Міністерство освіти і науки України

Національний технічний університет України

“Київський політехнічний інститут імені Ігоря Сікорського”

Факультет інформатики та обчислювальної техніки

Кафедра інформаційних систем та технологій

Лабораторна робота №5

Безпека інформаційних систем

«Дослідження криптосистеми Ель-Гамаль»

Виконала:

студентка групи ІА-34

Мартинюк Т.В.

Перевірила:

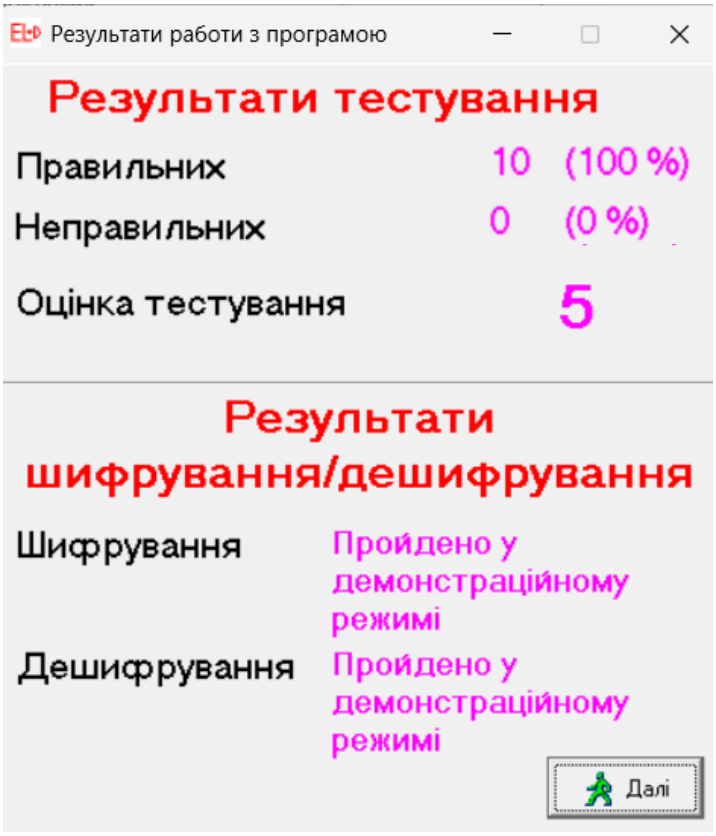
Шимкович Л. Л.

Київ – 2025

Тема: Дослідження криптосистеми Ель-Гамаль.

Хід роботи:

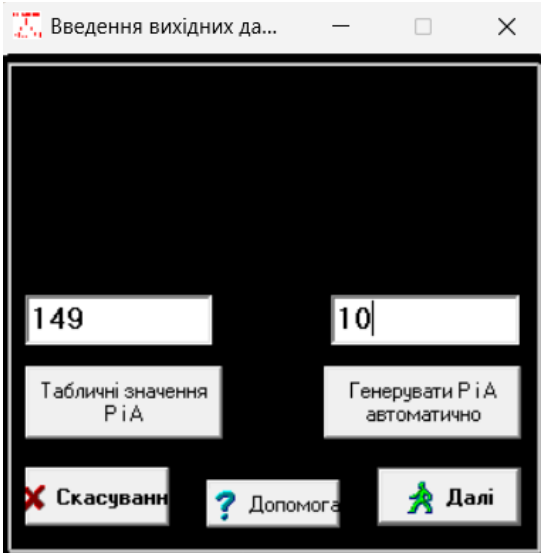
Теоретична частина:



Практична частина:

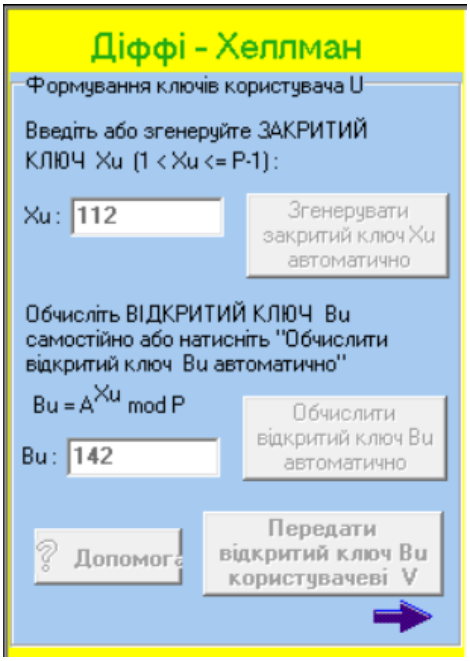
Формування ключів:

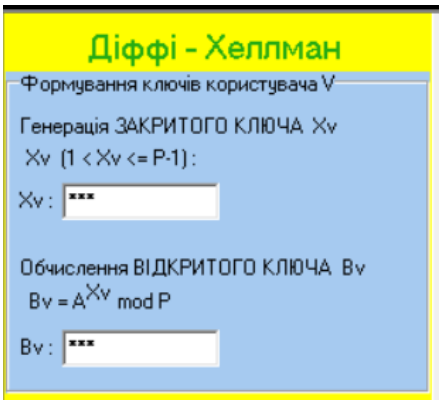
Обираємо числа P – просте число, та A – первісний елемент для P.

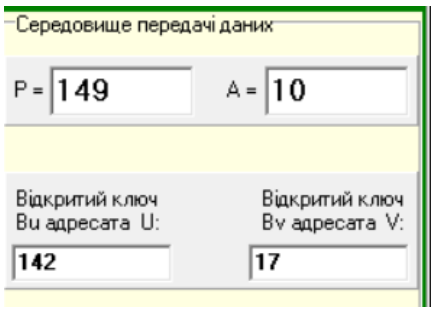


Обираємо закритий ключ X та обчислюємо публічний ключ B за формулою.

Bu = 10^112 mod 149 = 142





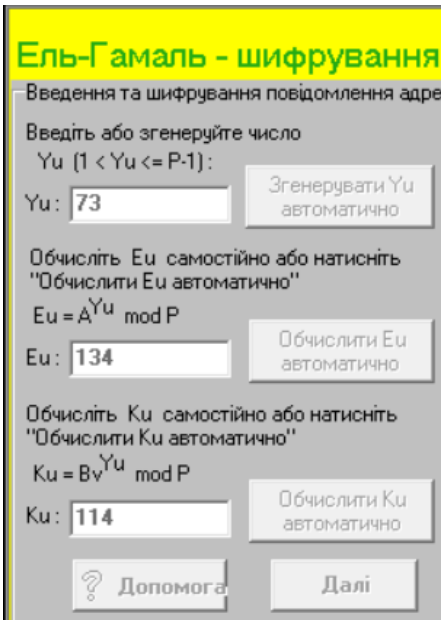


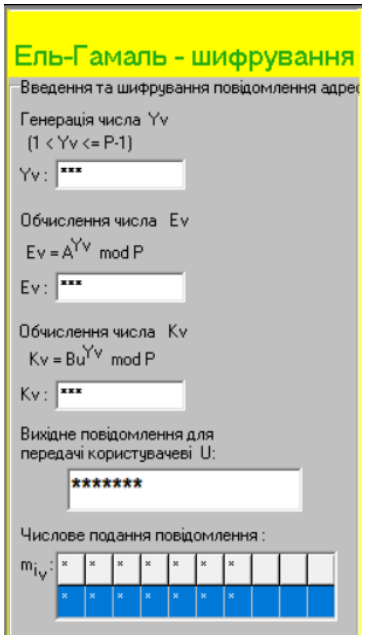
Шифрування:

Обираємо допоміжне число Y в межах від 1 до p-1. Обчислюємо число E, яке потім буде передано разом з криптограмою. Обчислюємо значення K, що безпосередньо використовується у формуванні криптограми.

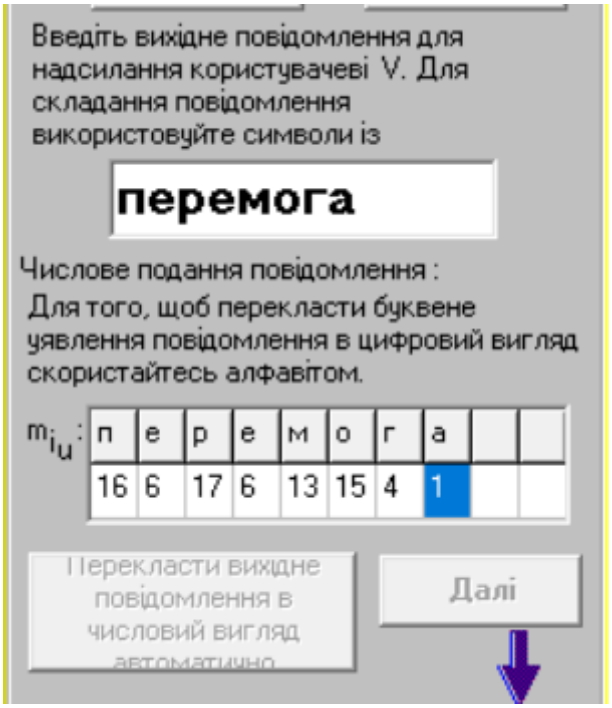
Eu = A^Yu mod P = 10^73 mod 149 = 134

Ku = Bv^Yu mod P = 17^73 mod 149 = 114

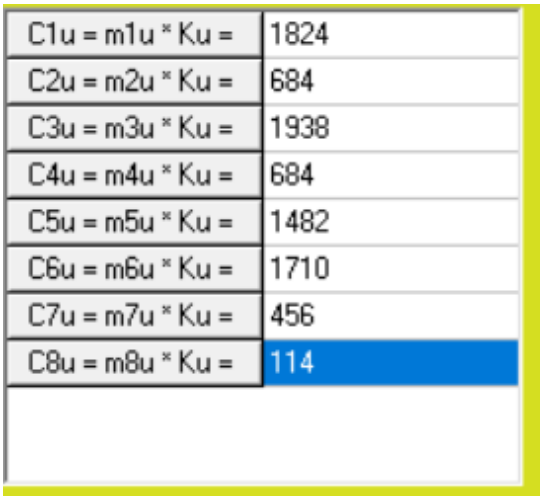


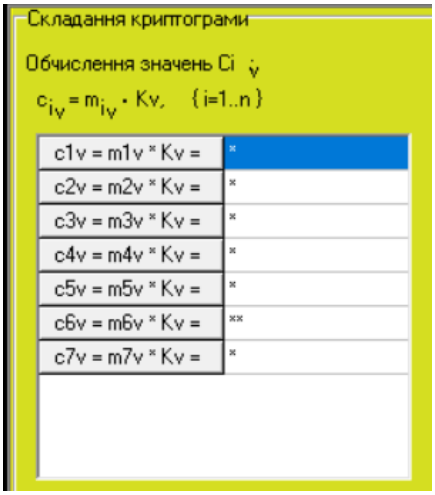


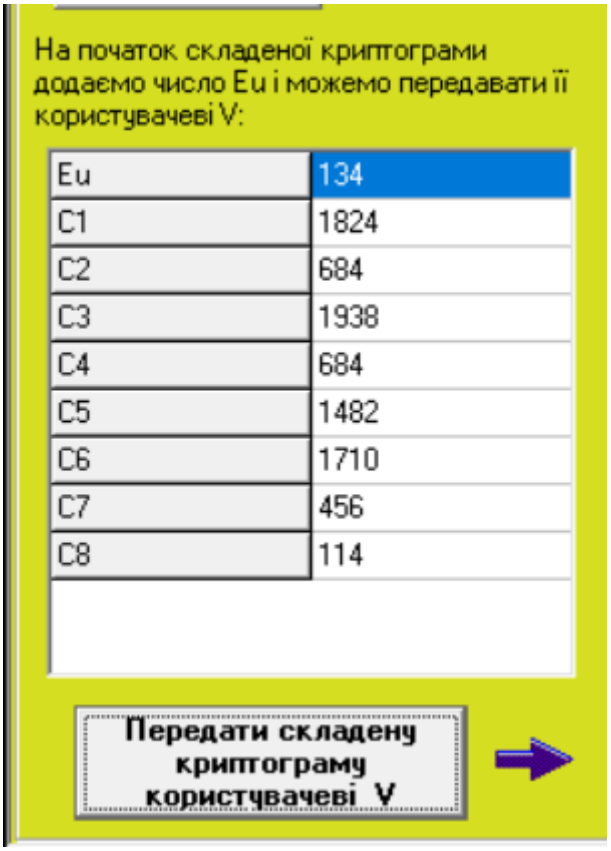
Вводимо текст повідомлення та переписуємо його у числовому представлені.

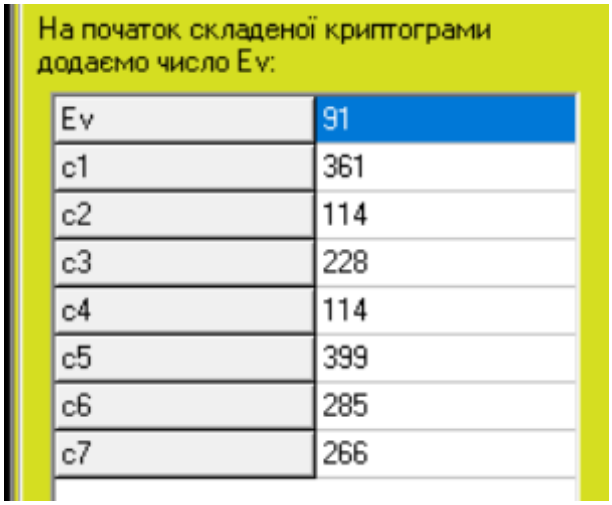


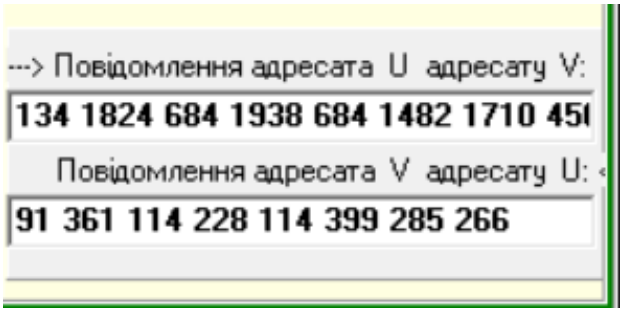
Використовуємо переписане числове представлення повідомлення та раніше обраховане значення К, обчислюємо текст криптограми. На початок вписуємо раніше обраховане значення Е та відправляємо одержувачу.





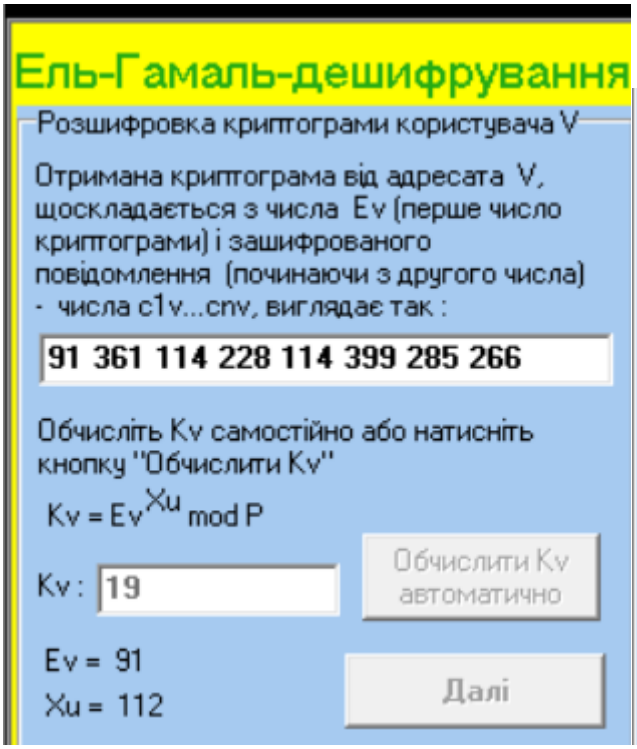




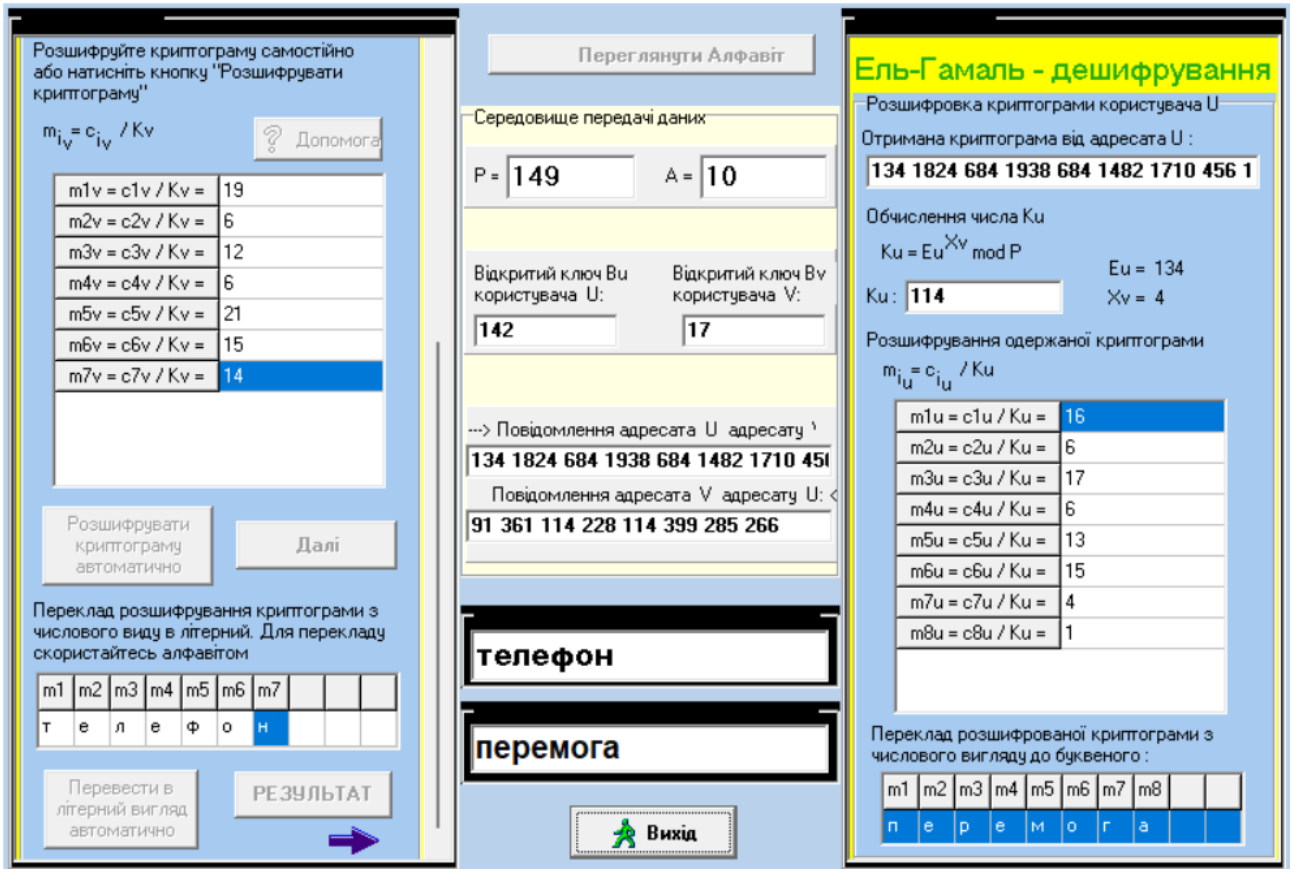


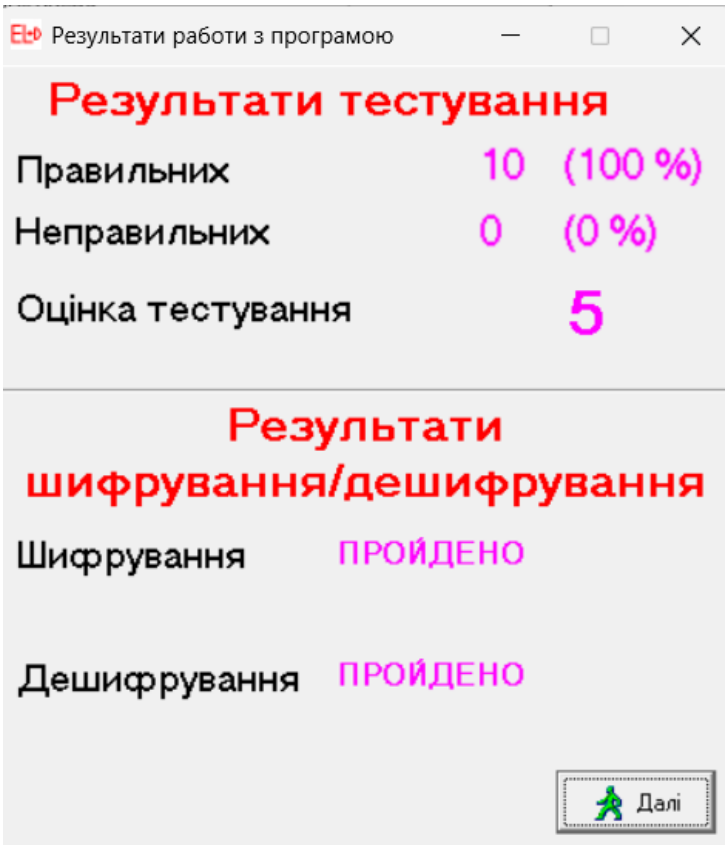
Дешифрування:

Використовуючи отримане значення E (перше число криптограми) обчислюємо значення K.



Використовуючи знайдене значення K розшифровуємо отриману криптограму. Переписуємо числове представлення повідомлення у звичайне.





Висновок: Під час виконання даної лабораторної роботи ми дослідили криптосистему Ель-Гамаль, навчились шифрувати дешифрувати дані.