План лабораторного заняття № 8
Тема № 3 “Безпека в інформаційних мережах”

Навчальний час: 3 год.

Міжпредметні зв’язки: навчальна дисципліна “Захист інформації в інформаційних системах” взаємопов’язана з такими дисциплінами як “Економіко-математичне моделювання”, “Інформатика” та ін.

Мета і завдання лабораторного заняття: ознайомлення з методами шифрування шифрування та дешифрування інформації.

Питання для перевірки базових знань за темою лабораторного заняття:

1. Що таке відкритий ключ?
2. Який ключ називають закритим?
3. Чи існує потреба у захищеному каналі при передачі повідомлення, що зашифроване асиметричним методом?
4. Опишіть принцип роботи асиметричного методу шифрування.
5. Які основні приклади криптосистем з відкритим ключем Ви знаєте?
6. У якому випадку використовується метод Діффі-Геллмана. У чому його особливість, недоліки?
7. Опишіть послідовність дій при використанні алгоритму Діффі-Геллмана.
8. Що таке керування ключами? Для чого воно використовується?

Завдання: ознайомлення з асиметричним методом шифрування (обмін секретним ключем за методом Діффі-Геллмана).

1) Автоматизувати обмін секретним ключем за методом Діффі-Геллмана.

1) Обчислити закриті ключі Y1, Y2 та загальний ключ Z для системи Діффі-Геллмана з параметрами A=3, P=7, X1=3, X2=6.

2) Обчислити закриті ключі Y1, Y2 та загальний ключ Z для системи Діффі-Геллмана з параметрами A=2, P= 21024, X1=12345, X2=654323.

3) Обчислити закриті ключі Y1, Y2 та загальний ключ Z для системи Діффі-Геллмана з параметрами A=5, P= 2786, X1=45376, X2=34567.

4) Обчислити закриті ключі Y1, Y2 та загальний ключ Z для системи Діффі-Геллмана з параметрами A=6, P= 3456, X1=6547, X2=34538.

Хід виконання лабораторної роботи:

Асиметричний криптографічний метод передбачає використання двох ключів: один – для шифрування даних, а для розшифровування – інший ключ. Перший ключ є відкритим і може бути опублікованим для використання усіма користувачами системи, які шифрують дані. Розшифровування даних за допомогою відкритого ключа неможливе. Для розшифровування даних одержувач зашифрованої інформації використовує другий ключ, який є секретним (закритим).

Перевагою асиметричного методу шифрування є те, що він забезпечує більш високий рівень захищеності даних. На відміну від симетричного методу шифрування, при асиметричному методі немає необхідності відправнику повідомлення та його одержувачу здійснювати передачу секретного ключа по спеціально захищеному каналу зв’язку. Захист інформації забезпечується використанням пари ключів:

- відкритого ключа (public key) для кодування (шифрування) даних;

- закритого (private key), що використовується виключно для розшифровування повідомлень, що були закодовані відкритим ключем.

Користувач поширює тільки свій відкритий ключ. Проте закритий тримає в таємниці. Якщо хтось відправить Адресатові повідомлення, з яким має ознайомитись тільки він, то відправник шифрує своє повідомлення відкритими ключем Адресата. Після чого відправляє зашифроване повідомлення будь-яким способом Адресатові. Прочитати зашифроване повідомлення неможливо. Його треба спочатку розшифрувати. Це можливо тільки закритим ключем, який є тільки у Адресата. Звідси, якщо хтось отримує повідомлення, прочитати його не зможе.
Адресат, отримавши повідомлення, розшифровує його приватним ключем. Якій є тільки в нього.

Асиметричний метод шифрування передбачає, що вираховування закритого ключа з відкритого є надто ускладненим процесом, а отже, дані при передачі повідомлення є надійно захищеними.

Прикладами криптосистем з відкритим ключем є схема Ель-Гамаля , RSA, Діффі-Геллмана і DSA.

Криптографічний стійкість алгоритму Діффі-Геллмана заснована на складності проблеми дискретного логарифмування.

Для захисту даних у схемах з використанням алгоритму Діффі-Геллмана використовують додаткові методи односторонньої або двосторонньої аутентифікації.

Розглянемо алгоритм передачі секретного ключа за методом Діффі-Геллмана:
1) нехай маємо два числа v=3 та n=19;
2) перша особа обирає випадкове ціле число x=3;
3) друга особа, яка бере участь в обміні секретним ключем, обирає випадкове число 4;
4) перша особа обчислює значення $v_x \bmod n = 3_3 \bmod 19 = 27 \bmod 19 = 8$ та повідомляє його другій особі;
5) друга особа обчислює значення $v_y \bmod n = 3_4 \bmod 19 = 5$ та повідомляє його першій особі;
6) перша особа обчислює значення $5_3 \bmod 19 = 11$;
7) друга особа обчислює значення $8_4 \bmod 19 = 11$.
Отже, отримане значення і є шуканим секретним ключем, який і був згенерований першою та другою особою спільно.

Додаткові завдання для студентів: опрацювання теоретичного матеріалу теми, написати план-конспект заняття за вибраною темою із використанням демонстраційного матеріалу.

Форми контролю знань – презентація виконаних завдань, обговорення виконаних завдань.

Рекомендована література до теми лабораторного заняття:
Основна та допоміжна література:

1. Харин Ю.С. Математические основы криптологии: учеб.пособ. / Ю.С.Харин, В.И.Берник, Г.В.Матвеев. – Мн.: БГУ, 1999. – 319 с.
2. Зима В. Безопасность глобальных сетевых технологий / В.Зима, А.Молдован, Н.Молдован. – СПб.: БХВ-Петербург, 2003. – 368 с.
3. Щербаков А. Прикладная криптография / А. Щербаков, А.Домашев. – М., 2003. – 404 с.
4. Пономаренко Н.Н. Защита информации в телекоммуникационных системах: учеб. пособ. / Н. Н. Пономаренко. – Х.: Нац. аэрокосм. ун-т им. Н.Е. Жуковского «Харьк.авиац.ин-т», 2015. – 40 с.
5. Алферов А.П. Основы криптографии: учеб. пособ. / А.П.Алферов, А.Ю.Зубов, А.С.Кузьмин,
6. А.В.Черемушкин. – М.: Гелиос АРВ, 2002 – 480 с.
7. Басалова Г.В. Основы криптографии / Г.В. Басалова. – М.: Национальный Открытый Университет "ИНТУИТ", 2016. – 283 с. URL: https://www.twirpx.com/file/1907188/

8. Воробьев С.П., Орловский Н.М. Зашита информации: учеб. пособ. / С.П,Воробьев, Н.М.Орловский. ЮРГПУ (НПИ) им. М.И. Платова.– Новочеркасск: ЮРГПУ(НПИ), 2015.– 27 с.

Інтернет-ресурси:
https://books.ifmo.ru/file/pdf/56.pdf
http://booksshare.net/index.php?id1=4&category=cryptography&author=alferov-ap&book=2002

Обладнання заняття, ТЗН тощо: комп'ютери.