**ШИФРУВАННЯ FIPS 197 (АЛГОРИТМ RIJNDAEL)**»

**ЛАБОРАТОРНА РОБОТА № 3**

**ОСНОВНІ КРИПТОПЕРЕТВОРЕННЯ В АМЕРИКАНСЬКОМУ СТАНДАРТІ ШИФРУВАННЯ FIPS 197 (АЛГОРИТМ RIJNDAEL)**

**Мета роботи:** Ознайомитися з чинним стандартом шифрування США – блочним алгоритмом RIJNDAEL.

**Використовуване програмне забезпечення:** пакет математичних обчислень Maple.

**3.1 Завдания на лабораторну роботу**

1. Оберіть довільній текст довжиною 16 літер. Кожну літеру замініть відповідним шістнадцятирічним ASCII-кодом. Сформуйте матрицю – 4 стовпця по 4 шістнадцятирічних числа. Отримуєте початковий State .   
**Sunsets over sea - 53 75 6E 73 65 74 73 20 6F 76 65 72 20 73 65 61**  
ASCII-код і подальший перевід його в шістнадцятирічну систему числення:

Код ASCII для букви "S": 83 (десяткове число)  
Для перетворення числа з десяткової системи числення (у даному випадку, 83) в шістнадцятирічну систему числення потрібно виконати наступні дії:

Розділити число на 16 і запам'ятати залишок. Повторювати цю дію доти, поки не буде отримано 0.

83 / 16 = 5, залишок 3

5 / 16 = 0, залишок 5  
Записати залишки у зворотному порядку – 53  
За заданим 128-бітним ключем нульового раунду



сформуйте відповідну State матрицю – 4 стовпця по 4 шістнадцятирічних числа.

Обчисліть перетворення додавання раундового ключа AddRoundKey(,) (див. Приклад Додатку В). Новий State позначте .

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| State S0:  ['53', '65', '6F', '20']  ['75', '74', '76', '73']  ['6E', '73', '65', '65']  ['73', '20', '72', '61'] | + | State R0:  ['00', '04', '08', '0C']  ['01', '05', '09', '0D']  ['02', '06', '0A', '0E']  ['03', '07', '0B', '0F'] | = | ['53', '61', '67', '2C']  ['74', '71', '7F', '7E']  ['6C', '75', '6F', '6B']  ['70', '27', '79', '6E'] |

2. Обчисліть перетворення заміна байтів ByteSub() для кожного елементу State  за допомогою таблиці В.1 (див. Додаток В). Новий State позначте .

|  |  |  |
| --- | --- | --- |
| ['53', '61', '67', '2C']  ['74', '71', '7F', '7E']  ['6C', '75', '6F', '6B']  ['70', '27', '79', '6E'] | Bytesub  = | ['ED', 'EF', '85', '71']  ['92', 'A3', 'D2', 'F3']  ['50', '9D', 'A8', '7F']  ['51', 'CC', 'B6', '9F'] |

3. Обчисліть перетворення зрушення рядків ShiftRow() для рядків матриці State  (див. Приклад Додатку В). Новий State позначте .

|  |  |  |
| --- | --- | --- |
| ['ED', 'EF', '85', '71']  ['92', 'A3', 'D2', 'F3']  ['50', '9D', 'A8', '7F']  ['51', 'CC', 'B6', '9F'] | ShiftRow() | ['ED', 'EF', '85', '71']  ['A3', 'D2', 'F3', '92']  ['A8', '7F', '50', '9D']  ['9F', '51', 'CC', 'B6'] |

4. Обчисліть перетворення MixColumn() перемішування стовпців матриці State  (див. Приклад Додатку В). Новий State позначте .

|  |  |  |
| --- | --- | --- |
| ['ED', 'EF', '85', '71']  ['A3', 'D2', 'F3', '92']  ['A8', '7F', '50', '9D']  ['9F', '51', 'CC', 'B6'] | MixColumn() | ['08', '86', '83', '64']  ['cc', '80', '44', '44']  ['bf', '30', '99', '03']  ['02', '25', 'b4', 'eb'] |

5. За заданим 128-бітним ключем першого раунду



сформуйте відповідну State матрицю – 4 стовпця по 4 шістнадцятирічних числа.

Обчисліть перетворення додавання раундового ключа AddRoundKey(, ). Кінцевий State позначте .

|  |  |  |
| --- | --- | --- |
| R1  D6 D2 DA D6  AA AF A6 AB  74 72 78 76  FD FA F1 FE | AddRoundKey(, ) | ['DE', '54', '59', 'B2']  ['66', '2F', 'E2', 'EF']  ['CB', '42', 'E1', '75']  ['FF', 'DF', '45', '15'] |

6. Перетворити кінцевий внутрішній стан  на текст.



['DE', '54', '59', 'B2']

['66', '2F', 'E2', 'EF']

['CB', '42', 'E1', '75']

['FF', 'DF', '45', '15']

- DE66CBFF542F42DF59E2E145B2EF7515 - ÞfËÿT/BßYâáE²ïu§

7. Отримано 128-бітне зашифроване повідомлення .



Після 9-того раунду розшифрування обчислено State  (візьміть із таблиці 3.1 згідно з номером варіанту N).

Відомі ключі першого і нульового раундів відповідно  і : ,

.

Знайдіть відкритий текст повідомлення .

Для цього

обчисліть перетворення додавання раундового ключа AddRoundKey(, ), новий State позначте ;

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ,  ['2d', '29', '20', 'b9']  ['2d', '78', 'bb', '3a']  ['a9', '6c', 'bf', '0b']  ['1e', 'de', 'f5', '53'] | + | ['D6', 'D2', 'DA', 'D6']  ['AA', 'AF', 'A6', 'AB']  ['74', '72', '78', '76']  ['FD', 'FA', 'F1', 'FE'] | = | ['FB', 'FF', '73', 'C8']  ['83', 'D7', 'CA', '75']  ['54', 'C9', 'C7', '83']  ['44', 'C0', 'FA', 'AD'] |

обчисліть зворотне перетворення InvMixColumn() – перемішування стовпців матриці State , новий State позначте ;

|  |  |  |
| --- | --- | --- |
| ['FB', 'FF', '73', 'C8']  ['83', 'D7', 'CA', '75']  ['54', 'C9', 'C7', '83']  ['44', 'C0', 'FA', 'AD'] | InvMixColumn() | ['84', '45', '34', 'f9']  ['02', '85', 'd8', 'a8']  ['fb', '31', '93', '8f']  ['15', 'd0', 'fb', '4d'] |

обчисліть зворотне перетворення зрушення рядків InvShiftRow() для рядків матриці State , новий State позначте ;

|  |  |  |
| --- | --- | --- |
| ['84', '45', '34', 'f9']  ['02', '85', 'd8', 'a8']  ['fb', '31', '93', '8f']  ['15', 'd0', 'fb', '4d'] | InvShiftRow() | ['84', '45', '34', 'f9']  ['a8', '02', '85', 'd8']  ['93', '8f', 'fb', '31']  ['d0', 'fb', '4d', '15'] |

обчисліть зворотне перетворення заміна байтів InvByteSub() для кожного елементу State  за допомогою таблиці В.2, новий внутрішній стан позначте ;

|  |  |  |
| --- | --- | --- |
| ['84', '45', '34', 'f9']  ['a8', '02', '85', 'd8']  ['93', '8f', 'fb', '31']  ['d0', 'fb', '4d', '15'] | InvByteSub() | ['4f', '68', '28', '69']  ['6f', '6a', '67', '2d']  ['22', '73', '63', '2e']  ['60', '63', '65', '2f'] |

обчисліть перетворення додавання раундового ключа AddRoundKey(,), новий State позначте ;

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ['4f', '68', '28', '69']  ['6f', '6a', '67', '2d']  ['22', '73', '63', '2e']  ['60', '63', '65', '2f'] | AddRoundKey  (,) | R0  00 04 08 0C  01 05 09 0D  02 06 0A 0E  03 07 0B 0F | = | ;  ['4F', '6C', '20', '65']  ['6E', '6F', '6E', '20']  ['20', '75', '69', '20']  ['63', '64', '6E', '20'] |

Кінцевий State  відповідає відкритому тексту повідомлення. Перетворити внутрішній стан  на текст .



['4F', '6C', '20', '65']

['6E', '6F', '6E', '20']

['20', '75', '69', '20']

['63', '64', '6E', '20']

- 4F6E20636C6F7564206E696E65202020 - On cloud nine (Ідіома – бути на

7-му небі від щастя)