Лабораторна робота №2

Програмна реалізація алгоритмів шифрування RSA та Ель-Гамаля.

*Мета роботи*: створити учбовий варіант криптографічної системи з відкритим ключем на

алгоритмах RSA, Ель-Гамаля та Ель-Гамаля для еліптичних кривих.

**Завдання до роботи**

Програмна реалізація має бути оформлена як деяка програмна оболонка.

У програмній реалізації має бути розроблений інтерфейс, зручний для експлуатації програми, в інтерфейсі передбачити режим завдання параметрів системи за умовчанням і режим генерування параметрів системи. У програму включити простий алгоритм формування простих чисел і перевірки чисел на простоту. Оформити програми перевірки чисел на простоту як самостійні модулі, щоб при необхідності ці модулі можна було замінити на інші програмні реалізації.

Підготувати звіт по роботі. У звіт включити опис алгоритмів RSA та Ель-Гамаля і алгоритм перевірки чисел на простоту та Ель-Гамаля для еліптичних кривих. Підготувати для демонстрації програми контрольний приклад.

Обгрунтувати вибір типу та параметрів еліптичної кривої.

У роботу включити програми:

* формування простого числа;
* перевірки чи є число простим
* шифрування та дешифрування даних.

**Контрольні запитання**

1.Дати визначення односторонньої функції.

2.Дати визначення односторонньої функції з секретом.

3. На якій базі зазвичай створюються криптографічні системи з відкритими ключами?

4. Перерахувати число параметрів в криптографічних системах RSA та Ель-Гамаля.

5. Перерахувати секретні параметри систем RSA та Ель-Гамаля.

6. Перерахувати відкриті параметри систем RSA та Ель-Гамаля.

7. Яким умовам повинні задовольняти параметри систем RSA та Ель-Гамаля?

8. На яких математичних задачах з теорії чисел базуються алгоритми RSA та Ель-Гамаля?

9. Опишіть схему шифрування тексту з використанням алгоритмів RSA та Ель-Гамаля.

10. Опишіть схему дешифрування тексту з використанням алгоритмів RSA та Ель-Гамаля.

11. Дати визначення еліптичної кривої.