МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет кібербезпеки, комп’ютерної та програмної інженерії

Кафедра інженерії програмного забезпечення



Лабораторна робота №1

з дисципліни «Безпека ПД»

На тему: «Симетричні системи шифрування»

Варіант №5

Виконав студент:

групи ПІ-421Б

Іванюк Н. О.

Перевірив викладач:

Радішевський М. Ф.

Київ 2022

**Порядок виконання роботи**

**Завдання 1.** Зашифрувати фразу, яка складається з прізвища студента та дати народження. Ключ вибрати рівний порядковому номеру студента в списку групи. Процес шифрування представити у вигляді таблиці 1. Результат шифрування та ключ передати викладачу для розшифровки іншим студентом у вигляді окремого файлу. Ім’я файлу складається з 3-х перших букв прізвища, імені та по батькові та ключа шифрування. Приклад: НФР\_14.

**Завдання 2.** Розшифрувати текст, виданий викладачем, по заданому ключу. Процес шифрування представити у вигляді подібному таблиці 1.

**Завдання 3.** Зашифрувати фразу, яка складається з прізвища матері студента та дати її народження. Символьний ключ вибрати самостійно, бажано довше фрази, яка шифрується. Процес шифрування представити у вигляді таблиці 3. Результат шифрування та ключ передати викладачу для розшифровки іншим студентом у вигляді окремого файлу. До імені файлу завдання 1 додати літеру Б. Приклад НФР\_14\_Б.

**Завдання 4.** Розшифрувати текст, виданий викладачем, по заданому ключу. Процес шифрування представити у вигляді подібному таблиці 3.

**Виконання**

Завдання 1.

Завдання 1 було розділене на 2 частини і вкладено до файлів *ІНО\_5.docx* та *Зашифрована\_фраза\_Завдання1.txt*, виконання завдання та рішення відповідно.

Завдання 3.

Завдання 3 було розділене на 2 частини і вкладено до файлів *ІНО\_5\_Б.docx* та *Зашифрована\_фраза\_Завдання3.txt*, виконання завдання та рішення відповідно.

**Висновок:** Під час виконання лабораторної роботи вивчив симетричні системи шифрування, а саме простої підстановки та багато-абеткову систему шифрування. Також здобув практичний досвід в шифруванні даних цими системами. Дав відповіді на такі контрольні запитання:

**Контрольні питання**

1. Чому система шифрування зветься симетричною?

2. Як підрахувати кількість ймовірних ключів в системі шифрування з простою підстановкою?

3. Що треба робити, якщо сума номера букви та ключа більше розміру абетки.

4. Які недоліки метода простої підстановки усуває багато-абеткова система шифрування?

**Відповіді на контрольні запитання:**

Запитання 1: Системи шифрування називаються симетричними тому, що для їх шифрування і дешифрування використовується один і той же ключ.

Запитання 2: Для підрахування кількості ймовірних ключів в системі шифрування з простою підстановкою достатньо скористатися формулою . *Див примітка 1*

Запитання 3: Для того щоб вирішити проблему де сума номера букви та ключа більше розміру абетки достаньо від цієї суми відняти N.

Запитання 4: Недоліком простої підстановки є сильно обмежена кількість ключів які дорівнюють N-1. Багато-абеткова система шифрування усуває цю проблему таким чином що для кожного символу шифрованої фрази існує свій ключ, тобто збільшуючи кількість можливих ключів.

**Примітки :**

1. N- це розмір абетки (кількість різних символів в абетці).