ІНДИВІДУАЛЬНЕ ДОСЛІДНИЦЬКЕ ЗАВДАННЯ

Тема: «Знайомство та програмна реалізація системи шифрування тексту з використанням алгоритмів блокового шифрування …». Алгоритм обирається зі списку.

Метою індивідуальної роботи є знайомство студентів з принципами роботи сучасних алгоритмів блочного шифрування та проблемами, пов'язаними з їх програмною реалізацією.

Середовищем розробки індивідуальної роботи є будь-яке інструментальне середовище, що здатне створювати виконавчі модулі для операційних систем (MS-DOS, Widows, Linux), та у якості вхідної мови програмування використовує мови високого рівня, що дозволить здійснити перевірку на базі комп. парку ЗНУ.

Звіт з виконання індивідуальної роботи складається з двох складових:

1. Програмна система (включаючи всі необхідні файли).
2. Пояснювальна записка (звіт)
3. Презентація (у форматі Microsoft Power Point) обраного алгоритму блокового шифрування.

Пояснювальна записка (звіт) повинна бути представлена в електронному та друкованому (для очної форми навчання) варіантах.

Вимоги до друкованого варіанту:

1. Пояснювальна записка друкується на листах формату А4 з однієї сторони.
2. Параметри сторінки:
   - Ліве поле — 2.5 сантиметри.
   - Праве поле — 1.5 сантиметри.
   - Верхнє поле — 2.0 сантиметри.
   - Нижнє поле — 2.0 сантиметри.
3. Шрифтове оформлення:
   - Гарнітура — Times New Roman.
   - Кегль — 14 пунктів.
4. Абзацне оформлення:
   - міжрядковий інтервал — одинарний.
   - абзацний відступ — 6 пунктів.
   - вирівнювання — з обох сторін (по ширині).
5. Кожний розділ повинен починатися з нової сторінки.
6. Інтервал після назви розділу — 6 пунктів.
7. Шрифтове оформлення назви розділу:
   - Гарнітура — Times New Roman
   - Кегль — 16 пунктів.
   - Зображення — напівжирне.
8. Перед початком параграфу в межах розділу розрив сторінки робити не треба.
9. Перед назвою параграфу розділу інтервал 6 пунктів.
10. Шрифтове оформлення назви параграфу:
    - Гарнітура — Times New Roman.
    - Кегль — 14 пунктів.

- ♦ Зображення — напівжирне.

11. Шрифтове оформлення назви пунктів в межах параграфу — довільне.
12. Вирівнювання усіх назв (розділів, параграфів, пунктів) — за центром.
13. Наприкінці усіх заголовків крапки бути не повинно.
14. Додатки нумеруються буквами українського (чи російського) алфавіту.
15. Розділи (крім вступу та заключення) нумеруються арабськими цифрами.
16. Номери сторінок повинні знаходитись у правому верхньому куті).
17. Перша сторінка (титульний лист) не повинна містити номеру.
18. Виноски повинні бути сторінкові. Їх використання не рекомендується.
19. Усі ілюстрації та їх назви повинні мати вирівнювання за центром та мати підпис виду «Рис. 1 Назва»
20. Усі назви таблиць повинні мати вирівнювання за правим полем та мати підпис виду «Таблиця 1. Назва»

Електронний варіант пояснювальної записки необхідно надати в одному з форматів *.docx, *.pdf або *.tex.

Пояснювальна записка складається з таких основних частин:

1. Титульний лист (див. приклад)
2. Зміст.
3. Теоретична частина.
4. Практична частина.
5. Висновки
6. Список використаних джерел.
7. Додатки.

Зміст необхідно створювати автоматично, використовуючи відповідні можливості текстового процесору.

Вступ складається з декількох абзаців, у яких вказано: область використання блочних шифрів, їх місце серед інших систем шифрування, необхідність програмної реалізації системи шифрування тексту з використанням алгоритмів блочного шифрування, назву алгоритму, що використовується при створенні програмної системи, середовище її розробки тощо.

Теоретична частина складається з одного чи декількох розділів, у яких описуються алгоритми, програмні комплекси, функції бібліотек, можливості та функції середовища розробки, що використовуються при створенні індивідуальної роботи.

Практична частина складається з одного чи декількох розділів, що безпосередньо описують процес реалізації алгоритму та створення програмної системи шифрування тексту.

У висновках необхідно указати стисло функціональні можливості створеної програмної системи, сильні та слабкі міста обраного алгоритму блочного шифрування.

Список використаних літературних та інтернет джерел створюється за вимогами ДСТУ 8302:2015.

Додатки (якщо вони є) можуть містити програмний код, блок-схеми, концептуальні схеми, та інше.

Презентація алгоритму повинна мати довільний дизайн та містити такі

обов’язкові розділи:

1. Назва алгоритму, клас (наприклад мережа Фейстеля);
2. Автори, якщо відомо;
3. Параметри (довжина ключа та блоку тексту у байтах);
4. Повний алгоритм (можливо частинами або блоками) у загальноприйнятному форматі.

А також може містити можливі приклади апаратних застосувань.

Технічні вимоги до програмної системи: програмна система повинна бути консольним додатком, що приймає параметри з командного рядка. Першим параметром повинна бути (у будь-якому вигляді) назва операції (шифрування чи дешифрування). Другим параметром повинно бути ім’я текстового файлу з початковим (шифрованим) текстом. Третім параметром повинно бути ім’я файлу з ключем. Четвертим параметром повинно бути ім’я текстового файлу з зашифрованим (початковим) текстом.

У якості алфавіту для початкового тексту можна прийняти будь-яку загально прийняту систему кодування символів (де присутня кирилиця), але назву системи кодування необхідно явно указати в звіті.

У якості ключа (залежно від алгоритму) в текстовому файлі вказується відповідне число з необхідною розрядністю в десятковій, шістнадцятковій (з символом ‘H’ чи ‘h’ у кінці) або двійковій (з символом ‘B’ чи ‘b’ укінці) системах числення.

При некоректно введених параметрах чи їх відсутності програмна система повинна вивести параметри її запуску та систему кодування початкового тексту.

Завдання до індивідуальної роботи. У якості алгоритмів для реалізації системи шифрування тексту можна використовувати наступні блокові шифри:

1. Blowfish
2. IDEA
3. Camelia
4. Serpent
5. Mars
6. Towfish
7. Square
8. Kasumi
9. Khazad
10. Khufu
11. Noekeon
12. RC6
13. SAFER (SK-64, SK-128, +)
14. Shakal (1, 2)

УВАГА !!! Для реалізації можна використати інший блоковий шифр, погодивши цей вибір з викладачем.