Лабораторна робота №5
Асиметричні криптосистеми. Електронний цифровий підпис.

Студнти із непарними номерами у списку групи пишуть 1 варіант,
з парними – 2 варіант.

Варіант 1. Асиметрична криптосистема RSA. Цифровий підпис Ель-Гамаля.

1. Створити криптографічну систему на основі алгоритму RSA. Програма повинна генерувати два великих випадкових простих числа *p і q*, обчислювати *E і D*.
2. Система шифрування повинна задовольняти наступним вимогам: 1) читати з текстового файлу відкрите повідомлення; 2) шифрувати повідомлення за допомогою ключа *n*, *E*; Результат записувати у файл.
3. Створити цифровий підпис. Програма повинна: 1) генерувати велике випадкове просте число *p* та *g* – первісний корінь за модулем *p*, генерувати закритий ключ та обчислювати *h.* 2) обчислювати хеш повідомлення 3) обчислювати цифровий підпис знайденого хешу і записувати його значення у файл.
4. Створити систему перевірки цифрового підпису. Система повинна задовольняти таким вимогам: 1) читати з текстового файлу зашифроване повідомлення та цифровий підпис; 2) розшифровувати повідомлення за допомогою таємного ключа *D* і знаходити хеш повідомлення; 3) проводити верифікацію (перевірку) цифрового підпису; 4) робити висновок про істинність отриманого повідомлення і цифрового підпису.

Варіант 2. Асиметрична криптосистема Ель-Гамаля. Цифровий підпис RSA.

1. Створити криптографічну систему на основі алгоритму Ель-Гамаля. Програма повинна генерувати велике випадкове просте число *p* та *g* – первісний корінь за модулем *p*. Генерувати закритий ключ. Обчислити решту відкритих параметрів алгоритму (*h*).
2. Система шифрування повинна задовольняти наступним вимогам: 1) читати з текстового файлу відкрите повідомлення; 2) шифрувати повідомлення за допомогою відкритого ключа *p*, *g, h*; Результат записувати у файл.
3. Створити цифровий підпис. Програма повинна: 1) генерувати два великих випадкових простих числа *p i q*, обчислювати *E i D;* 2) обчислювати хеш повідомлення; 3) обчислювати цифровий підпис знайденого хешу і записувати його значення у файл.
4. Створити систему перевірки цифрового підпису. Система повинна задовольняти таким вимогам: 1) читати з текстового файлу зашифроване повідомлення та цифровий підпис; 2) розшифровувати повідомлення за допомогою таємного ключа *a* і знаходити хеш повідомлення; 3) проводити верифікацію (перевірку) цифрового підпису; 4) робити висновок про істинність отриманого повідомлення і цифрового підпису.