Асиметрична криптографія
Лабораторна робота № 3

Криптосистема Рабіна
Атака на протокол доведення знання без розголошення

Мета
Ознайомлення із криптосистемою Рабіна та особливостям її реалізації.
Ознайомлення з криптографічними протоколами взагалі та протоколами доведення знання без розголошення зокрема. Ознайомлення із перевагами, недоліками та особливостями реалізації різних криптографічних протоколів. Аналіз наведеного протоколу; реалізація атаки на цей протокол.**Постановка задачі**
1. Самостійно підібрати текст для шифрування (2-3 кб) та ключі довжиниr= 2, 3,4, 5, а також довжини 10-20 знаків.Зашифруватиобраний відкритий текстшифромВіженера з цими ключами.
2. Підрахувати індексивідповідностіrІдлявідкритого тексту тавсіходержанихшифротекстіві порівняти їх значення.
3. Використовуючи наведені теоретичні відомості, розшифрувати наданийшифртекст(згідно свого номеру варіанта).Зокрема, необхідно:–визначити довжину ключа, використовуючи або метод індексів відповідності, абостатистику співпадіньDr(на вибір);–визначити символи ключа, прирівнюючи найчастіші літери у блоці донайчастішої літери у мові;–визначити символи ключа за допомогою функціїM(g)i;–розшифрувати текст, використовуючи знайдений ключ; в разі необхідностіскорегувати ключ

Хід роботи
Булот реалізовано шифрування, нажаль невалося релізувати розшифрування та підписи через проблему з падінгом. Проблеми з’являлися на кожному кроці, найкращий результат, що було досягнуто при розшифруванні то це розшифрування але в не те що потрібно.

Висновок
В процесі виконання цієї лабораторної роботи ми вдосконалили свої навички роботи в команді, а також дуже довго шукали помилки через які сталося проблема з розшифруванням, проте розібратися не вдалося