НТУУ «КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»

ТЕПЛОЕНЕРГЕТИЧНИЙ ФАКУЛЬТЕТ

Кафедра АПЕПС

«Засоби захисту інформації»

Лабораторна робота № 5

ШИФРУВАННЯ DES В ПРИКЛАДНІЙ ПРОГРАМІ

*Варіант №12*

*Студента 5 курсу групи ТВ-31с*

Пєхота О.Е.

Перевірив:

кандидат фізико-математичних наук,

доцент Ю.А. Тарнавський

Київ –2014

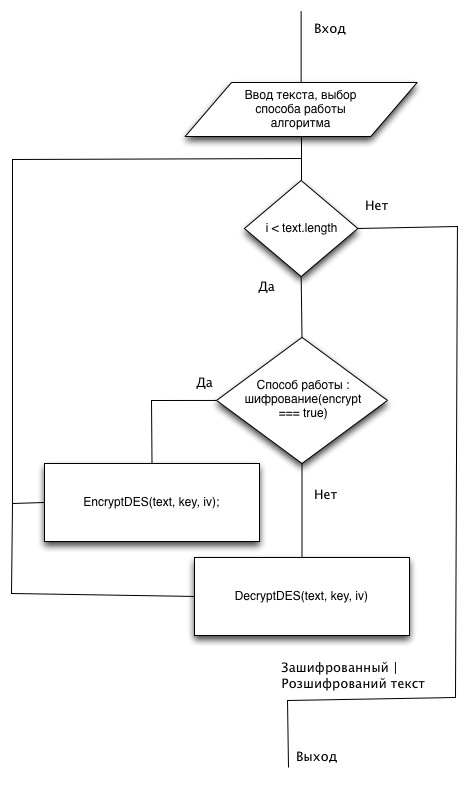
# Варіант завдання

Ознайомитись з шифруванням даних методом DES і надати його програмну реалізацію

# Хід виконання завдання

1. Створюємо серверний додаток на мові програмування javascript.
2. Підключаємо необхідні бібліотеки для обробки запитів на сервер та методи для шифрування-дешифрування даних *(додаток1)*
3. Створюємо html сторінку для взяємодії з користувачем.
4. Додамо в сторінку візуальні елементи, а також код для обробки дій користувача та відправки запитів на сервер за допомогою мови програмування javascript. *(додаток 2)*
5. Запускаемо сервер та html сторінку користувача.
6. Ввводимо змінну 8бітний ключ та поідомлення для шифрування.

# БЛок-Схема Алгоритму шифрування



# Висновки

Шифрування методом DES – гарний алгоритм шифрування, але історія показала що він досить слабкий для використання в повсякденній роботі. Тому для більшої надійності потрібно або змінювати алгоритм, або збільшувати криптостійкість.

# Додатки

**Додаток 1**

// ciphers.js

desCipher: **function** (text, key, inc) {

// http://www.programering.com/a/MTMzcDMwATM.html

**var** cipheriv = **function** (en, code, data) {

**var** buf1 = en.update(data, code), buf2 = en.final();

**var** r = **new** Buffer(buf1.length + buf2.length);

buf1.copy(r); buf2.copy(r, buf1.length);

**return** r;

};

**var** EncryptDES=**function** (data, key, vi) {

**return** cipheriv(crypto.createCipheriv('des', key, vi), 'utf8', data).toString('base64');

};

**var** DecryptDES = **function** (data, key, vi) {

**return** cipheriv(crypto.createDecipheriv('des', key, vi), 'base64', data) .toString('utf8');

};

**var** iv = **new** Buffer(8);

iv.fill(0);

**if**(inc) {

**return** EncryptDES(text, key, iv);

}

**return** DecryptDES(text, key, iv);

}

**Додаток 2**

