

Міністерство освіти і науки України
Харківський радіотехнічний фаховий коледж

ЛАБОРАТОРНА РОБОТА №1
Найпростіші способи шифрування даних, шифр Цезаря.
з дисципліни
«Технології захисту інформації»

Виконала:
студентка групи ПІ-431
Узун Діана Дмитрівна
Керівник роботи:
Бриксін В.О.

Харків 2024

ЗАХИСТ ІНФОРМАЦІЇ

ЛАБОРАТОРНА РОБОТА №1

Найпростіші способи шифрування даних, шифр Цезаря.

Мета роботи: застосувати практично найпростіші оборотні перетворення вихідних даних із метою шифрування інформації.

Завдання

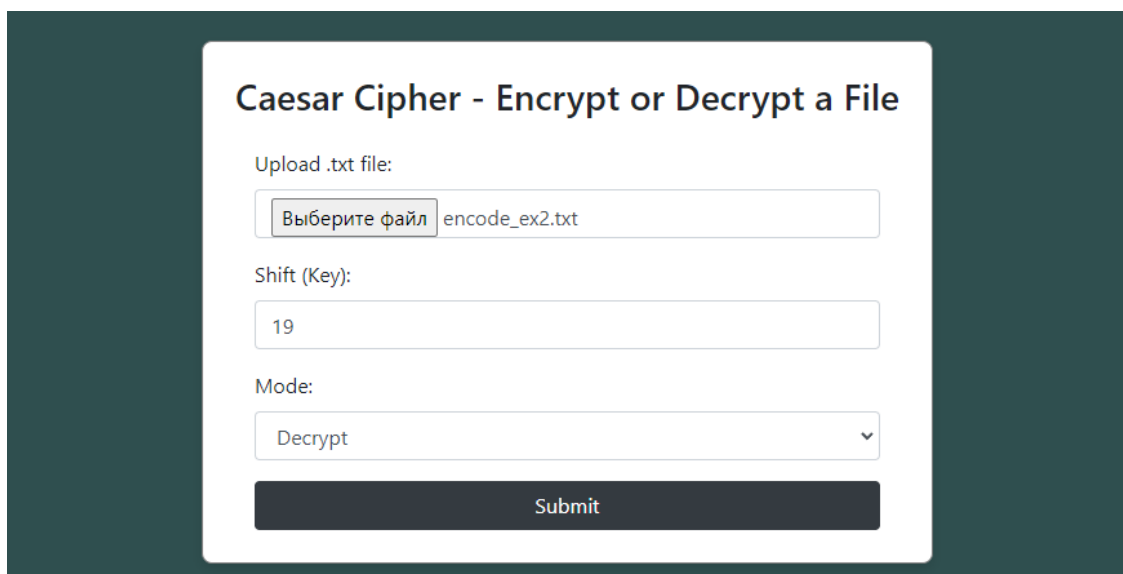
1. Підготувати тестовий приклад: текстовий файл (англійською чи українською мовами), що містить 500-1500 символів. На початку файлу мають бути вказані прізвища студентів, які виконують це завдання.
2. Реалізувати додаток, що перевіряє оборотність шифрування/дешифрування (шляхом порівняння файлів).
3. Реалізувати додаток, що демонструє шифрування та дешифрування інформації. Переконайтеся у оборотності шифрування.

Варіант	Метод шифрування	Зсув літер алфавіту	Ключ
19	Код Цезаря	У право	19

Результати виконання завдань

Додаток був написаний на мові програмування Python, за допомогою фреймворку Flask. вихідний код програми був викладений на GitHub: <https://github.com/ddianaoo/Caesar-Cipher.git>.

Графічний вигляд:



Caesar Cipher - Encrypt or Decrypt a File

Upload .txt file:

Выберите файл encode_ex2.txt

Shift (Key):

19

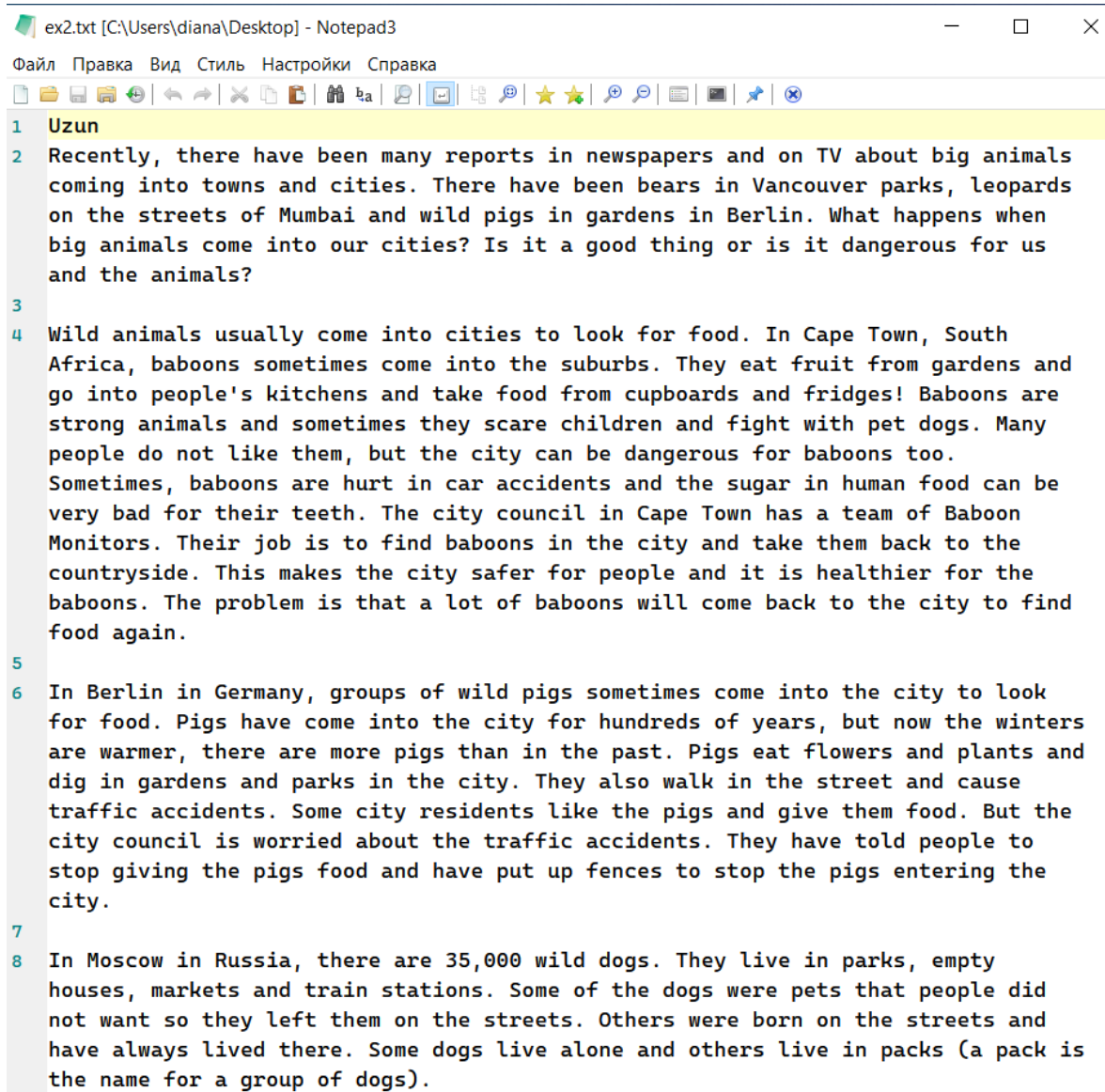
Mode:

Decrypt

Submit

Тестування додатку

1. Файл для шифрування:



2. Заповнення та відправка форми:

Caesar Cipher - Encrypt or Decrypt a File

Upload .txt file:

Выберите файл

ex2.txt

Shift (Key):

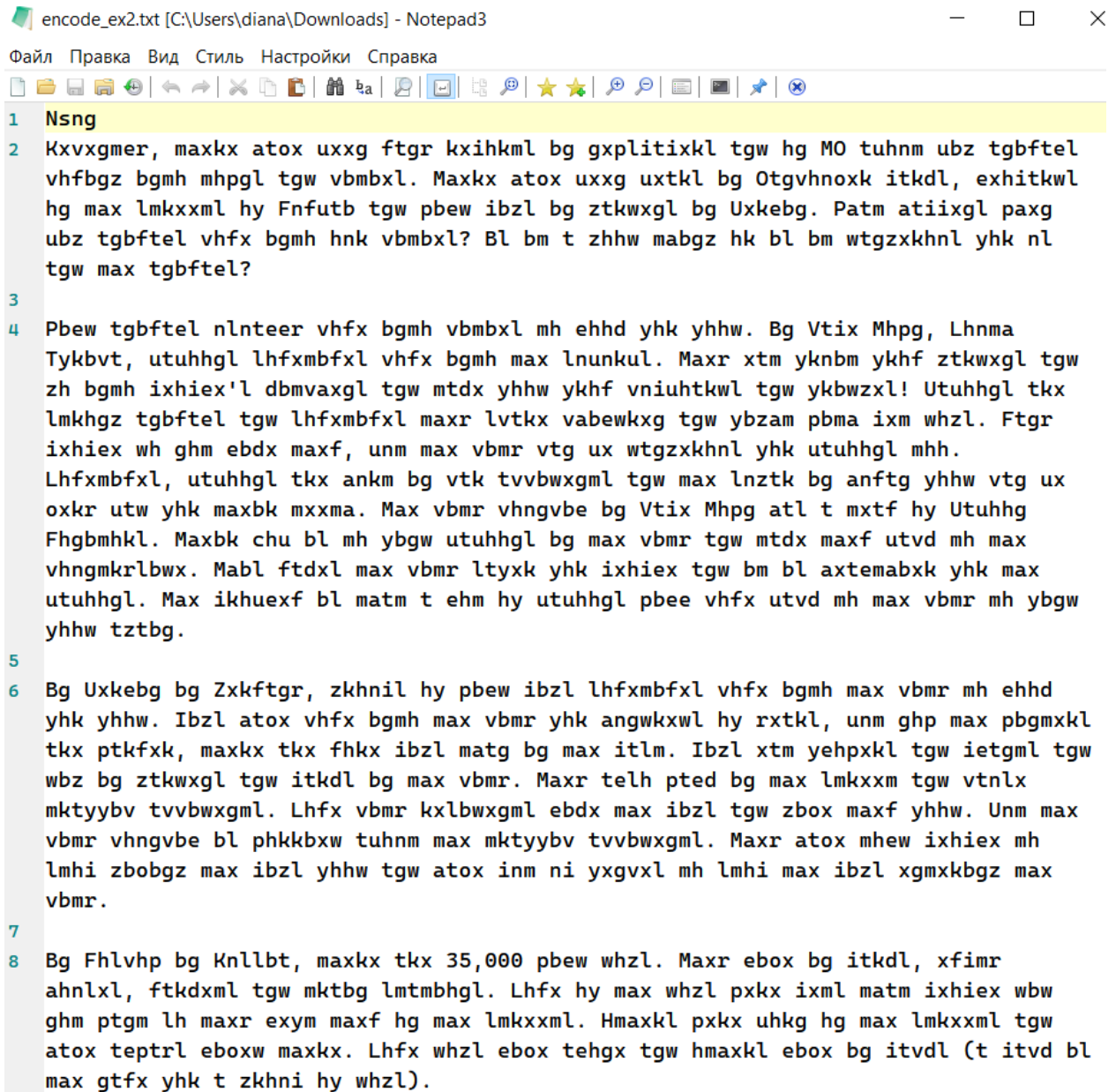
19

Mode:

Encrypt

Submit

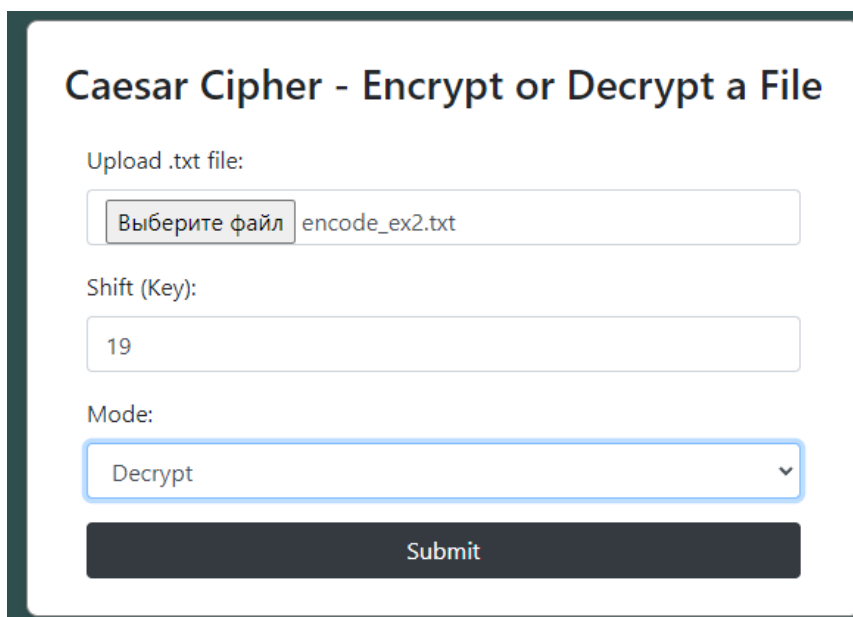
3. Отриманий файл після шифрування:



The screenshot shows a Notepad3 window with the title bar 'encode_ex2.txt [C:\Users\diana\Downloads] - Notepad3'. The menu bar includes 'Файл', 'Правка', 'Вид', 'Стиль', 'Настройки', and 'Справка'. The toolbar contains various icons for file operations and editing. The text in the editor is as follows:

```
1 Nsng
2 Kxvvgmer, maxx atox uxxg ftgr kxihtml bg gxplitixkl tgw hg M0 tuhnm ubz tgbftel
  vhfbgz bgmh mhppl tgw vbmbxl. Maxx atox uxxg uxtkl bg Otvhnoxk itkdl, exhitkwl
  hg max lmkxxml hy Fnfutb tgw pbew ibzl bg ztkwxgl bg Uxkebg. Patm atiixgl paxg
  ubz tgbftel vhfz bgmh hnk vbmbxl? Bl bm t zhhw mabgz hk bl bm wtgzxkhn1 yhk nl
  tgw max tgbftel?
3
4 Pbew tgbftel nlnteer vhfz bgmh vbmbxl mh ehhd yhk yhhw. Bg Vtix Mhpg, Lhnma
  Tykbvt, utuhhgl lhfxbfxl vhfz bgmh max lnunkul. Maxr xtm yknbm ykhf ztkwxgl tgw
  zh bgmh ixhiex'l dbmvaxgl tgw mtdx yhhw ykhf vniuhtkwl tgw ykbwzxl! Utuhhgl tkx
  lmkhgz tgbftel tgw lhfxbfxl maxr lvtkx vabewkxg tgw ybzam pbma ixm whzl. Ftgr
  ixhiex wh ghm ebdx maxf, unm max vbmr vtg ux wtgzxkhn1 yhk utuhhgl mhh.
  Lhfxbfxl, utuhhgl tkx ankml bg vtk tvvbwxgml tgw max lnztk bg anftg yhhw vtg ux
  oxkr utw yhk maxbk mxxma. Max vbmr vhnvgbe bg Vtix Mhpg atl t mxtf hy Utuhhg
  Fhgbmhkl. Maxbk chu bl mh ybgw utuhhgl bg max vbmr tgw mtdx maxf utvd mh max
  vhnmgkrlbw. Mabl ftdxl max vbmr ltyxk yhk ixhiex tgw bm bl axtemabxk yhk max
  utuhhgl. Max ikhuexf bl matm t ehm hy utuhhgl pbee vhfz utvd mh max vbmr mh ybgw
  yhhw tztbg.
5
6 Bg Uxkebg bg Zxkftgr, zkhn1 hy pbew ibzl lhfxbfxl vhfz bgmh max vbmr mh ehhd
  yhk yhhw. Ibzl atox vhfz bgmh max vbmr yhk angwkxwl hy rxtkl, unm ghp max pbgmxl
  tkx ptkfxk, maxx tkx fhkx ibzl matg bg max itlm. Ibzl xtm yehpxkl tgw ietgml tgw
  wbz bg ztkwxgl tgw itkdl bg max vbmr. Maxr telh pted bg max lmkxxm tgw vtnlx
  mktyybv tvvbwxgml. Lhfz vbmr kxlbwxgml ebdx max ibzl tgw zbox maxf yhhw. Unm max
  vbmr vhnvgbe bl phkkbxw tuhnm max mktyybv tvvbwxgml. Maxr atox mhew ixhiex mh
  lmhi zbobgz max ibzl yhhw tgw atox inm ni yxgvxl mh lmhi max ibzl xgmxbgz max
  vbmr.
7
8 Bg Fhlvhp bg Knllbt, maxx tkx 35,000 pbew whzl. Maxr ebox bg itkdl, xfimr
  ahnlxl, ftkdxml tgw mktbg lmtmbhgl. Lhfz hy max whzl pxkx ixml matm ixhiex wbw
  ghm ptgm lh maxr exym maxf hg max lmkxxml. Hmaxkl pxkx uhkg hg max lmkxxml tgw
  atox teptrl eboxw maxx. Lhfz whzl ebox tehgx tgw hmaxkl ebox bg itvdl (t itvd bl
  max gtfx yhk t zkhn1 hy whzl).
```

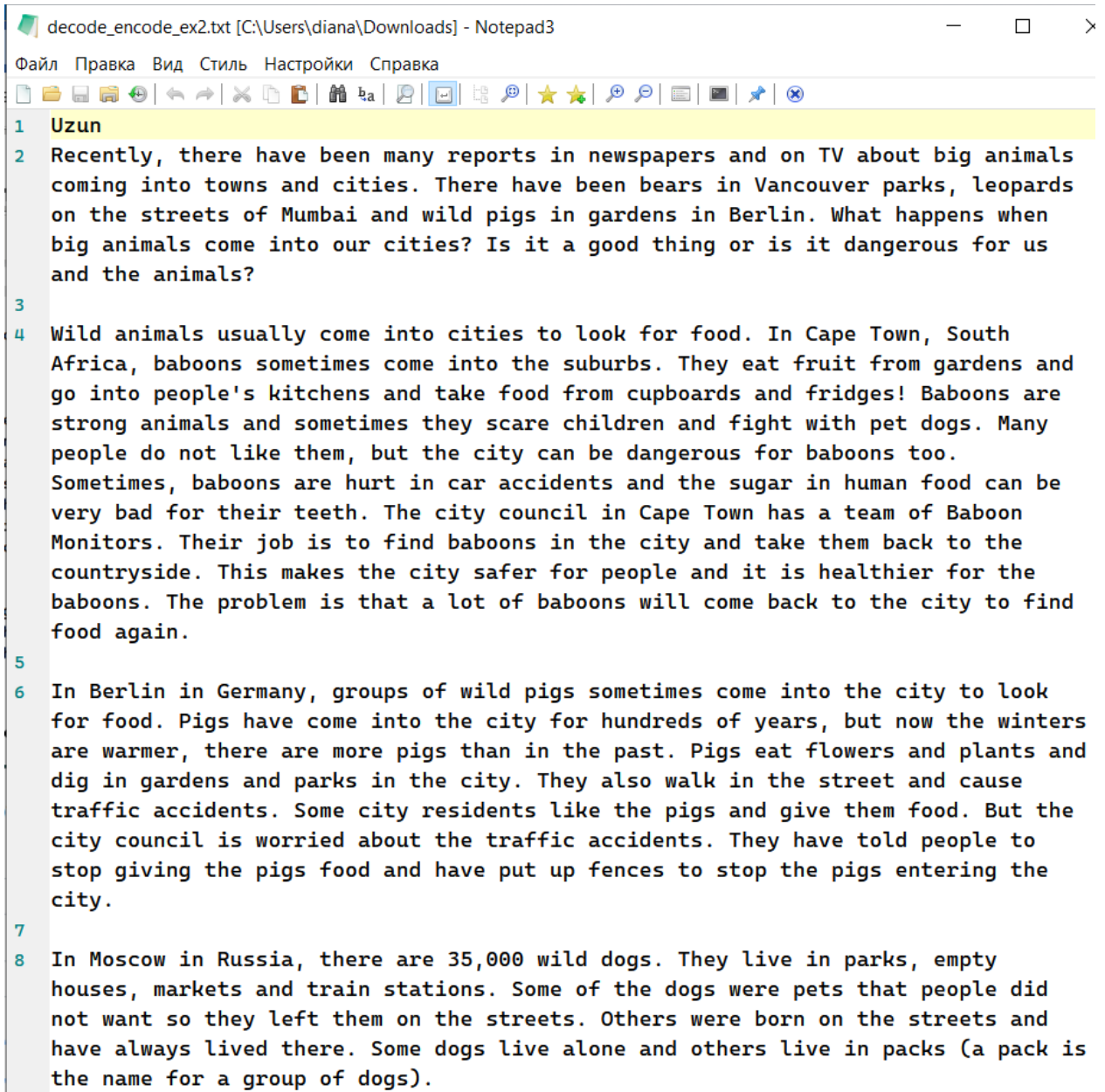
4. Візьмемо отриманий файл для дешифрування:



The screenshot shows a web application titled 'Caesar Cipher - Encrypt or Decrypt a File'. It has the following fields and controls:

- Upload .txt file:** A file selection button labeled 'Выберите файл' and a text input field containing 'encode_ex2.txt'.
- Shift (Key):** A text input field containing the number '19'.
- Mode:** A dropdown menu with 'Decrypt' selected.
- Submit:** A dark grey button at the bottom.

5. Отриманий файл після дешифрування:



The screenshot shows a Notepad3 window with the title 'decode_encode_ex2.txt [C:\Users\diana\Downloads] - Notepad3'. The menu bar includes 'Файл', 'Правка', 'Вид', 'Стиль', 'Настройки', and 'Справка'. The toolbar contains various icons for file operations and editing. The text is displayed in a monospaced font with line numbers on the left. The text is as follows:

```
1  Uzun
2  Recently, there have been many reports in newspapers and on TV about big animals
   coming into towns and cities. There have been bears in Vancouver parks, leopards
   on the streets of Mumbai and wild pigs in gardens in Berlin. What happens when
   big animals come into our cities? Is it a good thing or is it dangerous for us
   and the animals?
3
4  Wild animals usually come into cities to look for food. In Cape Town, South
   Africa, baboons sometimes come into the suburbs. They eat fruit from gardens and
   go into people's kitchens and take food from cupboards and fridges! Baboons are
   strong animals and sometimes they scare children and fight with pet dogs. Many
   people do not like them, but the city can be dangerous for baboons too.
   Sometimes, baboons are hurt in car accidents and the sugar in human food can be
   very bad for their teeth. The city council in Cape Town has a team of Baboon
   Monitors. Their job is to find baboons in the city and take them back to the
   countryside. This makes the city safer for people and it is healthier for the
   baboons. The problem is that a lot of baboons will come back to the city to find
   food again.
5
6  In Berlin in Germany, groups of wild pigs sometimes come into the city to look
   for food. Pigs have come into the city for hundreds of years, but now the winters
   are warmer, there are more pigs than in the past. Pigs eat flowers and plants and
   dig in gardens and parks in the city. They also walk in the street and cause
   traffic accidents. Some city residents like the pigs and give them food. But the
   city council is worried about the traffic accidents. They have told people to
   stop giving the pigs food and have put up fences to stop the pigs entering the
   city.
7
8  In Moscow in Russia, there are 35,000 wild dogs. They live in parks, empty
   houses, markets and train stations. Some of the dogs were pets that people did
   not want so they left them on the streets. Others were born on the streets and
   have always lived there. Some dogs live alone and others live in packs (a pack is
   the name for a group of dogs).
```

Опис отриманих результатів

В процесі тестування програми було проведено шифрування та дешифрування текстових файлів за допомогою алгоритму Цезаря із заданим зсувом. Після шифрування вміст початкового файлу було перетворено відповідно до алгоритму, що змістив літери на визначену кількість позицій вправо.

Після застосування операції дешифрування до зашифрованого файлу, вміст було відновлено до початкового стану. Це дозволяє зробити висновок, що програма успішно реалізує необхідну логіку, зокрема коректну оборотність

процесів шифрування та дешифрування. Початковий і кінцевий файли в результаті виявились ідентичними, що підтверджує правильність роботи програми.

Висновки

У процесі виконання лабораторної роботи №1 було досліджено один із найпростіших методів шифрування даних — шифр Цезаря. Цей метод базується на зсуві літер алфавіту на певну кількість позицій.

Результати роботи показали, що шифр Цезаря дійсно дозволяє здійснювати оборотне перетворення інформації, тобто після шифрування дані можуть бути коректно відновлені шляхом дешифрування. Це підтверджує функціональність і простоту цього методу для базового захисту інформації.

Мета роботи, яка полягала в практичному застосуванні найпростіших оборотних перетворень для шифрування даних, була досягнута.