ФЕДЕРАЛЬНОЕ АГЕНСТВО СВЯЗИ

Московский технический университет связи и информатики

Кафедра защиты информации

Курсовая работа

По теме**: “Реализация алгоритма DES”**

Выполнил студент

Группы: БВТ1501

Нгуен Тхе Ань

Москва 2019

**Задание на курсовой проект**

1. Запишите первые семь букв своей фамилии латинскими буквами в привычном вам виде. Для фамилий короче 7 букв недостающие символы считайте пробелами.

2. Переведите полученные 7 символов в двоичный вид с помощью таблицы ASCII (Приложение 1).Обратите внимание, коды символов представлены в таблице в шестнадцатеричной форме.

3. Рассчитайте простейший хэш-код от полученных 7 символов – ротационный XOR

4. С помощью алгоритма шифрования DEA (описанного в стандарте DES) произведите шифрование полученного 8-ми байтного блока информации:

– В качестве пароля используйте набор из 7 разных букв, также переведенных в двоичную форму при помощи таблицы ASCII.

– Для шифрования используйте только 4 раунда шифрования из предусмотренных стандартом 16-ти.

– Записывайте все промежуточные данные (значения всех блоков в приведенных блок-схемах для каждого раунда).

6. Результирующие 64 бита разбейте на 8 байтов и переведите в символы в соответствии с таблицей ASCII.

Исходные данные: Nguyen

ASC II: 4e 67 75 79 65 6e 20 20

Binary:

|  |  |
| --- | --- |
| N | 01001110 |
| g | 01100111 |
| u | 01110101 |
| y | 01111001 |
| e | 01100101 |
| n | 01101110 |
|  | 00100000 |
|  | 00100000 |

Ротационный XOR:

|  |  |
| --- | --- |
| Zero | 00000000 |
| ← | 00000000 |
| N | 01001110 |
| XOR | 01001110 |
| ← | 10011100 |
| g | 01100111 |
| XOR | 11111011 |
| ← | 11110111 |
| u | 01110101 |
| XOR | 10000000 |
| ← | 00000101 |
| y | 01111001 |
| XOR | 01111100 |
| ← | 11111000 |
| e | 01100101 |
| XOR | 10011101 |
| ← | 00111011 |
| n | 01101110 |
| XOR | 01010101 |
| ← | 10101010 |
|  | 00100000 |
| XOR | 10001010 |
| ← | 00010101 |
|  | 00100000 |
| XOR | 00110101 |

Начальная 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 |
| 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 |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 0 | 0 | 1 | 1 | 1 | 0 |
| 1 | 1 | 1 | 1 | 1 | 0 | 1 | 1 |
| 1 | 0 | 0 | 0 | 0 | 0 | 1 | 0 |
| 0 | 1 | 1 | 1 | 1 | 1 | 0 | 0 |
| 1 | 0 | 0 | 1 | 1 | 1 | 0 | 1 |
| 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 |
| 1 | 0 | 0 | 0 | 1 | 0 | 1 | 0 |
| 0 | 0 | 1 | 1 | 0 | 1 | 0 | 1 |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 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 |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 0 | 1 | 0 | 1 | 0 | 1 | 1 |
| 1 | 0 | 1 | 1 | 1 | 0 | 1 | 0 |
| 1 | 0 | 1 | 1 | 1 | 0 | 0 | 1 |
| 1 | 0 | 1 | 1 | 0 | 0 | 1 | 0 |
| 0 | 1 | 0 | 1 | 0 | 1 | 1 | 0 |
| 1 | 0 | 0 | 0 | 1 | 0 | 1 | 0 |
| 0 | 1 | 0 | 1 | 1 | 0 | 1 | 1 |
| 0 | 1 | 0 | 0 | 0 | 1 | 1 | 1 |

Ключ шифрования: 12345678

ASC II: 49 50 51 52 53 54 55 56 57

Binary:

|  |  |
| --- | --- |
| 1 | 00110001 |
| 2 | 00110010 |
| 3 | 00110011 |
| 4 | 00110100 |
| 5 | 00110101 |
| 6 | 00110110 |
| 7 | 00110111 |
| 8 | 00111000 |

56-ти битный ключ C1D1

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **PC-1 (Выбор 1)** | | | | | | | **PC-2 (Выбор 2)** | | | | | |
| 57 | 49 | 41 | 33 | 25 | 17 | 9 | 14 | 17 | 11 | 24 | 1 | 5 |
| 1 | 58 | 50 | 42 | 34 | 26 | 18 | 3 | 28 | 15 | 6 | 21 | 10 |
| 10 | 2 | 59 | 51 | 43 | 35 | 27 | 23 | 19 | 12 | 4 | 26 | 8 |
| 19 | 11 | 3 | 60 | 52 | 44 | 36 | 16 | 7 | 27 | 20 | 13 | 2 |
| 63 | 55 | 47 | 39 | 31 | 23 | 15 | 41 | 52 | 31 | 37 | 47 | 55 |
| 7 | 62 | 54 | 46 | 38 | 30 | 22 | 30 | 40 | 51 | 45 | 33 | 48 |
| 14 | 6 | 61 | 53 | 45 | 37 | 29 | 44 | 49 | 39 | 56 | 34 | 53 |
| 21 | 13 | 5 | 28 | 20 | 12 | 4 | 46 | 42 | 50 | 36 | 29 | 32 |
| **PC-1 (Выбор 1)** | | | | | | | **PC-2 (Выбор 2)** | | | | | |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 0 |
| 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 0 |
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 |
| 1 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 1 | 0 |
| 0 | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 1 |
| 1 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 1 | 0 |
| 1 | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 0 |

Разделим входные данные на два блока:

L1 = 1011 1010 1001 0010 0110 1010 1011 0111

R1 = 1011 1010 1001 0010 0110 1010 1011 0111

Расширяем до 48 бит:

L\*1 = 110111 110101 010010 100100 001101 010101 010110 101111

Таблицы S – преобразований.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **0** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | **11** | **12** | **13** | **14** | **15** |  |
| **0** | 14 | 4 | 13 | 1 | 2 | 15 | 11 | 8 | 3 | 10 | 6 | 12 | 5 | 9 | 0 | 7 | ***S*1** |
| **1** | 0 | 15 | 7 | 4 | 14 | 2 | 13 | 1 | 10 | 6 | 12 | 11 | 9 | 5 | 3 | 8 |
| **2** | 4 | 1 | 14 | 8 | 13 | 6 | 2 | 11 | 15 | 12 | 9 | 7 | 3 | 10 | 5 | 0 |
| **3** | 15 | 12 | 8 | 2 | 4 | 9 | 1 | 7 | 5 | 11 | 3 | 14 | 10 | 0 | 6 | 13 |
|  | **0** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | **11** | **12** | **13** | **14** | **15** |  |
| **0** | 15 | 1 | 8 | 14 | 6 | 11 | 3 | 4 | 9 | 7 | 2 | 13 | 12 | 0 | 5 | 10 | ***S*2** |
| **1** | 3 | 13 | 4 | 7 | 15 | 2 | 8 | 14 | 12 | 0 | 1 | 10 | 6 | 9 | 11 | 5 |
| **2** | 0 | 14 | 7 | 11 | 10 | 4 | 13 | 1 | 5 | 8 | 12 | 6 | 9 | 3 | 2 | 15 |
| **3** | 13 | 8 | 10 | 1 | 3 | 15 | 4 | 2 | 11 | 6 | 7 | 12 | 0 | 5 | 14 | 9 |
|  | **0** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | **11** | **12** | **13** | **14** | **15** |  |
| **0** | 10 | 0 | 9 | 14 | 6 | 3 | 15 | 5 | 1 | 13 | 12 | 7 | 11 | 4 | 2 | 8 | ***S*3** |
| **1** | 13 | 7 | 0 | 9 | 3 | 4 | 6 | 10 | 2 | 8 | 5 | 14 | 12 | 11 | 15 | 1 |
| **2** | 13 | 6 | 4 | 9 | 8 | 15 | 3 | 0 | 11 | 1 | 2 | 12 | 5 | 10 | 14 | 7 |
| **3** | 1 | 10 | 13 | 0 | 6 | 9 | 8 | 7 | 4 | 15 | 14 | 3 | 11 | 5 | 2 | 12 |
|  | **0** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | **11** | **12** | **13** | **14** | **15** |  |
| **0** | 7 | 13 | 14 | 3 | 0 | 6 | 9 | 10 | 1 | 2 | 8 | 5 | 11 | 12 | 4 | 15 | ***S*4** |
| **1** | 13 | 8 | 11 | 5 | 6 | 15 | 0 | 3 | 4 | 7 | 2 | 12 | 1 | 10 | 14 | 9 |
| **2** | 10 | 6 | 9 | 0 | 12 | 11 | 7 | 13 | 15 | 1 | 3 | 14 | 5 | 2 | 8 | 4 |
| **3** | 3 | 15 | 0 | 6 | 10 | 1 | 13 | 8 | 9 | 4 | 5 | 11 | 12 | 7 | 2 | 14 |
|  | **0** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | **11** | **12** | **13** | **14** | **15** |  |
| **0** | 2 | 12 | 4 | 1 | 7 | 10 | 11 | 6 | 8 | 5 | 3 | 15 | 13 | 0 | 14 | 9 | ***S*5** |
| **1** | 14 | 11 | 2 | 12 | 4 | 7 | 13 | 1 | 5 | 0 | 15 | 10 | 3 | 9 | 8 | 6 |
| **2** | 4 | 2 | 1 | 11 | 10 | 13 | 7 | 8 | 15 | 9 | 12 | 5 | 6 | 3 | 0 | 14 |
| **3** | 11 | 8 | 12 | 7 | 1 | 14 | 2 | 13 | 6 | 15 | 0 | 9 | 10 | 4 | 5 | 3 |
|  | **0** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | **11** | **12** | **13** | **14** | **15** |  |
| **0** | 12 | 1 | 10 | 15 | 9 | 2 | 6 | 8 | 0 | 13 | 3 | 4 | 14 | 7 | 5 | 11 | ***S*6** |
| **1** | 10 | 15 | 4 | 2 | 7 | 12 | 9 | 5 | 6 | 1 | 13 | 14 | 0 | 11 | 3 | 8 |
| **2** | 9 | 14 | 15 | 5 | 2 | 8 | 12 | 3 | 7 | 0 | 4 | 10 | 1 | 13 | 11 | 6 |
| **3** | 4 | 3 | 2 | 12 | 9 | 5 | 15 | 10 | 11 | 14 | 1 | 7 | 6 | 0 | 8 | 13 |
|  | **0** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | **11** | **12** | **13** | **14** | **15** |  |
| **0** | 4 | 11 | 2 | 14 | 15 | 0 | 8 | 13 | 3 | 12 | 9 | 7 | 5 | 10 | 6 | 1 | ***S*7** |
| **1** | 13 | 0 | 11 | 7 | 4 | 9 | 1 | 10 | 14 | 3 | 5 | 12 | 2 | 15 | 8 | 6 |
| **2** | 1 | 4 | 11 | 13 | 12 | 3 | 7 | 14 | 10 | 15 | 6 | 8 | 0 | 5 | 9 | 2 |
| **3** | 6 | 11 | 13 | 8 | 1 | 4 | 10 | 7 | 9 | 5 | 0 | 15 | 14 | 2 | 3 | 12 |
|  | **0** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | **11** | **12** | **13** | **14** | **15** |  |
| **0** | 13 | 2 | 8 | 4 | 6 | 15 | 11 | 1 | 10 | 9 | 3 | 14 | 5 | 0 | 12 | 7 | ***S*8** |
| **1** | 1 | 15 | 13 | 8 | 10 | 3 | 7 | 4 | 12 | 5 | 6 | 11 | 0 | 14 | 9 | 2 |
| **2** | 7 | 11 | 4 | 1 | 9 | 12 | 14 | 2 | 0 | 6 | 10 | 13 | 15 | 3 | 5 | 8 |
| **3** | 2 | 1 | 14 | 7 | 4 | 10 | 8 | 13 | 15 | 12 | 9 | 0 | 3 | 5 | 6 | 11 |

Таблица кодировки ASC II:

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Код (Hex)** | **Символ** | **Код (**Hex) | **Символ** | **Код (Hex)** | **Символ** | **Код (Hex)** | **Символ** | **Код (Hex)** | **Символ** | **Код (Hex)** | **Символ** |
| 20 | Пробел | 30 | . | 40 | @ | 50 | P | 60 | ' | 70 | p |
| 21 | ! | 31 | 0 | 41 | A | 51 | Q | 61 | a | 71 | q |
| 22 | " | 32 | 1 | 42 | B | 52 | R | 62 | b | 72 | r |
| 23 | # | 33 | 2 | 43 | C | 53 | S | 63 | c | 73 | s |
| 24 | $ | 34 | 3 | 44 | D | 54 | T | 64 | d | 74 | t |
| 25 | % | 35 | 4 | 45 | E | 55 | U | 65 | e | 75 | u |
| 26 | & | 36 | 5 | 46 | F | 56 | V | 66 | f | 76 | v |
| 27 | ' | 37 | 6 | 47 | G | 57 | W | 67 | g | 77 | w |
| 28 | ( | 38 | 7 | 48 | H | 58 | X | 68 | h | 78 | x |
| 29 | ) | 39 | 8 | 49 | I | 59 | Y | 69 | i | 79 | y |
| 2A | \* | 3A | 9 | 4A | J | 5A | Z | 6A | j | 7A | z |
| 2B | + | 3B | : | 4B | K | 5B | [ | 6B | k | 7B | { |
| 2C | , | 3C | ; | 4C | L | 5C | \ | 6C | l | 7C | | |
| 2D | - | 3D | < | 4D | M | 5D | ] | 6D | m | 7D | } |
| 2E | . | 3E | > | 4E | N | 5E | ^ | 6E | n | 7E | ~ |
| 2F | / | 3F | ? | 4F | O | 5F | \_ | 6F | o | 7F | DEL |

**Выводы по работе**

1. В курсовом проекте изучали блочный алгоритм шифрования DES, на вход подавали блок информации, 8 символов фамилии (64 бита информации). Затем блоки представляются в виде хэш-функций. Для того, чтобы избавится от любой регулярности, которая присутствует во входных значениях, в курсовом проекте используется ротационный хэш-код.

2. Цель курсовой работы закодировать свою фамилию с помощью стандарта шифрования DES, который базируется на алгоритме DEA. DEA представляет собой алгоритм криптозащиты блочного шифрования. Вся информация разбивается на блоки размером 64 бита. Входной блок данных, состоящий из 64 бит, преобразуется в выходной блок данных идентичной длины. Ключ состоит из 64 разрядов, 8 из которых могут использоваться для контроля четности. Ключ шифрования должен быть известен как отправляющей, так и принимающей стороне. В алгоритме шифрования DES широко используются перестановки битов текста для удаления статистических связей между символами.

При шифровании и дешифровании используется один и тот же алгоритм.

Размещено на Allbest.ru