Практичне заняття №3. Створення програмної реалізації простих алгоритмів шифрування

8.1 Мета заняття

Опрацювати навички з використання простих алгоритмів шифрування для застосування в практичних цілях, створення програмної реалізації одного з простих алгоритмів шифрування і знайомство з методами криптоаналізу або створенням захищеного каналу передачі даних.

8.2 Завдання для виконання

Для виконання даного практичного заняття вам знадобитися вибрати одне з наступних завдань і виконати його. Допускається використання будь-яких мов програмування. Потрібно об'єднання в бригади по дві людини.

Завдання 1

1. Реалізація шифру "одноразовий блокнот" в варіанті розглянутому в попередньому практичному занятті.
2. Усунення всіх помилок допущених в описі алгоритму
3. Створення двох додатків, здатних обмінюватися по мережі зашифрованими повідомленнями

Завдання 2

1. Використовувати бібліотеку реалізовує шифр "одноразовий блокнот" для реалізації програми здатної проводити шифрування і дешифрування повідомлень користувача
2. Додати в програму можливість відправки повідомлень електронної пошти з зашифрованими повідомленнями користувача
3. Додати в програму функцію прийому повідомлень електронної пошти і дешифрування їх вмісту

Завдання 3

1. Реалізувати шифр цезаря програмно
2. Реалізувати атаку на зашифрований текст

Завдання 4

1. Програмно реалізувати алгоритм розглянутий на минулому практичному занятті.
2. Реалізувати атаку на текст зашифрований реалізованим алгоритмом

8.3 Захист практичного завдання

Захист практичного завдання проводиться індивідуально або бригадою у складі двох студентів. Викладачу надається звіт та студент відповідає на теоретичні запитання в особистій бесіді.

Звіт включає в себе:

- мета практичного заняття;
- індивідуальне завдання;
- хід його вирішення;
- результат виконання;
- висновки.

8.4 Контрольні питання

1. Що таке атака (криптоаналіз)?
2. Які вимоги існують до основних методів криптоаналізу, опишіть їх?
3. Опишіть алгоритм Цезаря.
4. Опишіть алгоритм «одноразовий блокнот».
5. Опишіть використання методу повного перебору для атаки на алгоритм Цезаря.

Чому повний перебір не використовується при атаці на алгоритм шифрування «одноразовий блокнот»?