**Лабораторна робота 5**

**Програмна реалізація криптографічних протоколів**

**Мета роботи** – ознайомиться з криптографічними протоколами, які в даний час широко використовуються для забезпечення інформаційної безпеки. Освоїти основні поняття, які пов'язані з криптографічними протоколами.

**Завдання до роботи**

Реалізувати два прості протоколи. Протокол Діффі-Хелмана формування загального ключа і протокол підкидання монети. Підготувати звіт. У звіті дати алгоритми протоколів і описати їх програмні реалізації. Підготувати для демонстрації учбові варіанти контрольних прикладів, які моделюють роботу з використанням криптографічних протоколів.

**Теоретичний матеріал**

**Схема Діффі-Хеллмана**

**Протокол формування загального ключа по відкритому каналу зв'язку**

1. Є два користувачі (абонента) A і B.

2. Дано просте число p, яке відоме користувачам A і B.

3. Вибирається загальне число g, g < p-1.

4. Абоненти A і B незалежно один від одного вибирають відповідно секретні ключі а, 0 < а < p-1 і b, 0 < b < p-1.

5. Абонент A посилає абонентові B повідомлення

.

6. Абонент B посилає абонентові A повідомлення

.

7. Абонент A обчислює загальний ключ

*.*

8. Абонент B обчислює загальний ключ

.

**Протокол взаємної аутентифікації**

Існує декілька схем аутентифікації джерела даних ([1],[7]).Приведемо умови і алгоритм реалізації однієї з них.

1. Дано двох абонентів A і B.

2. Дани просте число p і число *g, g<p-1*, які відомі абонентам *A і B*.

3. Абоненти A і B володіють відповідно відкритими функціями шифруваннz і закритими функціями де шифрування , які володіють властивостями

*,*

де М-код –передаване повідомлення. Відзначимо, що рівність не залежить від порядку вживання функцій*.*

4. Абоненти A і B незалежно один від одного вибирають відповідно секретні ключі а, 0 < а < p-1 і b, 0 < b < p-1.

5. Абонент A посилає абонентові B повідомлення

*.*

*6.* Абонент B

• обчислює загальний ключ

;

• використовуючи закриту функцію , створює підпис (повідомлення)

;

• використовуючи ключ до, шифрує підпис

де загальна функція шифрування;

• відправляє абонентові A повідомлення

7. Абонент A

• обчислює загальний ключ

;

• використовуючи закриту функцію DA, створює підпис (повідомлення)

;

• використовуючи ключ до, шифрує підпис

;

• відправляє абонентові B повідомлення

• перевіряє підпис B, обчислюючи

де - загальна функція дешифровки.

8. Абонент B перевіряє підпис A, обчислюючи

.

**Контрольні питання**

1.Дати визначення протоколу.

2.Перерахувати завдання захисту інформації, в яких використовуються криптографічні протоколи.

3.Способи класифікації криптографічних протоколів.

4.Класифікація криптографічних протоколів за функціональним призначенням.

5.Призначення протоколу аутентифікації повідомлень.

6.Призначення протоколу ідентифікації.

7.Призначення протоколу обміну секретами.

8.Перерахувати основні види атак на протоколи*.*