[Лабараторна робота №4 14](#_Toc21504117)

**Мета роботи**

Мета роботи – дослідження статистичних властивостей відкритого тексту (ВТ) та шифрованого тексту (ШТ), вивчення простих методів шифрування та дешифрування інформації та їх властивостей (для шифрів заміни та шифрів перестановок).

# КОРОТКІ ТЕОРЕТИЧНІ ВІДОМОСТІ

**2.2. Статистичні характеристики ВТ і ШТ.**

Для кожної мови є певні характерні властивості ВТ. Частота використання букв в текстовому повідомлені залежить перш за все від мови, яка використовується і від предметної області (про що описується в повідомленні). Для кожної мови є якісь характерні особливості. Наприлад для англійської мови – це часто вживані артиклі  ***the*** і ***a.***  В французькій мові - це також артиклі ***le, la*** і ***less*** **.** Для російської мови характерно часто вживана буква ***о.*** Крім цього кожна мова і її алфавіт має конкретну кількість вживаних символів. Крім цього в криптоаналізі є дуже важливим параметром частоти використання певних буквосполучень. І кожна мова цей параметр має свій характерний частотний опис – частота використання букв і буквосполучень. Крім цих параметрів необхідно виділити кількість символів, які використовуються в ШТ. Окремі символи можуть замінятися іншими окремими символами або цифровими замінниками. Значність цифрозамінників визначають з допомогою аналізу ШТ. Для цього використовується аналіз повторень одинакових груп (буквосполучень) в ШТ і аналіз відстаней між ними. Цифрозамінники букв ВТ можуть замінятися 2-х, 3-х, 5-х значними цифровими групами. Якщо є бажання не збільшувати об’єм ШТ порівняно з ВТ, то частіше використовуються 2-х значні цифрові групи. Таким чином на першому етапі роботи з ШТ виконується відповідальна робота для визначення мови, яка відповідає ВТ, визначається можливі шифри, які використані для формування ШТ. Достовірність отриманих статистичних характеристик залежить перш за все від кількісних характеристик обробленого матеріалу. Якщо кількість символів ВТ і ШТ обчисляється кількома десятками, то такі статистичні дані не можуть мати високої достовірності. Статистичні дані можна сприймати як більш-менш достовірні, якщо кількість символів обчисляється кількома сотнями (і більше).

Більшість штучних мов (і всі природні мови) мають характерний частотний розподіл букв і інших знаків. Наприклад, буква Е найбільш часто зустрічається в англійській мові, а Z найбільш рідка. Однак це зовсім не говорить про те, що не будуть попадатися англійські (вихідні), повідомлення, в яких інша буква буде зустрічатися частіше, ніж Е, і рідше, ніж Z. Але для *дуже* великого числа англійських повідомлень можуть бути встановлені певні характерні частоти. Більшість повідомлень, зашифрованих методом перестановки або одноалфавітної підстановки, зберігають характерний частотний розподіл і, таким чином, дають крипто-аналітику шлях до розкриття шифру. Криптоаналітики часто використовують індекс відповідності (ІВ) для визначення того, чи знаходяться вони на правильному шляху.

По визначенню ІВ являє собою оцінку суми квадратів імовірностей кожної букви. Це використовується особливо у тих випадках, коли об'єм зашифрованого тексту відносно великий. Шифровки, які дають значення ІВ більші, ніж 0,066 (для англійської мови), самі повідомляють про те,що ймовірно використовувалася одноалфавітна підстановка, даючи, таким чином криптоаналітикам інструмент для того, щоб приступити до розгадки шифру. Якщо ІВ знаходиться між 0,052 і 0,066, то, ймовірно, був використаний двохалфавітний шифр підстановки. Криптоаналітик просто бере символ, що найчастіше зустрічається, і передбачає, що це пропуск, потім бере наступний найбільш частий символ і передбачає, що це Е, і т.д., щоб прийти до можливого рішення. Цей процес можна автоматизувати застосувавши ЕОМ, однак аналіз можливих варіантів повідомлень повинна робити людина. Справа дуже ускладнюється, коли криптоаналітик стикається з рівномірним розподілом символів (IВ=1/26=0,038 для англійської мови), який виходить при використанні багатоалфавітної підстановки. На наступних етапах виконуються певні дії для отримання ВТ на основі ШТ і статистичних даних, які отримані при статистичні обробці ШТ.

**2.3.1. 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 взаємооднозначна 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. Проілюструємо шифрування методом підстановки шифром який не є шифром Цезара.

**Початкове повідомлення:** WE NEED MORE SNOW FOR BETTER SKIING.

**Ключ:**

вхід: bABCDEFGHIJKLMNOPQRTUVWXYZ

вихід: VZHLANQRCWDXFOUSPBTIELGMbKY

**Зашифрований текст:**

МNVUNNAVOSTNVIUSMVQSTVHNEENTVIXWWUR

Зашифроване повідомлення отримано таким чином. Беремо знак з початкового повідомлення в рядку ВХІД ключа і замінюємо його відповідним знаком з рядка ВИХІД.

Цей метод підстановки, хоч до деякої міри і є ефективним для заплутування при випадковому прочитанні, не зможе надовго зупинити досвідченого промислового шпигуна, оскільки він легко піддається здійснюваному за допомогою ЕОМ частотному аналізу зустрічності букв і пар букв. 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.

Існують машини, що мають команду ТРАНСЛЮВАТИ, яка забезпечує дуже легкі для використання шифри підстановки. Наприклад, на ІВМ 370 користувач встановлює таблицю з 256 байтів. Двійкове значення кожного байта, яке користувач хоче зашифрувати, використовується як індекс в таблиці для пошуку відповідного перетвореного байта. Це перетворення здійснюється за одну машинну команду.

**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.

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 викоистовується 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.

# ЛАБОРАТОРНЕ ЗАВДАННЯ

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 трьохграм (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 (і розшифрувати ) 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.

# Лабораторна робота№1

Статистичний аналіз відкритого тексту

Хід роботи

**Відкритий текст:**

IT INT RODUCED 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 ALGOR

ITHMS, 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 HASBEEN 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 DIFFIEHELLMAN 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 COMM

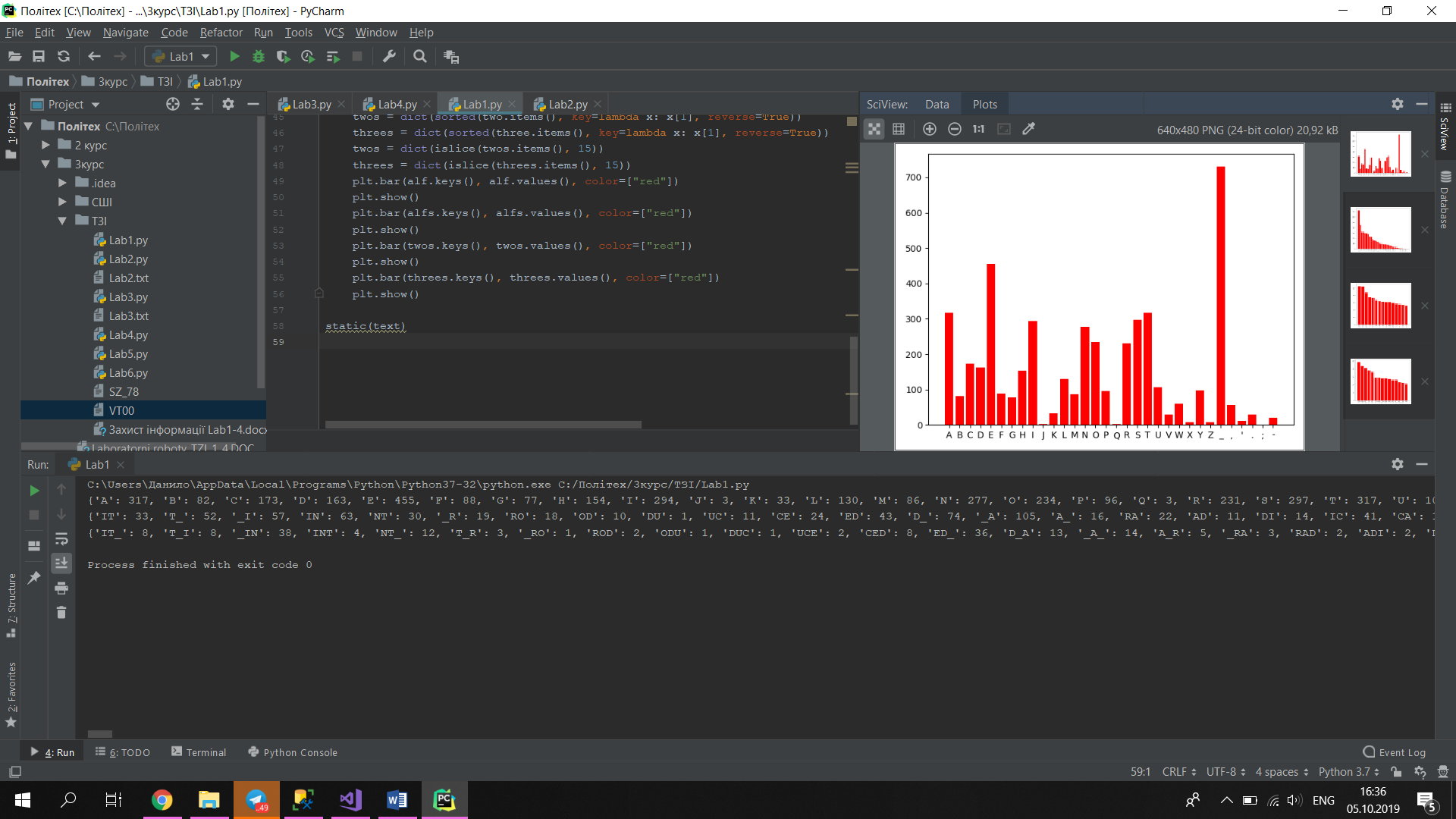
UNICATION FACILITIES FOR BUSINESSES SUCH AS BANKS AND OTHER LARGE FINANCIAL ORGANIZATIONS. AFTER 'ADVICE' AND MODIFICATION BY NSA, ACTING BEHIND THE SCENES, IT WAS ADOPTED AND PUBLISHED AS A FEDERAL INFORMATION PROCESSING STANDARD PUBLICATI ON IN-. DES WAS THE FIRST PUBLICLY ACCESSIBLE CIPHER TO BE 'BLESSED' 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 OFFICI

ALLY 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

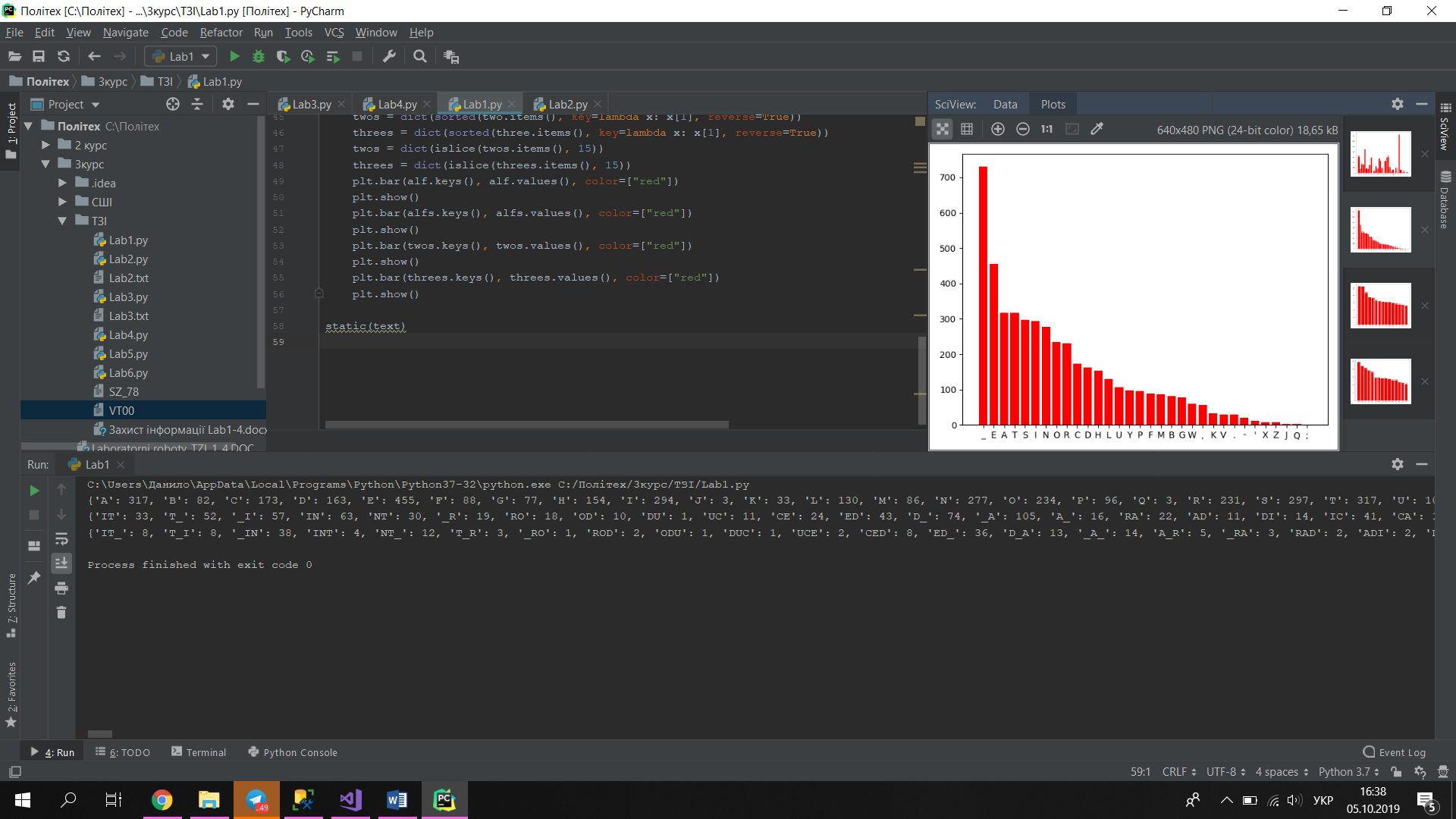
**Програма:**

import matplotlib.pyplot as plt  
from itertools import islice  
  
f = open('VT00', 'r')  
text = f.read()  
  
  
def static(text):  
 alf = {'A': 0, 'B': 0, 'C': 0, 'D': 0, 'E': 0, 'F': 0, 'G': 0, 'H': 0, 'I': 0, 'J': 0, 'K': 0, 'L': 0, 'M': 0, 'N': 0,  
 'O': 0, 'P': 0, 'Q': 0, 'R': 0, 'S': 0, 'T': 0, 'U': 0, 'V': 0, 'W': 0, 'X': 0, 'Y': 0, 'Z': 0, '\_': 0, ',': 0,  
 "'": 0, '.': 0, ';': 0, '-': 0}  
 two = {}  
 three = {}  
 for i in text.upper():  
 if i in alf:  
 k = alf.get(i)  
 k += 1  
 alf[i] = k  
 if i == ' ':  
 k = alf.get('\_')  
 k += 1  
 alf['\_'] = k  
 print(alf)  
 for i in range(len(text)):  
 t = text[i:i + 2].upper()  
 c = 0  
 for k in range(len(text)):  
 if t == text[k:k + 2].upper():  
 c += 1  
 if ' ' in t:  
 t = t.replace(' ', '\_')  
 two[t] = c  
 print(two)  
 for i in range(len(text)):  
 t = text[i:i + 3].upper()  
 c = 0  
 for k in range(len(text)):  
 if t == text[k:k + 3].upper():  
 c += 1  
 if ' ' in t:  
 t = t.replace(' ', '\_')  
 three[t] = c  
 print(three)  
 alfs = dict(sorted(alf.items(), key=lambda x: x[1], reverse=True))  
 twos = dict(sorted(two.items(), key=lambda x: x[1], reverse=True))  
 threes = dict(sorted(three.items(), key=lambda x: x[1], reverse=True))  
 twos = dict(islice(twos.items(), 15))  
 threes = dict(islice(threes.items(), 15))  
 plt.bar(alf.keys(), alf.values(), color=["red"])  
 plt.show()  
 plt.bar(alfs.keys(), alfs.values(), color=["red"])  
 plt.show()  
 plt.bar(twos.keys(), twos.values(), color=["red"])  
 plt.show()  
 plt.bar(threes.keys(), threes.values(), color=["red"])  
 plt.show()

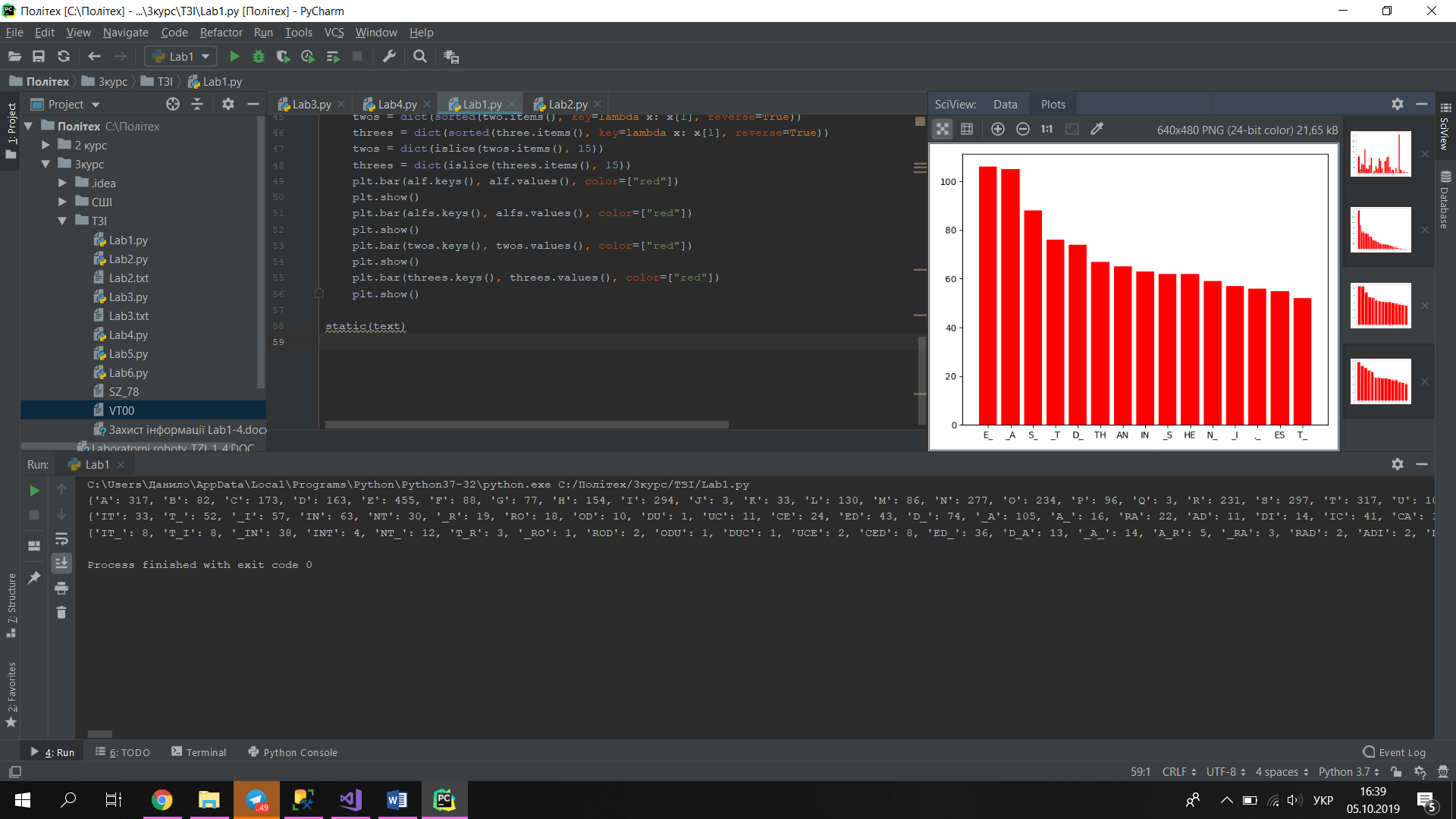
**Статичний аналіз**



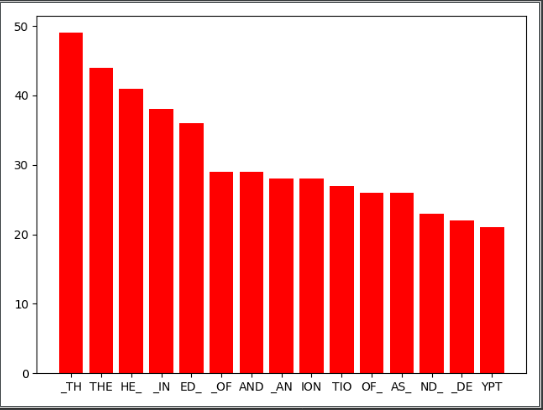
Таблиця 1. Статистичний аналіз по алфавіту



Таблиця 2. Статистичний аналіз по спаданню



Таблиця 3. Статистичний аналіз двограм



Таблиця 4. Статистичний аналіз триграм

**Висновок:**

Провівши статистичний аналіз ВТ, отримали гістограми в алфавітному порядку, по спаданню, біграм і триграм. Отже найбільше в тексті зустрічається пробіл далі буква Е і після неї А. В триграмах найбільше зустрчається \_TH і ТНЕ.

# Лабароторна робота №2

**Шифрований текст:**

.'T,PF-SPFL--LNVP,F-ZF-,DFPAP,DF Z;;TMWPFVPDGF-ZF '-F-ST;FTYFNZY-PC-HFPLNSFMTYL,DF'YT-FZQFTYQZ,XL-TZYHFZ,FMT-HFSL;FLFALW'PGFLFJMT-FVPDFBZ'WOFSLAPF.'LO,TWWTZYHF Z;;TMWPFVPD;F-ZF-,DFLYOFOPNT SP,F-SPFXP;;LRPGFBT-SFXZOP,YF-PNSYZWZRDHF-SP;PFY'XMP,;FL,PFMPNZXTYRFPL;TP,F-ZFOPNT SP,IFSZBPAP,HFL;F-PNSYZWZRDFLOALYNP;HF;ZFOZP;F-SPF.'LWT-DFZQFPYN,D -TZYGF;TYNPFBBTTHFZYPFZQF-SPFXZ;-FYZ-LMWPFLOALYNP;FTYF-SPF;-'L WTNL-TZYF ,ZR,LX;FQZ,FNZX '-P,JLTOPOFOP;TRYFNLYFMPF,'YFZYFLWXZ;-FLYDFNZX '-P,FNZY;T;-TYRFZQFNPY-,LWF ,ZNP;;TYRF'YT-HFXPXZ,DFLYOF;ZXPF-D PFZQFTY '-FLYOFZ'- '--ST;FSZWO;F-,'PFMPNL';PFOPNT SP,TYRFLYFPYN,D -POFXP;;LRPFMDFM,'-PFQZ,NPFBZ'WOFMP

**Код програми:**

from Lab1 import static  
f = open('Lab2.txt', 'r')  
text = f.read()  
alf = ['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', ' ', '.', ',', ';', '-', "'"]  
key = 11  
decode = {}  
dtext = ""  
for i in alf:  
 k = alf.index(i) - key  
 decode[i] = k  
for i in text:  
 try:  
 if i != '\n':  
 dtext += alf[decode.get(i)]  
 else:  
 dtext += i  
 except TypeError:  
 continue  
print(dtext)  
  
static(dtext)

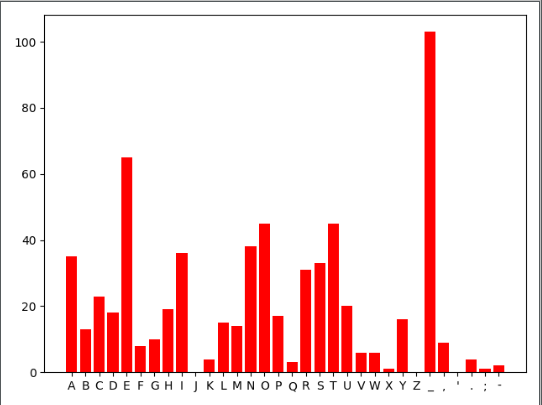
Ключ = 11

**Вільний текст:**

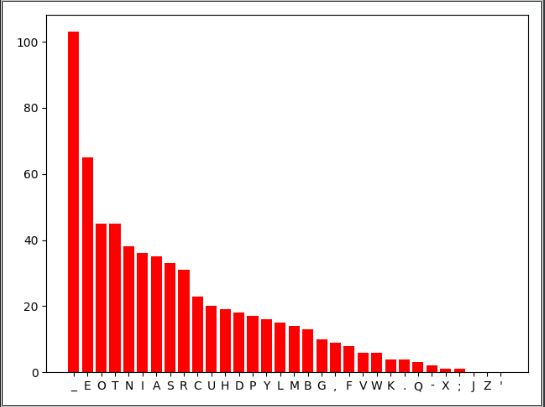
QUIRE THE ATTACKER TO TRY EVERY POSSIBLE KEY. TO PUT THIS IN CONTEXT, EACH BINARY UNIT OF INFORMATION, OR BIT, HAS A VALUE. A -BIT KEY WOULD HAVE QUADRILLION, POSSIBLE KEYS TO TRY AND DECIPHER THE MESSAGE. WITH MODERN TECHNOLOGY, THESE NUMBERS ARE BECOMING EASIER TO DECIPHER; HOWEVER, AS TECHNOLOGY ADVANCES, SO DOES THE QUALITY OF ENCRYPTION. SINCE WWII, ONE OF THE MOST NOTABLE ADVANCES IN THE STU

APPLICATION PROGRAMS FOR COMPUTER-AIDED DESIGN CAN BE RUN ON ALMOST ANY COMPUTER CONSISTING OF CENTRAL PROCESSING UNIT, MEMORY AND SOME TYPE OF INPUT AND OUTPUT THIS HOLDS TRUE BECAUSE DECIPHERING AN ENCRYPTED MESSAGE BY BRUTE FORCE WOULD BE

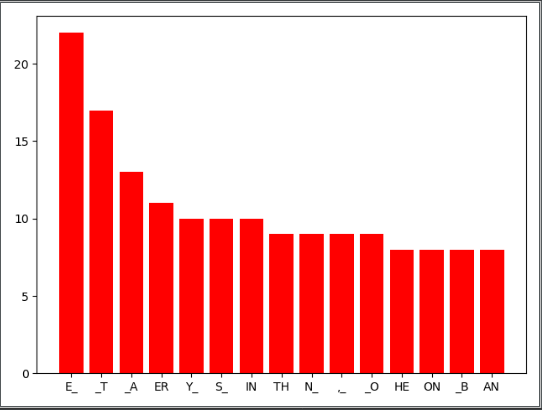
**Статичний аналіз**



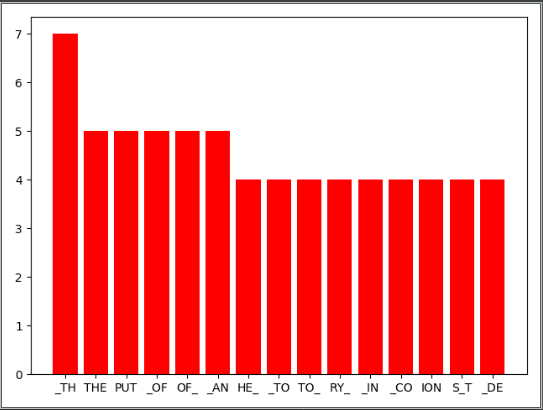
Таблиця 1. Статистичний аналіз по алфавіту



Таблиця 2. Статистичний аналіз по спаданню



Таблиця 3. Статистичний аналіз біграм



Таблиця 4. Статистичний аналіз триграм

**Висновок:**

Провівши статистичний аналіз ШТ і підібравши ключ ми отримали шо зміщення по Шифру Цезаря це 11. І провівши статистику по ВТ отримали дуже подібні графіки де пробіл і Е співпадають з Першою лабараторною роботою.

# Лабараторна робота №3

**Шифрований текст:**

.'T,PF-SPFL--LNVP,F-ZF-,DFPAP,DF Z;;TMWPFVPDGF-ZF '-F-ST;FTYFNZY-PC-HFPLNSFMTYL,DF'YT-FZQFTYQZ,XL-TZYHFZ,FMT-HFSL;FLFALW'PGFLFJMT-FVPDFBZ'WOFSLAPF.'LO,TWWTZYHF Z;;TMWPFVPD;F-ZF-,DFLYOFOPNT SP,F-SPFXP;;LRPGFBT-SFXZOP,YF-PNSYZWZRDHF-SP;PFY'XMP,;FL,PFMPNZXTYRFPL;TP,F-ZFOPNT SP,IFSZBPAP,HFL;F-PNSYZWZRDFLOALYNP;HF;ZFOZP;F-SPF.'LWT-DFZQFPYN,D -TZYGF;TYNPFBBTTHFZYPFZQF-SPFXZ;-FYZ-LMWPFLOALYNP;FTYF-SPF;-'L WTNL-TZYF ,ZR,LX;FQZ,FNZX '-P,JLTOPOFOP;TRYFNLYFMPF,'YFZYFLWXZ;-FLYDFNZX '-P,FNZY;T;-TYRFZQFNPY-,LWF ,ZNP;;TYRF'YT-HFXPXZ,DFLYOF;ZXPF-D PFZQFTY '-FLYOFZ'- '--ST;FSZWO;F-,'PFMPNL';PFOPNT SP,TYRFLYFPYN,D -POFXP;;LRPFMDFM,'-PFQZ,NPFBZ'WOFMP

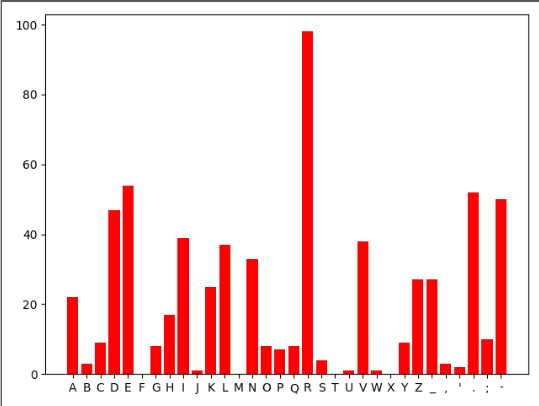
**Код програми:**

from Lab1 import static  
f = open('SZ\_78', 'r')  
text = f.read()  
alf = ['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', ' ', '.', ',', ';', '-', "'", '\n']  
decode=['F', ',', 'G', 'O', 'I', ';', 'M', 'L', 'N', 'K', 'H', 'R', 'J', 'S', 'B', 'W', 'Y', ' ', 'Z', 'Q', '-', 'A', 'X', "'", 'P', 'C', 'D', 'E', 'V', 'U', 'T', ".", '\n']  
dtext = ""  
for i in text:  
 dtext += decode[alf.index(i)]  
static(text)  
print(dtext)

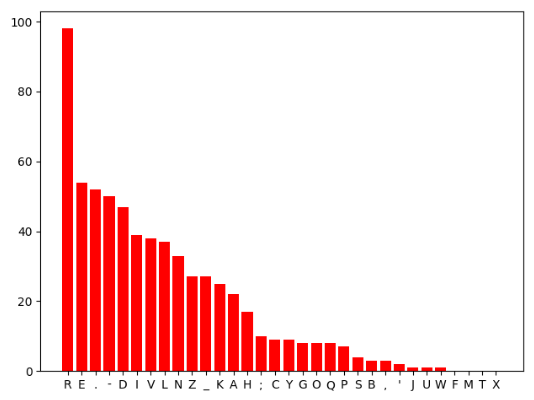
**Вільний текст:**

D ORGANIZING OF THE TRAFFIC FOR GROUP OF CONNECTED CROSSROADS OF THE CITY DISTRICT PROVIDES SYNCHRONIZING AND ALLOWS TO MINIMIZE THE DELAY ON THE MOST LOADED ROUTES BY TRANSITION FROM PACKAGE SWITCHING, FORMED BY CARS OR PEDESTRIANS, TO CHANNEL SWITCHING. THE IDENTIFICATION AND VERIFICATION OF THE PROPOSED MODELS ARE FULFILLED ON THE BASIS OF THE EXPERIMENTAL RESEARCHES, WHICH ARE CARRIED OUT WITHTHE BEHAVIOUR OF THE CARS IN TRANSITIONAL ZONE AND BUFFER-SLUICE IS DEFINED ON THE BASIS OF THE COLLECTED STATISTICAL DATA WHICH DESCRIBE DISTRIBUTION OF TRANSPORT FLOW ON THE CITY TERRITORY DURING DAY. THE AUTOMATIC DECISION OF PLANNING AN

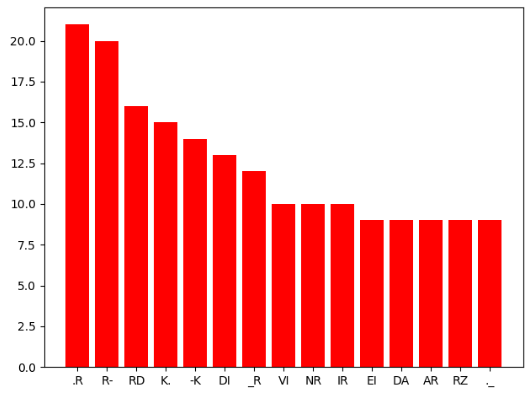
**Статичний аналіз**



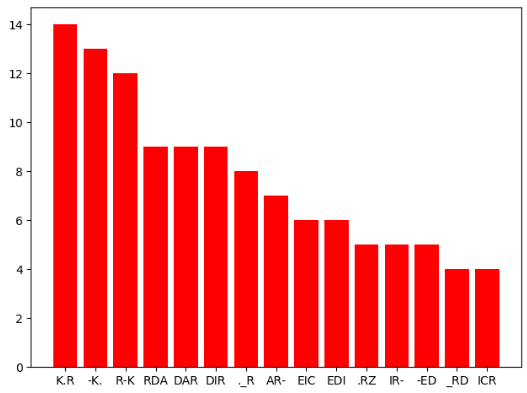
Таблиця 1. Статистичний аналіз по алфавіту



Таблиця 2. Статистичний аналіз по спаданню



Таблиця 3. Статистичний аналіз біграм



Таблиця 4. Статистичний аналіз триграм

**Висновок:**

Провівши статистичний аналіз 1 і 2 лабараторної роботи і проаналізувавши статистику шифрованого тексту де пробіл це R, а триграма ТНЕ це –К., після цього методом підстановки розгадав і весь алфавіт, і отримав ВТ.

# Лабараторна робота №4

**Вільний текст:**

QUIRE THE ATTACKER TO TRY EVERY POSSIBLE KEY. TO PUT THIS IN CONTEXT, EACH BINARY UNIT OF INFORMATION, OR BIT, HAS A VALUE. A -BIT KEY WOULD HAVE QUADRILLION, POSSIBLE KEYS TO TRY AND DECIPHER THE MESSAGE. WITH MODERN TECHNOLOGY, THESE NUMBERS ARE BECOMING EASIER TO DECIPHER; HOWEVER, AS TECHNOLOGY ADVANCES, SO DOES THE QUALITY OF ENCRYPTION. SINCE WWII, ONE OF THE MOST NOTABLE ADVANCES IN THE STU

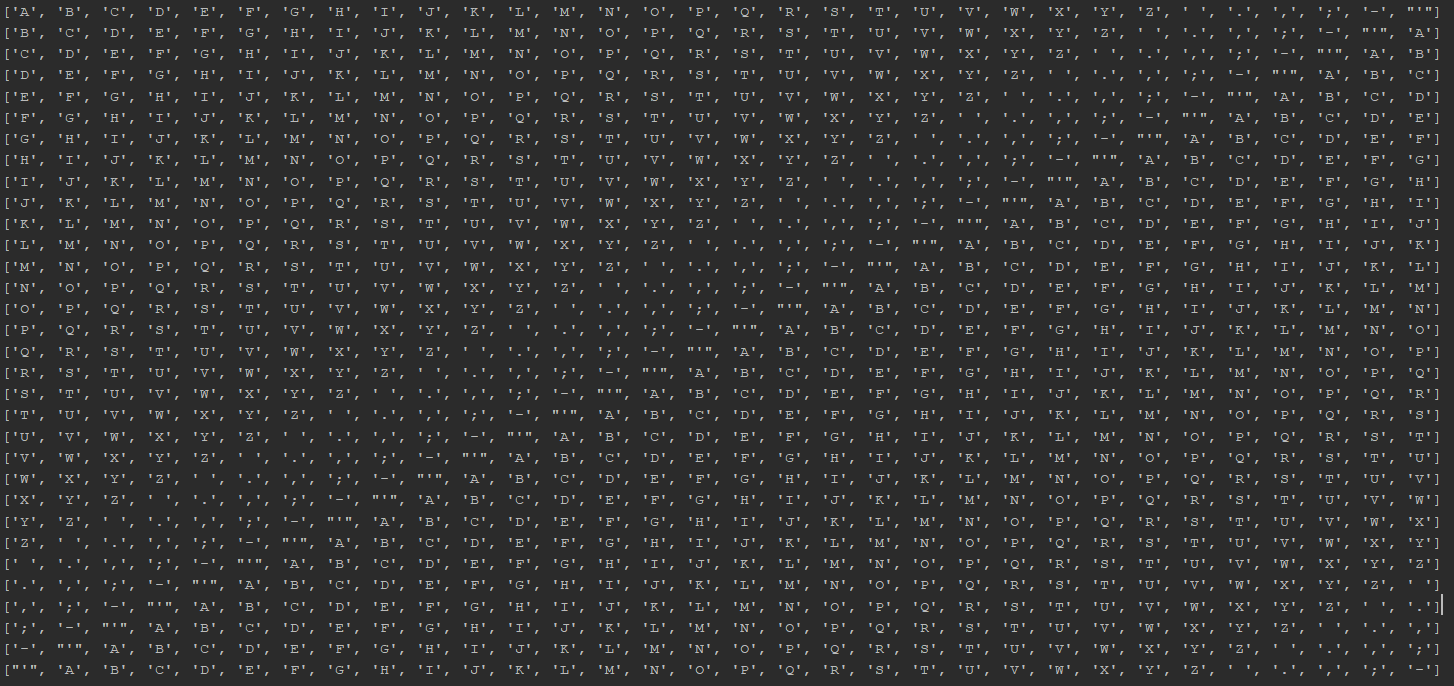
APPLICATION PROGRAMS FOR COMPUTER-AIDED DESIGN CAN BE RUN ON ALMOST ANY COMPUTER CONSISTING OF CENTRAL PROCESSING UNIT, MEMORY AND SOME TYPE OF INPUT AND OUTPUT THIS HOLDS TRUE BECAUSE DECIPHERING AN ENCRYPTED MESSAGE BY BRUTE FORCE WOULD BE

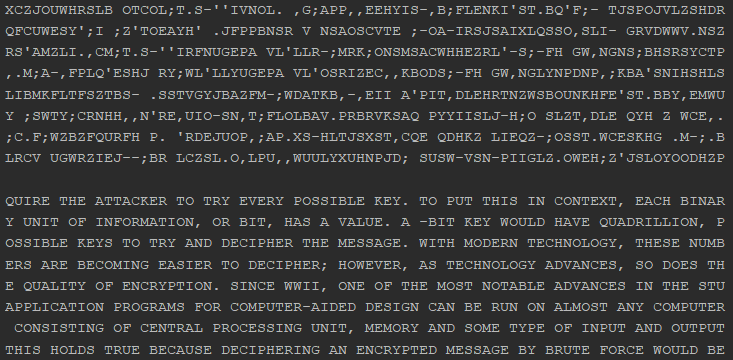
**Код програми:**

alf = ['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', ' ', '.', ',', ';', '-', "'"]  
table = []  
key = 'HORYK DANYLO'  
f = open('Lab3.txt', 'r')  
text = f.read()  
key\_str = ''  
dtext = ''  
for i in range(0, len(alf)):  
 k = alf[:i]  
 c = alf[i:]  
 table.append(c + k)  
print(\*table, sep="\n")  
  
count = len(text) // len(key)  
for i in range(0, count):  
 key\_str += key  
key\_str += key[:len(text) % len(key)]  
  
for i in range(0, len(text)):  
 if text[i] != '\n':  
 dtext += table[alf.index(text[i])][alf.index(key\_str[i])]  
 else:  
 dtext += '\n'  
print(dtext, "\n")  
print(text)

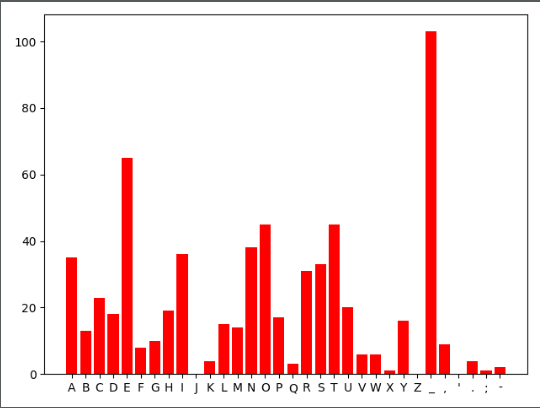
Ключ = Horyk Danylo

**Результати виконання:**

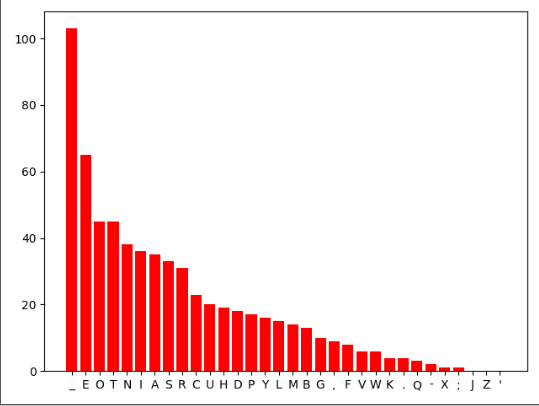




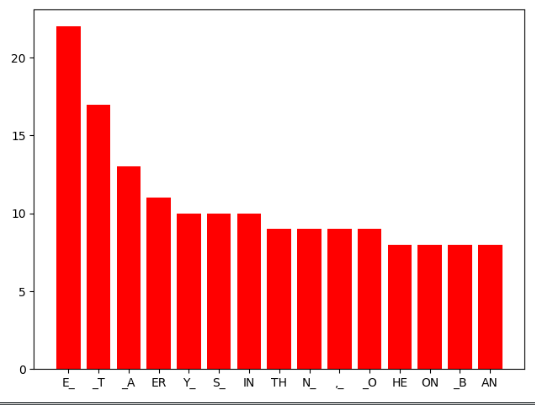
**Статичний аналіз**



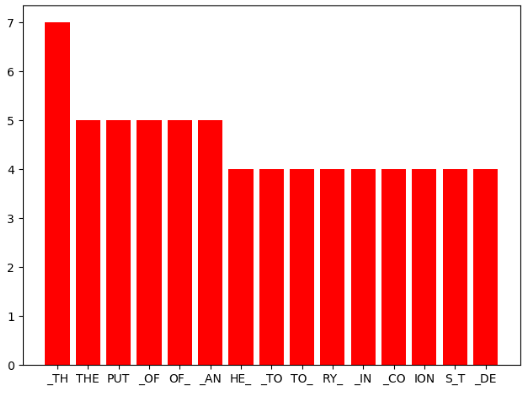
Таблиця 1. Статистичний аналіз по алфавіту ВТ



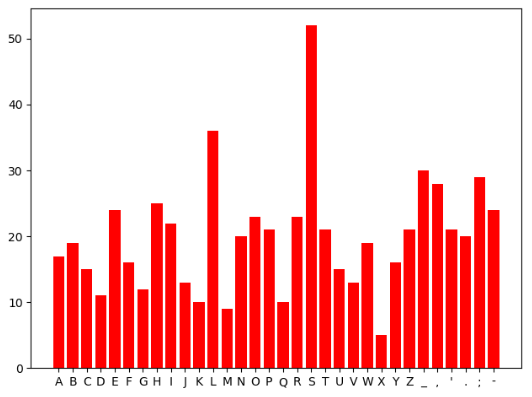
Таблиця 2. Статистичний аналіз по спаданню ВТ



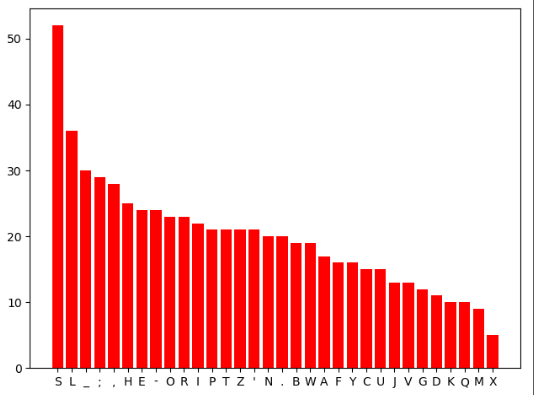
Таблиця 3. Статистичний аналіз біграм ВТ



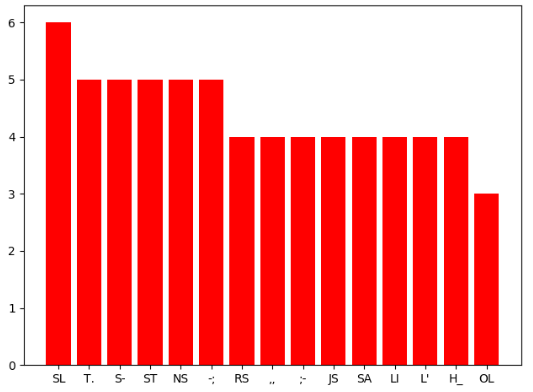
Таблиця 4. Статистичний аналіз триграм ВТ



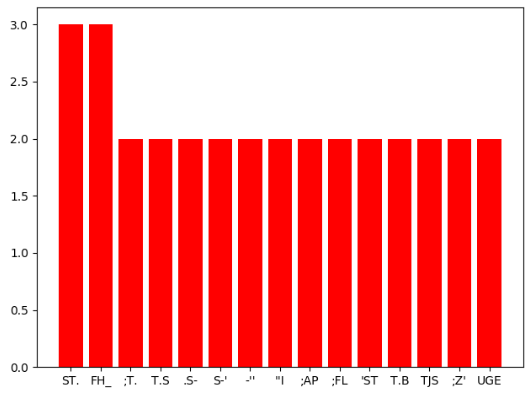
Таблиця 5. Статистичний аналіз по алфавіту ШТ



Таблиця 6. Статистичний аналіз по спаданню ШТ



Таблиця 7. Статистичний аналіз біграм ШТ



Таблиця 8. Статистичний аналіз триграм ШТ

**Висновок:**

Зробивши лабараторну роботу за Шифром Віженера і праналізувавши її, визначив що в залежності від ключа використовуються тільки деякі стовпці таблиці. Провівши статистичний аналіз ШТ і ВТ то S це пробіл, а L це Е.