ДЕРЖАВНИЙ ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД
«ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ»
МІНІСТЕРСТВА ОСВІТИ І НАУКИ
КАФЕДРА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Вказівки з виконання самостійної та індивідуальної роботи

З КУРСУ

«Основи криптології»

Освітньо-кваліфікаційний рівень: бакалавр

Галузь знань: 0403 Системні науки та кібернетика

Напрям підготовки: 6.040302 «**Інформатика**»

Укладач:
ст.викл. каф. ІТ ЗНУ
Маслєнніков В.О.

Запоріжжя 2013

Тема індивідуальної роботи: «Знайомство та програмна реалізація системи шифрування тексту з використанням алгоритму блочного шифрування …». Алгоритм береться зі списку.

Метою індивідуальної роботи є знаймство студентів з принципами роботи 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 (усі різновиди) та Linux (усі різновиди), та у якості вхідної мови програмування використовує наступні: C, C++, Pascal, Fortran, Basic або мови Ассемблеру для мікропроцессорів архітектури x86.

Звіт з виконання індивідуальної роботи складається з двох складових:

1. Програмна система (включаючи всі необхідні файли) на змінному носії інформації (гнучкому диску, CD диску тощо).
2. Пояснювальна записка (звіт)
3. Презентація (у форматі Microsoft Power Point) обраного алгоритму блочного шифрування.

Пояснювальна записка (звіт) повинна бути представлена в друкованому та електроному варіантах.

Вимоги до друкованого варіанту:

1. Пояснювальна записка друкується на листах формату A4 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:
   - міжстроковий 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 розрів стрінки 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 арабскими цифрами.
16. Номери сторінок повиннні знаходитись у правому верхньому куті).
17. Перша сторінка (титульний лист) не повинен 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»

Електроний варіант пояснювальної записки необхідно надати в форматах MS Word (версія не нижче 97), PDF або TeX. Якщо пояснювальна записка надається в форматі MS Word, то її оформлення повинно зберігатися незалежно від компьютеру, на якому документ буде використовуватися (тобто для кожного типу абзаців необхідно визначити відповідний стиль, який зберігти у документі).
Пояснювальна записка складається з таких основних частин:

1. Титульний лист (див. приклад)
2. Реферат.
3. Зміст.
4. Вступ.
5. Теоретична частина.
6. Практична частина.
7. Заключення.
8. Список використаних джерел.

Реферат не перевищує 1 сторінки і містить інформацію про об’єм пояснювальної записки, кількості ілюстрацій, таблиць, додатків та використаних літературних джерел. Крім цього, реферат повинен містити відомості про об’єкт дослідження, ціль дослідження, мету дослідження, результати та виводи, а також список ключових слів.
Зміст починається з нової сторінки після реферату і містить перелік всіх розділів пояснювальної записки. 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 (рідко) розділів, у яких описуються алгоритми, програмні комплеки, 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 заключенні (висновках) необхідно указати (кратко) функціональні можливості створенної програмної системи, сильні та слабкі міста обраного алгоритму блочного шифрування.
Список використаних літературних джерел створюється за загальними правилами. У пояснювальній записці дозволено використовувати посилання на internet ресурси у вигляді:

1. URL: http://kit.zsu.zp.ua

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, класс (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 (додаткові бали за індивідуальну роботу) наступні необов'якові розділи:

1. Тести;
2. Можливі приклади апаратних застосувань;
3. та інше.

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 алфавиту для початкового тексту можна прийняти будь-яку загально прийняту систему кодування символів (де присутня кириліця), але назву системи кодування (кодової страниці) необхідно явно указати в звіті.
У якості ключа (залежно від алгоритму) в текстовому файлі вказується відповідне число з необхідною розрядністю в десяткової, шістнадцятковій (з символом 'H' чи 'h' укінці) або двійковій (з символом 'B' чи 'b' укінці) системах числення.
При некоректо введених парамерах 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 блочні 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)

Для реалізації можна використати інший блочний шифр, погодивши цей вибір з керівником індивідуальної роботи.

Використані джерела

1. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии. Учебное пособие.—Гелиос-АРВ, 2001 г., 480 с.
2. Баричев С.Г., Гончаров В.В., Веров Р.Е. Основы современной криптографии. Учебное пособие.—2002 г., 175 с.
3. Панасенко С.П. Алгоритмы шифрования. Специальный справочник .— Издательство: BHV-СПб, 2009 г., —576 стр