КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

ІМЕНІ ТАРАСА ШЕВЧЕНКА

ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

КАФЕДРА ІНТЕЛЕКТУАЛЬНИХ ТЕХНОЛОГІЙ

ПОЯСНЮВАЛЬНА ЗАПИСКА ДО КУРСОВОЇ РОБОТИ З ПРОЕКТУВАННЯ АЛГОРИТМІВ ТА ПРОГРАМУВАННЯ

на тему:

“Алгоритм симетричного шифрування тексту на основі шифру Цезаря”

Виконав студент 2 курсу

групи КН - ХХ

Іваненко Іван Іванович

Засвідчую, що курсовій роботі немає запозичень з праць інших авторів без відповідних посилань

_____

Керівник курсової роботи:

к.т.н., доцент Петренко Петро Петрович

_____

Оцінка за курсову роботу:

_____

Члени комісії:

_____

Київ – 20ХХ

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ТАРАСА ШЕВЧЕНКА

ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

КАФЕДРА ІНТЕЛЕКТУАЛЬНИХ ТЕХНОЛОГІЙ

ЗАВДАННЯ

на курсову роботу з проектування алгоритмів та програмування

студенту Іваненку Івану Івановичу

1. Тема роботи:

Алгоритм симетричного шифрування тексту на основі шифру Цезаря

2. Термін здачі закінченого проекту: ХХ ххххxх ХХХХ р.

3. Вихідні дані до проекту: -

4. Зміст роботи:

Розділ 1. Аналіз технології шифрування інформації.

Розділ 2. Розробка алгоритму шифрування на основі шифру Цезаря.

Розділ 3. Розробка програми шифрування на основі шифру Цезаря.

5. Перелік презентаційного матеріалу:

Тема, мета та завдання к/р (1 слайд); Поняття шифрування та дешифрування (1 слайд); Аналіз алгоритмів шифрування (1 слайд); Принципи шифрування на основі шифру Цезаря (1 слайд); Алгоритми шифрування та дешифрування на основі шифру Цезаря(2 слайди); Алгоритм головної програми (1 слайд); Тестові приклади роботи програми (2-3 слайди); Висновки (1 слайд).

6. Дата видачі завдання: ХХ ххххxх ХХХХ р.

Графік виконання курсової роботи

№	Назва етапу	Терміни	Примітки / відмітка про виконання
1	Вибір теми та керівника курсової роботи	ХХ хххх – ХХ хххх	Заява на виконання курсової роботи, що підписана студентом та керівником
2	Обговорення з керівником постановки завдання та змісту пояснювальної записки до курсової роботи	ХХ хххх – ХХ хххх	Заповнений бланк завдання на курсову роботу, що підписаний студентом та керівником роботи
3	Аналіз постановки задачі, формалізація задачі, вибір методів та засобів реалізації поставленої задачі, аналіз літературних джерел	ХХ хххх – ХХ хххх	Сформований матеріал до розділу 1 пояснювальної записки курсової роботи, оформлення списку джерел
4	*Перше узгодження з керівником*	ХХ хххх – ХХ хххх	
5	Розробка алгоритму, вибір структур даних, проектування програмного інтерфейсу з користувачем.	ХХ хххх – ХХ хххх	Сформований матеріал до розділу 2 пояснювальної
6	*Друге узгодження з керівником*	ХХ хххх – ХХ хххх	
7	Розробка та тестування програмного продукту.	ХХ хххх – ХХ хххх	Готовий програмний продукт
8	*Демонстрація базового варіанту програмного продукту. Третє узгодження з керівником*	ХХ хххх – ХХ хххх	
9	Доопрацювання програмного продукту, всебічне заключне тестування, розробка керівництва користувача.	ХХ хххх – ХХ хххх	Сформований матеріал до розділу 3 пояснювальної записки, підготовлений демонстраційний приклад роботи програми
10	Оформлення пояснювальної записки, підготовка презентації	ХХ хххх – ХХ хххх	Готова пояснювальна записка та презентація для захисту курсової роботи

Керівник роботи _____ Петро ПЕТРЕНКО

Завдання прийняв
до виконання _____ Іван ІВАНЕНКО

Зміст

Вступ

Мета роботи: побудувати алгоритм шифрування на основі шифру Цезаря, дослідити ефективність алгоритму шифрування Цезаря.

Для досягнення поставленої мети необхідно вирішити такі завдання:

- дослідити літературні джерела, що описують алгоритми шифруванн;
- розробити програмний застосунок, що реалізую шифрування та дешифрування тексту за алгоритмом Цезаря;
- провести тестування працездатності розробленої програми, проаналізувати результат роботи.

В першому розділі було наведено поняття шифрування та дешифрування інформації, розглянуто поняття симетричного та асиметричного шифрування, проаналізовано існуючі алгоритми шифрування, обрано один - шифр Цезаря - для подальшої розробки.

В другому розділі здійснено проектування алгоритму шифрування на основі шифра Цезаря. З урахуванням того, що основною вадою алгоритму шифрування Цезаря є його простота, в даній курсовій роботі було запропоновано модифікувати цей алгоритм, шляхом динамічного змінення ключа шифрування при проході кожної нової літери.

В третьому розділі розроблені алгоритми головної програми та функцій шифрування та дешифрування даних на основі модифікованого шифру Цезаря. Розроблено тестові приклади роботи програми, що доводять її працездатність.

Опис використаних засобів розробки: для виконання курсової роботи була обрана мова програмування C++, а сама розробка велась у IDE Visual Studio.

Практичне значення отриманих результатів: алгоритм шифрування може бути використаний у соціальних мережах, банківських мережах та різних телекомунікаціях.

РОЗДІЛ 1. АНАЛІЗ ТЕХНОЛОГІЇ ШИФРУВАННЯ ІНФОРМАЦІЇ

1.1 Поняття шифрування та дешифрування інформації

Шифрування — це те, що уможливлює конфіденційність даних. Без шифрування інформація потенційно може передаватися третім особам під час передачі між мережами. У першу чергу шифрування потребує великий бізнес, тому що вони мають велику базу клієнтів та користувачів, яка зберігається на серверах. Але навіть якщо дані знаходяться в захищеній інфраструктурі, все одно існує ймовірність того, що вони можуть бути скомпрометовані. Шифрування файлів може додатково захистити їх, бо не дасть їх прочитати, навіть якщо вони були вкрадені.

Шифрування – це процес перетворення вхідного (початкового) тексту у шифрований (називається також криптограмою) за допомогою деякої криптографічної системи та ключа [1].

Криптографічна система - набір криптографічних перетворень або алгоритмів, призначених для роботи в єдиному технологічному ланцюжку з метою вирішення певного завдання захисту інформаційного процесу [2].

Ключ - інформація, необхідна для шифрування та дешифрування текстів[2].

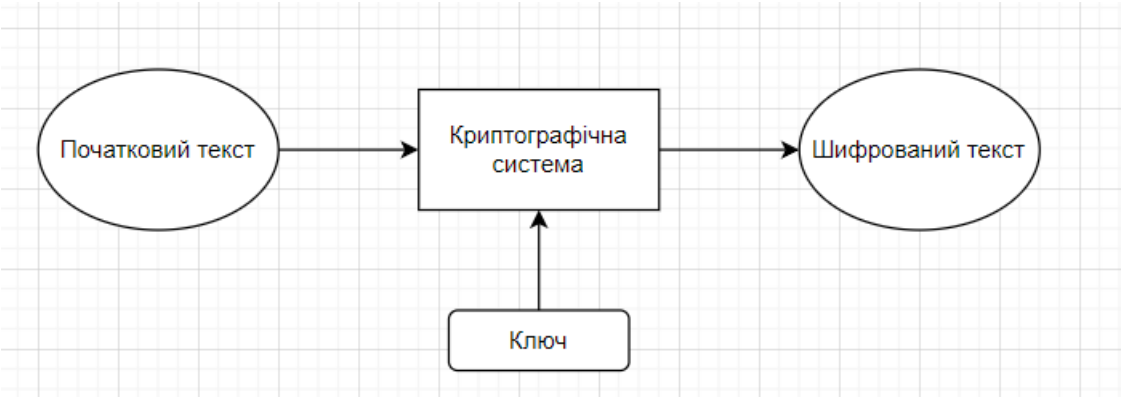

Рисунок 1.1 - Процес шифрування даних

Дешифрування - зворотний процес шифрування. На основі ключа шифрований текст перетворюється на початковий [2].

ТЕКСТ РОЗДІЛУ ПРОПУЩЕНО

1.4 Висновки до розділу 1

В результаті проведеного аналізу технології шифрування інформації в даній курсовій роботі буде застосовано криптографічну систему шифрування Цезаря, який відмінно підходить для ознайомлення з симетричним шифруванням.

РОЗДІЛ 2. РОЗРОБКА АЛГОРИТМУ ШИФРУВАННЯ НА ОСНОВІ ШИФРУ ЦЕЗАРЯ

2.1 Алгоритм шифрування тексту на основі шифру Цезаря

Шифр Цезаря - це вид шифру підстановки, в якому кожен символ у початковому тексті замінюється символом, що знаходиться на деякому постійному числі позицій ліворуч або правіше за нього в алфавіті.

ТЕКСТ РОЗДІЛУ ПРОПУЩЕНО

2.5 Висновки до розділу 2

Шифр Цезаря є зручним для реалізації, але занадто простий для дешифрування. Щоб зробити алгоритм більш стійким до дешифровки його було модифіковано шляхом динамічного змінення ключа шифрування при проході кожної нової літери.

РОЗДІЛ 3. РОЗРОБКА ПРОГРАМИ ШИФРУВАННЯ НА ОСНОВІ ШИФРУ ЦЕЗАРЯ

ТЕКСТ ПРОПУЩЕНО

3.4 Висновок до 3 розділу

Будо розроблене програмне забезпечення шифрування та дешифрування текстів з застосуванням модифікованого алгоритму шифрування Цезаря.

Було проведене тестування, яке доводить працездатність розробленої програми. За результатами проведених експериментів встановлено, що запропонований алгоритм є більш стійким до дешифровки ніж звичайний шифр Цезаря.

ВИСНОВОК

Під час виконання курсової роботи було опрацьоване поняття шифрування, шифратора, криптографічної системи, ключа, дешифратора, симетричного та асиметричного методу шифрування. Ідеєю програми було реалізувати алгоритм симетричного шифрування з використанням криптографічної системи шифру Цезаря. З урахуванням того, що основною вадою алгоритму шифрування Цезаря є його простота, було запропоновано модифікувати цей алгоритм, шляхом динамічного змінення ключа шифрування при проході кожної нової літери.

Програмний застосунок розроблений мовою C++ у середовищі IDE Visual Studio Code.

Було реалізовано консольну програму, яка обробляє заданий тест та виводить зашифрований результат. Далі на основі цього результату відпрацьовує дешифратор, який повертає початковий тест.

Розроблену програму можна застосовувати для листування у інтернеті та для роботи у корпоративних і банківських мережах, але користуватися алгоритмом Цезаря не дуже безпечно. Отже, даний алгоритм не рекомендується використовувати у сучасних мережі.

Перелік використаних джерел

1. Глинчук Л.Я. Криптологія: навч.-метод. посіб. / Людмила Ярославівна Глинчук – Луцьк: Вежа-Друк, 2014. – 164 с.
2. Тарнавський Ю. А. Технології захисту інформації [Електронний ресурс] : підручник для студентів спеціальності 122 «Комп'ютерні науки», спеціалізацій «Інформаційні технології моніторингу довкілля», «Геометричне моделювання в інформаційних системах» / Ю. А. Тарнавський ; КПІ ім. Ігоря Сікорського. – Електронні текстові дані (1 файл: 2,04 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2018. – 162 с. – Назва з екрана.
3. Holden (2017). *The Mathematics of Secrets*. Princeton University Press
4. The Code Book: The Secret History of Codes and Codebreaking. Front Cover. Simon Singh. Fourth Estate, 2000 - Ciphers - 402 pages.

Додаток А. Програмний код застосунку

```
#include<iostream>
#include <string>
using namespace std;
```

ДАЛІ ТЕКСТ ПРОПУЩЕНО