Министерство образования Республики Беларусь

Учреждение образования

«Белорусский государственный университет информатики и радиоэлектроники»

Филиал

«Минский радиотехнический колледж»

Учебный предмет «Защита компьютерной информации»

**Отчет**

по выполнению лабораторной работы №4

«Реализация алгоритма получения ключей

для схемы шифрования DES, AES»

Выполнила: учащаяся гр.1к9391 Смаргун Е.А.

Проверила: Радкевич А. С.

Минск 2023

**Лабораторная работа № 4**

**Тема работы:** «Реализация алгоритма получения ключей

для схемы шифрования DES, AES»

**1. Цель работы**

Формирование умений получения ключей для схемы шифрования DES и AES.

**2. Задание**

Разработайте программу, имитирующую реализацию элементов метода криптографической защиты информации DES, AES. Программа должна выполнять реализацию алгоритма получения ключей для схемы шифрования DES, AES. В качестве ключа используйте номер варианта.

**3. Оснащение работы**

ЭВМ, Текстовый редактор.

**4. Порядок выполнения работы**

**Пример DES**

**Шифруемое сообщение** – ***шифровка*** = ***11111000 11101000 11110100 11110000 11101110*** ***11100010 11101010 11100000***

**Ключ шифрования *12345678*** = ***00110001 00110010 00110011 00110100 00110101 00110110*** ***00110111 00111000***

**Шаг 1 Начальная перестановка**

*Входная последовательность*

***1111100011101000111101001111000011101110111000101110101011100000*** - согласно таблице начальной перестановки перестанавливаем биты в сообщении.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 58 | 50 | 42 | 34 | 26 | 18 | 10 | 2 | 60 | 52 | 44 | 36 | 28 | 20 | 12 | 4 |
| 62 | 54 | 46 | 38 | 30 | 22 | 14 | 6 | 64 | 56 | 48 | 40 | 32 | 24 | 16 | 8 |
| 57 | 49 | 41 | 33 | 25 | 17 | 9 | 1 | 59 | 51 | 43 | 35 | 27 | 19 | 11 | 3 |
| 61 | 53 | 45 | 37 | 29 | 21 | 13 | 5 | 63 | 55 | 47 | 39 | 31 | 23 | 15 | 7 |

*Полученная последовательность* ***1111111100001101000101000000000011111111111111110101001101110000***

**Шаг 2 Получение последовательности L(0) и R(0)**

Делим полученную последовательность согласно таблицам.

Последовательности получаются путём деления блока в 64 бита на 2 равных части.

**L(0) перестановка**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 |

**L(0) последовательность полученная *11111111000011010001010000000000***

**R(0) перестановка**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 33 | 34 | 35 | 36 | 37 | 38 | 39 | 40 | 41 | 42 | 43 | 44 | 45 | 46 | 47 | 48 |
| 49 | 50 | 51 | 52 | 53 | 54 | 55 | 56 | 57 | 58 | 59 | 60 | 61 | 62 | 63 | 64 |

**R(0) последовательность полученная *11111111111111110101001101110000***

**Шаг 3 Функция выбора и перестановки последовательности В (преобразование ключа шифрования)**

Входная последовательность

***0011000100110010001100110011010000110101001101100011011100111000***

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 57 | 49 | 41 | 33 | 25 | 17 | 9 | 1 | 58 | 50 | 42 | 34 | 26 | 18 |
| 10 | 2 | 59 | 51 | 43 | 35 | 27 | 19 | 11 | 3 | 60 | 52 | 44 | 36 |
| 63 | 55 | 47 | 39 | 31 | 23 | 15 | 7 | 62 | 54 | 46 | 38 | 30 | 22 |
| 14 | 6 | 61 | 53 | 45 | 37 | 29 | 21 | 13 | 5 | 28 | 20 | 12 | 4 |

Полученная последовательность ***00000000000000001111111111110110011001111000100000001111***

**Шаг 4 Получение последовательностей C(0) D(0)**

Полученную последовательность(ключа) делим на две согласно таблицам.

**C(0)**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 |
| 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 |

**Последовательность C(0) = *0000000000000000111111111111***

**D(0)**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 29 | 30 | 31 | 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 | 40 | 41 | 42 |
| 43 | 44 | 45 | 46 | 47 | 48 | 49 | 50 | 51 | 52 | 53 | 54 | 55 | 56 |

**Последовательность D(0) = 0110011001111000100000001111**

**Шаг 5 получение последовательности C(i)**

По таблице сдвигаем биты в последовательностях

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| 1 | 1 | 2 | 2 | 2 | 2 | 2 | 2 | 1 | 2 | 2 | 2 | 2 | 2 | 2 | 1 |

**C(0) = 0000000000000000111111111111**

|  |  |
| --- | --- |
| C(1) | 0000000000000001111111111110 |
| C(2) | 0000000000000011111111111100 |
| C(3) | 0000000000001111111111110000 |
| C(4) | 0000000000111111111111000000 |
| C(5) | 0000000011111111111100000000 |
| C(6) | 0000001111111111110000000000 |
| C(7) | 0000111111111111000000000000 |
| C(8) | 0011111111111100000000000000 |
| C(9) | 0111111111111000000000000000 |
| C(10) | 1111111111100000000000000001 |
| C(11) | 1111111110000000000000000111 |
| C(12) | 1111111000000000000000011111 |
| C(13) | 1111100000000000000001111111 |
| C(14) | 1110000000000000000111111111 |
| C(15) | 1000000000000000011111111111 |
| C(16) | 0000000000000000111111111111 |

**Шаг 6 получение последовательности D(i)**

По той же таблице сдвигаем биты в последовательностях

**D(0) = 0110011001111000100000001111**

|  |  |
| --- | --- |
| D(1) | 1100110011110001000000011110 |
| D(2) | 1001100111100010000000111101 |
| D(3) | 0110011110001000000011110110 |
| D(4) | 1001111000100000001111011001 |
| D(5) | 0111100010000000111101100110 |
| D(6) | 1110001000000011110110011001 |
| D(7) | 1000100000001111011001100111 |
| D(8) | 0010000000111101100110011110 |
| D(9) | 0100000001111011001100111100 |
| D(10) | 0000000111101100110011110001 |
| D(11) | 0000011110110011001111000100 |
| D(12) | 0001111011001100111100010000 |
| D(13) | 0111101100110011110001000000 |
| D(14) | 1110110011001111000100000001 |
| D(15) | 1011001100111100010000000111 |
| D(16) | 0110011001111000100000001111 |

**Шаг 7 получение последовательностей K(i)**

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 14 | 17 | 11 | 24 | 1 | 5 | 3 | 28 | 15 | 6 | 21 | 10 |
| 23 | 19 | 12 | 4 | 26 | 8 | 16 | 7 | 27 | 20 | 13 | 2 |
| 41 | 52 | 31 | 37 | 47 | 55 | 30 | 40 | 51 | 45 | 33 | 48 |
| 44 | 49 | 39 | 56 | 34 | 53 | 46 | 42 | 50 | 36 | 29 | 32 |

Для получения последовательности K(i) произведём конкатенацию последовательностей C(i) и D(i). В полученной последовательности C(i)D(i) переставим биты согласно таблице.

**K(0) = 010100010010110010001100101001110100001111000000**

|  |  |
| --- | --- |
| K(1) | 010100000010110010101100010101110010101011000010 |
| K(2) | 010100001010110010100100010100001010001101000111 |
| K(3) | 110100001010110000100110111101101000010010001100 |
| K(4) | 111000001010011000100110010010000011011111001011 |
| K(5) | 111000001001011000100110001111101111000000101001 |
| K(6) | 111000001001001001110010011000100101110101100010 |
| K(7) | 101001001101001001110010100011001010100100111010 |
| K(8) | 101001100101001101010010111001010101111001010000 |
| K(9) | 001001100101001101010011110010111001101001000000 |
| K(10) | 001011110101000101010001110100001100011100111100 |
| K(11) | 000011110100000111011001000110010001111010001100 |
| K(12) | 000111110100000110011001110110000111000010110001 |
| K(13) | 000111110000100110001001001000110110101000101101 |
| K(14) | 000110110010100010001101101100100011100110010010 |
| K(15) | 000110010010110010001100101001010000001100110111 |
| K(16) | 010100010010110010001100101001110100001111000000 |

**Вывод:** сформировали умения получения ключей для схемы шифрования DES и AES.

**5. Контрольные вопросы и задания**

**1. Каким образом формируются последовательности C(0) и D(0)?**

Последовательности C(0) и D(0) в алгоритме DES формируются путем перестановки и сокращения исходного ключа размером 64 бита к размеру 56. Затем разделяется на две половины - C(0) и D(0) по 28 бит каждая.

**2. Какую длину имеют ключи DES?**

Ключи DES первоначально имеют 64 бита, а потом сокращаются до 48 бит каждый из 16 ключей.

**3. Опишите процедуру формирования ключей.**

Процедура формирования ключей DES состоит из нескольких этапов. Сначала исходный 64-битный ключ переставляется с помощью таблицы перестановки и сокращается до 56 бит, затем делится на две половины - С(0) и D(0) по 28 бит каждая. Затем происходит раундовая генерация ключей (всего 16 раундов), где на каждом шаге происходит сдвиг половин ключа влево на определенное количество бит, а затем они объединяются и переставляются с помощью таблицы, в результате чего получаются 48-битные раундовые ключи.

**4. Какую длину имеют ключи AES?**

Ключи AES могут иметь длину 128, 192 или 256 бит, в зависимости от выбранной длины ключа. На самом деле ключ может быть расширен до определенного размера с помощью процедуры расширения ключа, но наиболее распространенными являются ключи длиной 128, 192 и 256 бит.