НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ

«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ

імені Ігоря Сікорського»

Факультет прикладної математики

Кафедра прикладної математики

Звіт

з лабораторної роботи № 3

із дисципліни «Криптографічні методи захисту інформації»

на тему

*Стандарт шифрування DES*

|  |  |
| --- | --- |
| Виконав: | Керівник: |
| студент групи КМ-ХХ | *ст. викладач Бай Ю. П.* |
| *Іваненко І. І.* |  |

Київ — 2022

ЗМІСТ

[Постановка задачі 2](#_Toc100571354)

[Основні теоретичні відомості зі стандарту шифрування DES 3](#_Toc100571355)

[Контрольний приклад 4](#_Toc100571356)

[Шифрування тексту 5](#_Toc100571357)

[Розшифрування тексту 5](#_Toc100571358)

[Відповіді на контрольні запитання 5](#_Toc100571359)

[Список літератури 6](#_Toc100571360)

[Додаток 1 7](#_Toc100571361)

[Додаток 2 8](#_Toc100571362)

***Мета роботи:*** опрацювати загальну послідовність алгоритму DES, розробити криптосистему на основі стандарту шифрування DES, дослідити особливості алгоритму: нелінійні блоки, лавиновий ефект, режими роботи.

# Постановка задачі

1. Скласти програму для шифрування та розшифрування за алгоритмом DES 64-бітного блоку інформації, використовуючи 64-бітний ключ. Продемонструвати роботу програми на контрольному прикладі. Навести скріншоти детального покрокового виконання алгоритму.

Контрольний приклад:

<https://courses.cs.washington.edu/courses/cse467/99au/admin/Slides/Week6Lecture1/sld001.htm>. Виконати приклад в деталях. Зробити скріншоти до результатів слайдів 7, 9, 10, 11, 12, 13, 14, 15, 17, 19, 20, 21, 22, 23.

АБО

<https://page.math.tu-berlin.de/~kant/teaching/hess/krypto-ws2006/des.htm>

Виконати приклад в деталях (від «How DES Works in Detail» до результату), зробити скріншоти до всіх проміжних результатів.

2. Розширити функціональність програми для випадку відкритого тексту довільної довжини та 64-бітного ключа.

3. За стандартом DES зашифрувати текст довжиною від 8 до 80 символів, користуючись 64-бітним ключем.

4. Дано зашифроване за стандартом DES повідомлення довжиною від 8 до 80 символів та відомий 64-бітний ключ. Розшифрувати задане повідомлення.

5. Яка ефективна довжина ключа шифру DES?

6. Як працюють нелінійні блоки *S*1 … *S*8? Яким буде результат проходження 6-бітового блоку 111000 через блок *S*8 ?

7. Що означає лавиновий ефект? Продемонструвати лавиновий ефект при зміні одного біту на вході після трьох раундів шифрування.

8. Які існують режими роботи DES? У чому полягає режим CBC?

# Основні теоретичні відомості зі стандарту шифрування DES

……

# Контрольний приклад

<https://courses.cs.washington.edu/courses/cse467/99au/admin/Slides/Week6Lecture1/sld001.htm>

Виконати приклад в деталях. Зробити скріншоти до результатів слайдів 7, 9, 10, 11, 12, 13, 14, 15, 17, 19, 20, 21, 22, 23.

АБО

https://page.math.tu-berlin.de/~kant/teaching/hess/krypto-ws2006/des.htm

Виконати приклад в деталях (від «How DES Works in Detail» до результату), зробити скріншоти до результатів.

# Шифрування тексту

Зашифруємо текст

"Two wrongs don't make a right. " ,

використовуючи ключ *key* = '13 34 57 79 9B BC DF F1' (hex).

Зауважимо, що довжина відкритого тексту має бути кратною 64 бітам (8 байтам), довжина ключа має дорівнювати 64 бітам, з яких буде використано лише 56 бітів.

Одержуємо зашифрований текст:

… (hex)

# Розшифрування тексту

Дано зашифроване за стандартом DES повідомлення:

85 E8 13 54 0F 0A B4 05 (hex)

і відомо 64-бітний ключ:

*key* = '13 34 57 79 9B BC DF F1' (hex).

Розшифровуючи заданий криптотекст, одержимо:

01 23 45 67 89 AB CD EF (hex)

# Відповіді на контрольні запитання

…

# Список літератури

1. Тарнавський Ю.А. Технології захисту інформації [Електронний ресурс] / Ю. А. Тарнавський. – Київ: КПІ ім. Ігоря Сікорського, 2018. – 162 с.
2. Шнайер Б. Прикладная криптография: Протоколы, алгоритмы, исходные тексты на языке Си / Б. Шнайер. – М.: Диалектика, 2003. – 610 с.
3. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии. – М.: Гелиос АРВ, 2001. – 480 с.
4. Столлингс В. Криптография и защита сетей: принципы и практика, 2-е изд.: Пер. с англ. – М.: «Вильямс», 2001. – 672 с.
5. Гулак Г.М., Мухачов В.А., Хорошко В.О., Яремчук Ю.Є. Основи криптографічного захисту інформації. – Вінниця: ВНТУ, 2011. – 198 с.

# Додаток 1

Текст програми, що реалізує стандарт шифрування DES

# Додаток 2

Скріншоти шифрування та розшифрування тексту довжиною  
від 8 до 80 символів