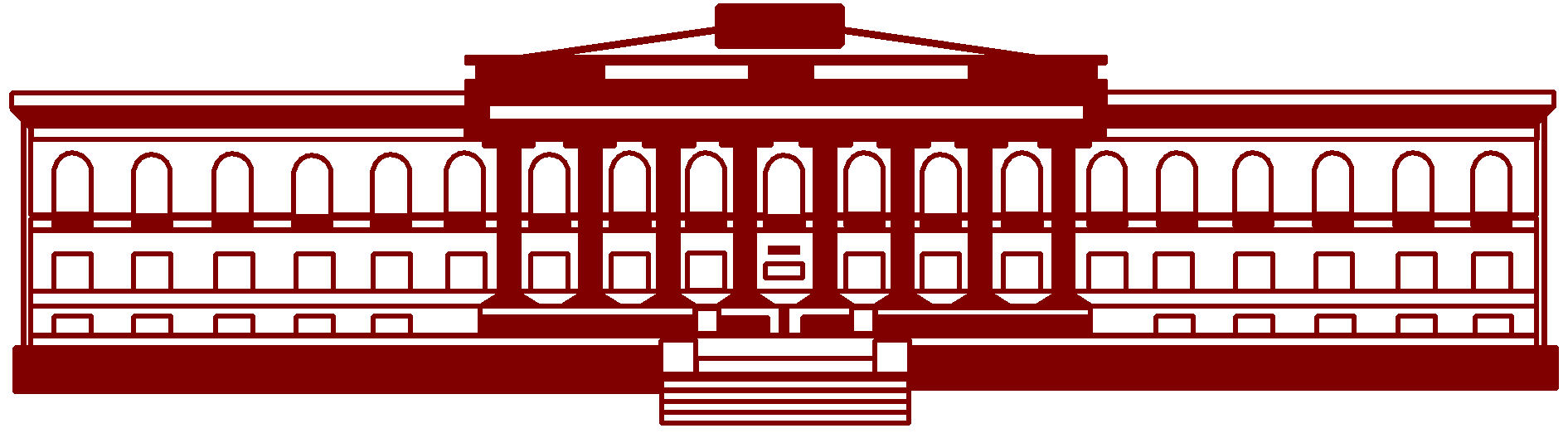
**КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ**

**імені ТАРАСА ШЕВЧЕНКА**

****

**ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ**

**Кафедра прикладних інформаційних систем**

**Звіт до лабораторної роботи №7**

**З курсу**

**«Безпека мереж і комп’ютерних систем»**

*студента 2 курсу*

*групи ПП-22*

*спеціальності 122 «Комп'ютерні науки»*

*ОП «Прикладне програмування»*

Шевлюк Вікторії Віталіївни

*Перевірив:*

д.т.н, професор

Сайко В. Г.

**Київ 2022**

**Тема:** Дослідження принципів роботи найпростіших алгоритмів шифрування (шифр Цезаря, шифрування з використанням логічної операції XOR). Криптографічний аналіз даних алгоритмів.

**Мета:** Ознайомитися з найпростішими методами криптографічного захисту інформації. Вивчити шифр Цезаря і методи його криптоаналізу. Засвоїти алгоритм шифрування за використанням логічної операції XOR.

**Завдання:**

1. Вивчити основні теоретичні положення щодо основ криптографічного захисту інформації, шифру Цезаря і алгоритму шифрування, заснованого на використанні логічної операції XOR, принципів злому даних шифрів.
2. Реалізувати програмно шифрування/дешифрування шифром Цезаря:

* алфавіт задається в тілі програми і виводиться на екран (АБВГҐДЕЄЖЗИІЇЙКЛМНОПРСТУФХЦЧШЩЬЮЯ \_.,0123456789);
* значення ключа вводиться з клавіатури;
* результат шифрування виводиться на екран і в файл «сypher1.txt».

3. Реалізувати програмно злам шифротексту, отриманого на етапі 2:

* алфавіт задається в тілі програми і виводиться на екран (АБВГҐДЕЄЖЗИІЇЙКЛМНОПРСТУФХЦЧШЩЬЮЯ \_.,);
* шифротекст вводиться з файлу «сypher1.txt»;
* величина ключа підбирається методом перебору в циклі від 1 до кількості символів у вихідному алфавіті;
* результат дешифрування виводиться на екран і в файл "open1.txt".

4. Реалізувати програмно XOR-шифрування:

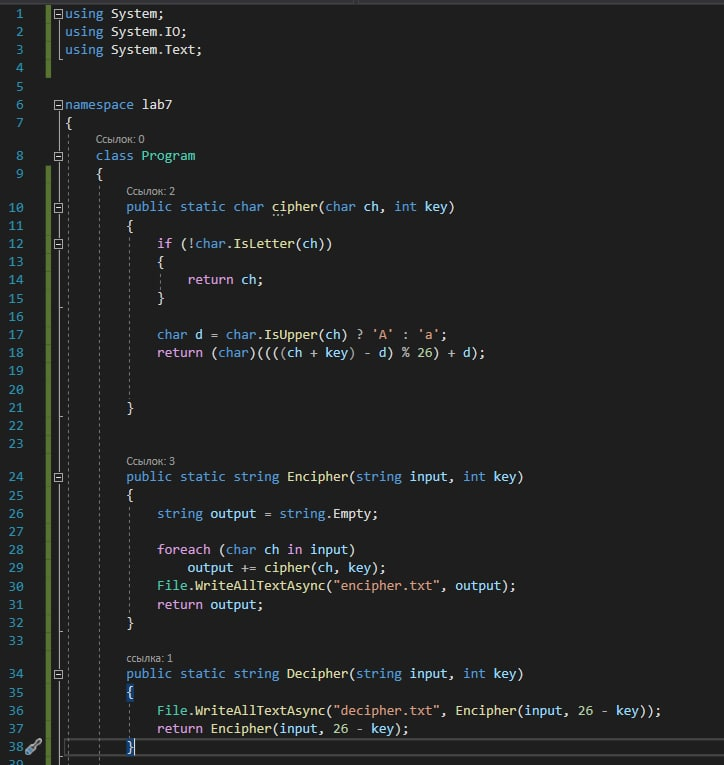
* в якості відкритого тексту взяти текст із завдання 2;
* значення ключа шифрування вводиться з клавіатури;
* результат шифрування виводиться на екран і в файл «сypher2.txt».

5. Реалізувати програмно XOR-дешифрування:

* рядок шифротексту вводиться з файлу «сypher2.txt»;
* значення ключа дешифрування вводиться з клавіатури;
* результат дешифрування виводиться на екран і в файл "open2.txt".

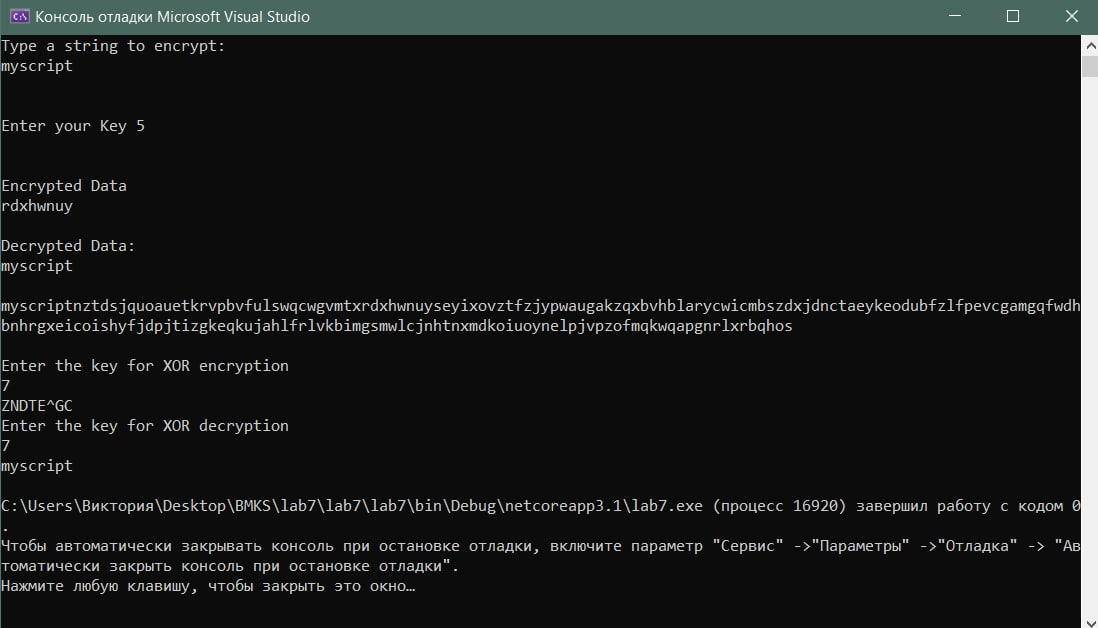
**Хід роботи:**

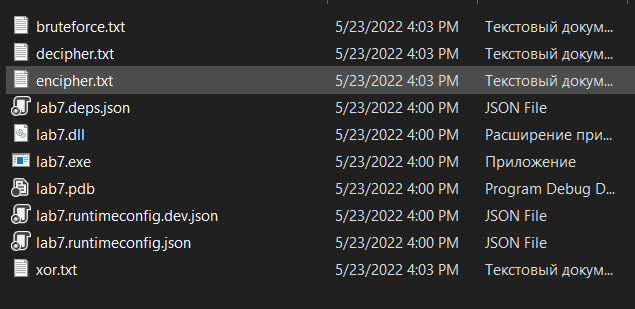
Вивчивши теоретичний матеріал та вимоги до програми, я написала наступний код, що здійснює шифруваня Цезарем і Ксором:



Результат роботи програми:





**Висновок:** у ході даної лабораторної роботи я навчилась реалізовувати шифрування Цезаря і з використанням операції Ксор. У шифрі Цезаря кожна буква алфавіту замінюється буквою, яка знаходиться на три позиції далі в цьому ж алфавіті. Якщо кожній букві призначити числовий еквівалент ( ,  і т.д.), то кожна буква відкритого тексту  замінюється буквою шифрованого тексту :



У загальному випадку зсув може бути будь-яким, тому узагальнений алгоритм Цезаря описується формулою



де  приймає значення в діапазоні від 1 до 25. Принцип дешифрування:



Якщо відомо, що певний текст був зашифрований за допомогою шифру Цезаря, то для зламу досить перевірити 25 можливих варіантів ключів.

Найпростішим і одним з найефективніших алгоритмів шифрування є так зване XOR-шифрування. Як відомо з булевої алгебри, операція логічного додавання «» по модулю 2 (або логічного виключаючого АБО - XOR, eXclusive OR) має наступну семантику:

таблиця істинності для XOR:

|  |  |  |
| --- | --- | --- |
| xi | yi | xi  yi |
| 0 | 0 | 0 |
| 0 | 1 | 1 |
| 1 | 0 | 1 |
| 1 | 1 | 0 |

тобто:

|  |  |  |
| --- | --- | --- |
| x | = | 10011101 |
|  | | |
| y | = | 01001100 |
| z | = | 11010001 |

Число  можна назвати кодуючим (або шифруючим) ключем. Дане криптографічне перетворення можна описати таким співвідношенням:

*.*

Тут  – шифротекст, а  – відповідний йому відкритий текст.

Дешифрування шифротекста за відомим ключем  згідно описаним властивостям операції XOR проводиться таким чином:

*.*

**Контрольні питання:**

1. ***Дайте визначення криптографії та криптоаналізу.***

Криптоаналіз – це наука про математичні методи забезпечення конфіденційності, цілісності і автентичності інформації.

1. ***Перерахуйте розділи криптології.***

Криптографія та криптоаналіз

1. ***Що таке алфавіт?***

Набір символів, з яких скаладається відкритий/закритий текст.

1. ***Дайте визначення поняттям закритий і відкритий текст.***

Відкритий текст - нешифроване повідомлення; закритий - шифроване

1. ***Що таке ключ?***

Секретний параметр (в ідеалі, відомий лише двом сторонам) для окремого контексту під час передачі повідомлення.

1. ***У чому полягає відмінність симетричних і асиметричних систем шифрування?***

У симетричному і відправник, і отримувач мають однаковий ключ. В асиметричному використовують пару ключів - закритий (відомий власнику) та відкритий

1. ***Що таке крипостійкість, і які її основні показники?***

Здатність криптографічного алгоритму протистояти криптоаналізу; обчислювальна складність повного перебору, виявлені слабкості

1. ***Які загальні вимоги висуваються до криптосистем?***

Число операцій, необхідних для визначення використаного ключа шифрування за фрагментом шифрованого повідомлення і відповідного йому відкритого тексту, повинно бути не менше загального числа можливих ключів.

Число операцій, необхідних для розшифрування інформації шляхом перебору всіляких ключів повинно мати строгу нижню оцінку і виходити за межі можливостей сучасних комп'ютерів (з урахуванням можливості використання мережевих обчислень).

Знання алгоритму шифрування не повинно впливати на надійність захисту.

Незначна зміна ключа повинна приводити до істотної зміни виду зашифрованого повідомлення навіть при використанні одного і того ж ключа.

Структурні елементи алгоритму шифрування повинні бути незмінними.

Додаткові біти, що вводяться в повідомлення в процесі шифрування, повинні бути повністю та надійно сховані в зашифрованому тексті.

Довжина шифрованого тексту повинна бути рівною довжині вихідного тексту.

Не повинно бути простих і легко встановлюваних залежностей між ключами, які послідовно використовуються в процесі шифрування.

Будь-який ключ з безлічі можливих повинен забезпечувати надійний захист інформації.

Алгоритм повинен допускати як програмно, так і апаратну реалізацію, при цьому зміна довжини ключа не повинно вести до якісного погіршення алгоритму шифрування.

1. ***У чому суть шифрування методом Цезаря?***

Зсув букв в повідомленні на певну кількість символів за алфавітом.

1. ***Які істотні недоліки методу Цезаря?***

Загально відомий, нестійкий

1. ***Яким чином проводиться злом методу Цезаря?***

Перебором у циклі зі зміною зсуву

1. ***У чому суть шифрування з використанням логічної операції XOR?***

