Навчально-науковий інститут інформаційних технологій
Харківський національний економічний університет
імені Семена Кузнеця

Звіт
З Виконання лабораторної роботи №8
за дисципліною: “Основи стеганографічного захисту інформації”

Виконав: студент кафедри
Кібербезпеки та інформаційних
технологій
4 курсу, спец. Кібербезпека,
групи 6.04.125.010.21.2
Бойко Вадим Віталійович
Перевірила:
Венгріна Олена Сергіївна

ХНЕУ ім. С. Кузнеця
2024

Мета роботи: Метою лабораторної роботи було вивчення методів приховування даних у текстових файлах за допомогою MathCAD. Зокрема, необхідно було набути навичок розробки алгоритмів для впровадження прихованих повідомлень у текстові документи з використанням пробілів та інших прийомів стеганографії

Хід роботи:

1. Для виконання лабораторної роботи було встановлено MathCAD із функціями для роботи з текстовими файлами.

Використовувався текстовий файл формату TXT, який містив достатній обсяг тексту для приховування повідомлення. Повідомлення "Hello World" було закодоване у двійкову форму.

2. Реалізація методу приховування повідомлення

Читання текстового файлу: Завантажено вміст файлу у вигляді рядка за допомогою функції READ_TEXT.

```
text_data := READ_TEXT("textfile.txt")
```

Підготовка прихованого повідомлення: Повідомлення "Hello World" було перетворено у двійковий код для впровадження у текст.

```
message := "Hello World"
binary_message := JOIN(DEC2BIN(ASC(message)), "")
```

Впровадження даних за допомогою пробілів: Додаткові пробіли в кінці рядків позначали "1", а їхня відсутність - "0".

```
modified_text := ""
FOR i IN 0..LENGTH(binary_message)-1 LOOP
  IF binary_message[i] = "1" THEN
    modified_text := modified_text & text_data[i] & " "
  ELSE
    modified_text := modified_text & text_data[i]
  END IF
END LOOP
```

Запис зміненого тексту у новий файл: Змінений текст записано до файлу modified_textfile.txt.

WRITE_TEXT("modified_textfile.txt", modified_text)

3. Реалізація функції вилучення прихованого повідомлення

Читання зміненого текстового файлу: Текст завантажено для аналізу прихованого повідомлення.

modified_text_data := READ_TEXT("modified_textfile.txt")

Вилучення прихованих даних: Визначення "1" або "0" базувалося на наявності або відсутності пробілів у кінці рядків.

```
extracted_bits := ""
FOR i IN 0..LENGTH(modified_text_data)-1 LOOP
  IF RIGHT(modified_text_data[i], 1) = " " THEN
    extracted_bits := extracted_bits & "1"
  ELSE
    extracted_bits := extracted_bits & "0"
  END IF
END LOOP
```

Відновлення повідомлення: Отримані біти було перетворено назад у текст.

extracted_message := BIN2CHAR(SPLIT(extracted_bits, 8))

4. Аналіз читаємості тексту

Візуальна перевірка: Текст після впровадження змін мав незначні відмінності, які були непомітними при звичайному перегляді.

Оцінка стійкості повідомлення: Метод вразливий до виявлення зайвих пробілів, особливо автоматичними інструментами. Рекомендується використовувати складніші методи, наприклад, невидимі символи Unicode.

Висновки

Аналіз якості: Приховане повідомлення не погіршило читаємість тексту.

Стійкість повідомлення: Метод із пробілами є простим, але вразливим до виявлення та видалення.

Рекомендації: Використання складніших методів (Unicode, шифрування) підвищить стійкість прихованих даних.

Відповіді на контрольні питання

Переваги та недоліки методу пробілів: Простота у реалізації є перевагою; низька стійкість до виявлення та форматування – недоліком.

Інші методи приховування: Невидимі символи, модифікація пунктуації, символи Unicode.

Захист від виявлення: Шифрування та комбінування методів підвищують захист.

Загальний висновок

Лабораторна робота продемонструвала основи текстової стеганографії та практичний досвід приховування й вилучення даних у MathCAD. Метод із пробілами простий у виконанні, але має обмежену стійкість, що обмежує його ефективність у складних сценаріях.