Міністерство освіти і науки України

Національний технічний університет України

Київський політехнічний інститут

Кафедра АПЕПС

Лабораторна робота №6

з курсу «Безпека програм і даних»

Виконав:

Студент групи ТВ-41

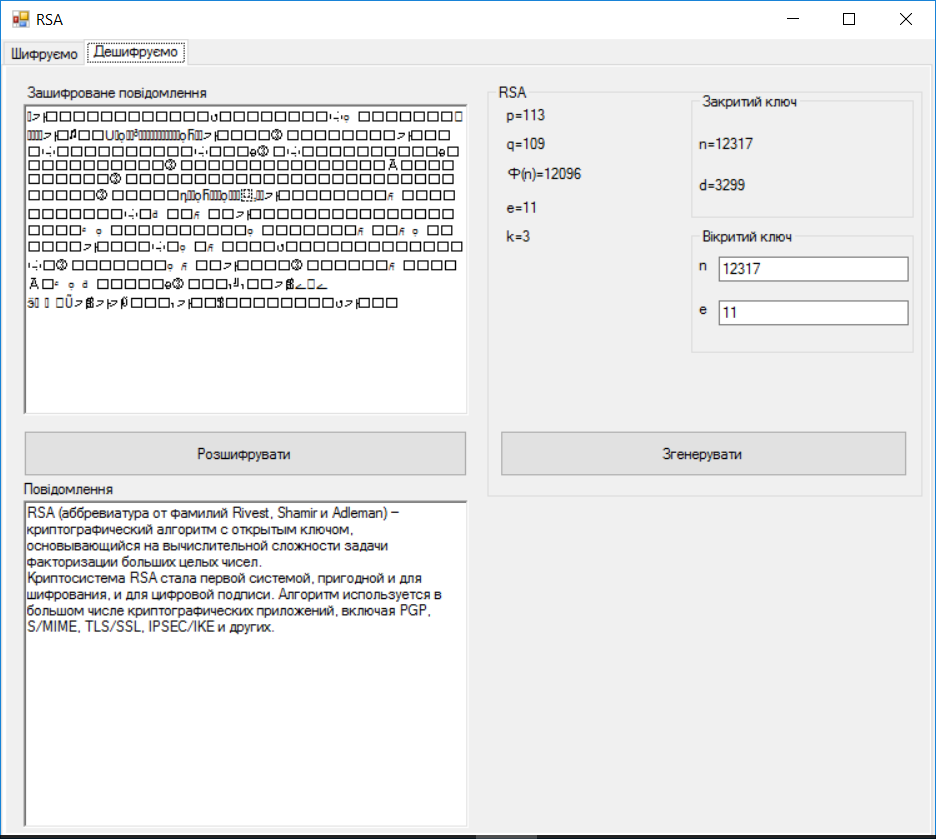
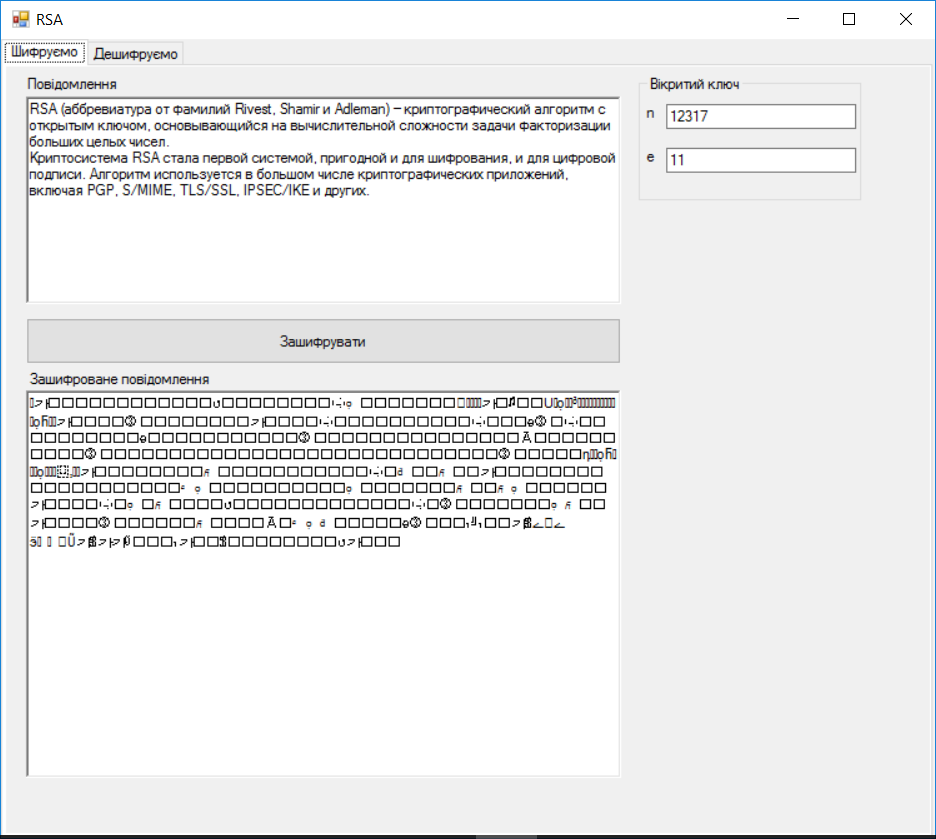
Курсенко Л. О.

Київ – 2017

**Тема:** Методи шифрування даних RSA і Діфі-Хелмана

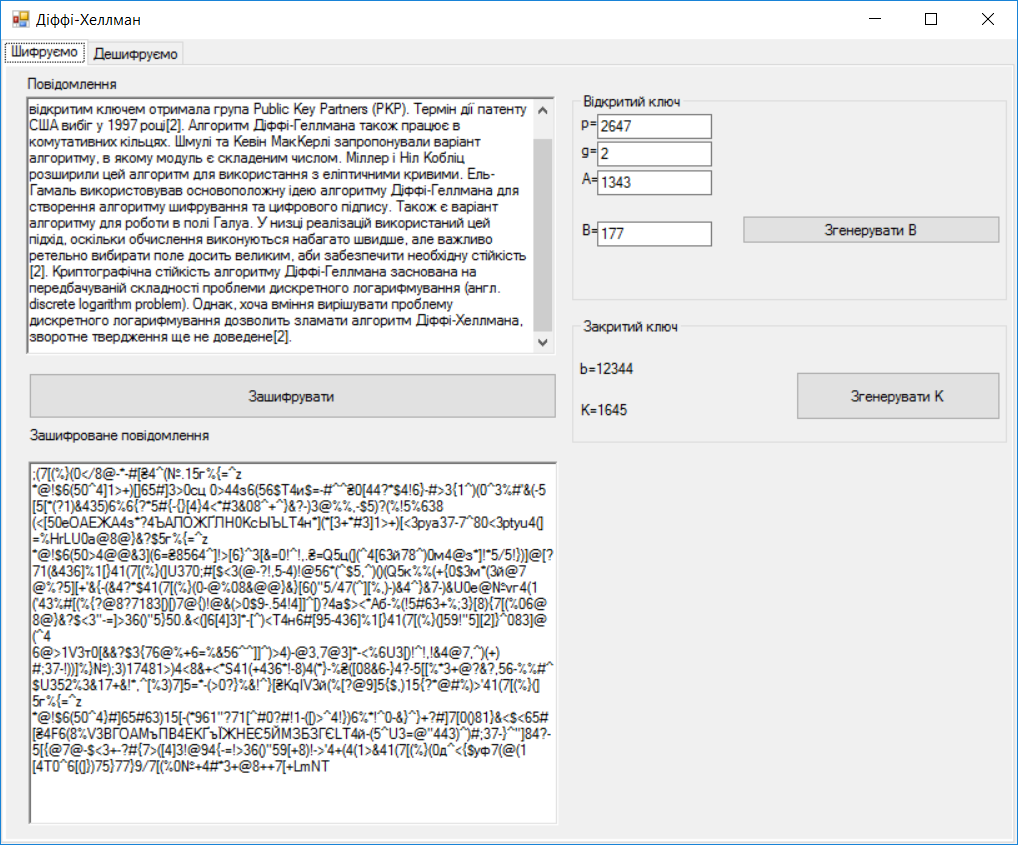
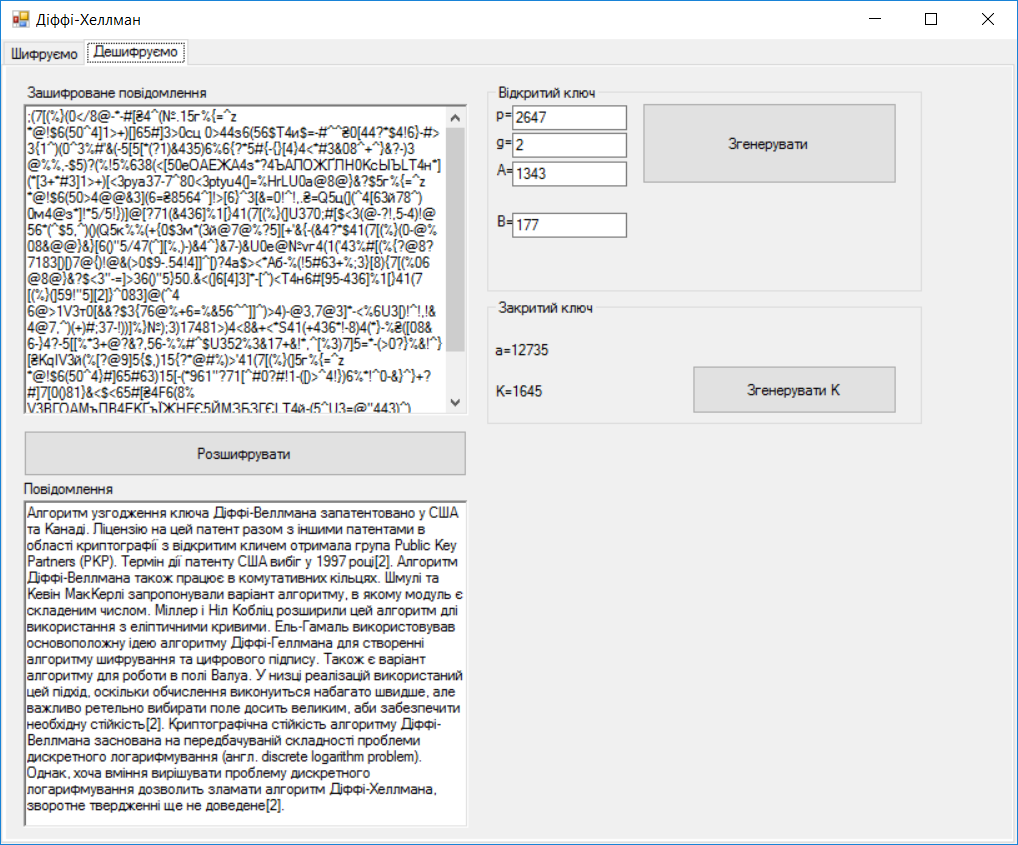
**Мета:** Реалізувати криптосистему, що шифрує дані методом шифрування даних RSA і Діфі-Хелмана.

Програма для роботи з методом асиметричного шифрування RSA.



Отримана програма дозволяє генерувати відкритий і закритий ключі, виконувати шифрування та дешифрування повідомлення.

Метод Діфі-Хелмана дозволяє отримати секретний ключ для симетричного шифрування.



Для шифрування в програмі використовується симетричний метод шифрування Віжнера.

Висновок: В результаті виконання лабораторної роботи я реалізував криптосистему, що шифрує дані методом шифрування даних RSA і Діфі-Хелмана.