**Лабораторна робота 4**

**Програмна реализація алгоритмів ЕЦП**

**Ціль роботи** – створити програму, яка реалізує різні варіанти схем ЕЦП, використовуючи алгоритми з відкритими ключами.

**Завдання до роботи**

Реалізувати ЕЦП на базі алгоритмів Ель-Гамаля, RSA, Шнорра і Рабіна. При формуванні ЕЦП на базі алгоритма RSA використовувати результати лабораторної работи № 2. Передбачити режими формування параметрів криптосистем. Програму оформити, як інтегроване середовище із зручним інтерфейсом формування ЕЦП і її перевірки. Підготувати звіт, в який включити опис алгоритмів формування ЕЦП, опис функцій з яких складається програма. Підготувати для демонстрації контрольний приклад. При формуванні цифрового підпису передбачити схему ЕЦП з використанням хеш-функцій (див. лабораторну роботу № 3).

**Контрольні питання:**

1.Перерахувати число параметрів в криптографічній системі Ель- Гамаля.

2.Перерахувати секретні параметри системи Ель-Гамаля.

3.Перерахувати відкриті параметри системи Ель-Гамаля.

4.На якому досить важкому завданні з теорії чисел базується криптографічна система Ель-Гамаля.

5.Описати схему формування ЕЦП з використанням алгоритму Ель- Гамаля.

6.Описати схему перевірку ЕЦП з використанням алгоритму Ель- Гамаля.

7.Описати схему формування цифрового підпису з вживання алгоритму RSA.

8.Описати схему перевірки цифрового підпису вживання алгоритму RSA.

9.Що загального між звичайним і цифровим підписами? Чим вони розрізняються?

10.Які завдання дозволяє вирішити цифровий підпис?

11.У чому полягає принципова складність в практичному вживанні систем цифрового підпису?

12.Чому в криптографічних системах, заснованих на відкритих ключах, не можна використовувати для шифрування і цифрового підпису?

13.Перевірити, що вказаний в тексті спосіб підбору підписаних повідомлень для схеми Ель-Гамаля дійсно дає вірні цифрові підписи.