**Харківський національний економічний університет**

**імені Семена Кузнеця**

**ЗВІТ**

**З ВИКОНАННЯ ЛАБОРАТОРНОЇ РОБОТИ № 5**

**за дисципліною: *“*Основи криптографічного захисту** ”

**на тему: “ДОСЛІДЖЕННЯ ВЛАСТИВОСТЕЙ**

**БЛОКОВОГО СИМЕТРИЧНОГО ШИФРУ AES”**

**Варіант №4**

**Виконав: студент факультету Інформаційних технологій**

**3 курсу, спец. Кібербезпека,**

**групи 6.04.125.010.21.2**

**Бойко Вадим Віталійович**

**Перевірив:**

**Чугай Андрій Михайлович**

**ХНЕУ ім. С. Кузнеця**

**2023**

**Мета:**

Дослідити процеси шифрування за допомогою алгоритму AES на

основі навчальної програми CrypТool 2

**Завдання:**

|  |  |
| --- | --- |
| Блок відкритого тексту | Ключ |
| 20304050607080910111213141516010 | 08101800283038404850586068707800 |

Генерація ключів

|  |  |
| --- | --- |
| Ключ (128 бітів) у 16-ій системі числення | 08101800283038404850586068707800 |
| Початковий ключ (128 бітів) у вигляді  матриці байтів: | |  |  |  |  | | --- | --- | --- | --- | | 08 | 28 | 48 | 68 | | 10 | 30 | 50 | 70 | | 18 | 38 | 58 | 78 | | 00 | 40 | 60 | 00 |   W0 W1 W2 W3 |
| Циклічний зсув W3: | |  | | --- | | 70 | | 78 | | 00 | | 68 |   W3 |
| Результат заміни кожного байту W3 з використанням S-боксу: | |  | | --- | | 50 | | BC | | 63 | | 45 | |
| W4 = SubBytes(W3) ⊕ Rcon(1) ⊕ W0: | |  | | --- | | 58 | | AC | | 78 | | 45 | |
| W5 = W1 ⊕ W4: | |  | | --- | | 70 | | 9C | | 43 | | 05 | |
| W6 = W2 ⊕ W5: | |  | | --- | | 38 | | CC | | 18 | | 65 | |
| W7 = W3 ⊕ W6: | |  | | --- | | 50 | | BC | | 63 | | 65 | |
| Ключ 1-го раунду (128 бітів) у вигляді матриці байтів: | |  |  |  |  | | --- | --- | --- | --- | | 58 | 70 | 38 | 50 | | AC | 9C | CC | BC | | 78 | 43 | 18 | 63 | | 45 | 05 | 65 | 65 |   W4 W5 W6 W7 |
| Ключ 2-го раунду (128 бітів) у вигляді матриці байтів: | |  |  |  |  | | --- | --- | --- | --- | | 3F | 4F | 77 | 27 | | 57 | CB | 07 | BB | | 36 | 75 | 6E | 0D | | 16 | 13 | 76 | 13 |   W8 W9 W10 W11 |
| Ключ 3-го раунду (128 бітів) у вигляді матриці байтів: | |  |  |  |  | | --- | --- | --- | --- | | D1 | 9E | E9 | CE | | 80 | 48 | 4C | F7 | | 48 | 3E | 50 | 5D | | DA | C9 | BF | AC |   W12 W13 W14 W15 |
| Ключ 4-го раунду (128 бітів) у вигляді матриці байтів: | |  |  |  |  | | --- | --- | --- | --- | | B1 | 2F | C6 | 08 | | CC | 87 | CB | 3C | | DA | E4 | B4 | E9 | | 51 | 98 | 27 | 8B |   W16 W17 W18 W19 |
| Ключ 5-го раунду (128 бітів) у вигляді матриці байтів: | |  |  |  |  | | --- | --- | --- | --- | | 4A | 65 | A3 | AB | | D2 | 55 | 9E | A2 | | E7 | 03 | B7 | 5E | | 61 | F9 | DE | 55 |   W20 W21 W22 W23 |
| Ключ 6-го раунду (128 бітів) у вигляді матриці байтів: | |  |  |  |  | | --- | --- | --- | --- | | 50 | 35 | 96 | 3D | | 8A | DF | 41 | E3 | | 18 | 18 | AF | F1 | | 03 | FA | 24 | 71 |   W24 W25 W26 W27 |
| Ключ 7-го раунду (128 бітів) у вигляді матриці байтів: | |  |  |  |  | | --- | --- | --- | --- | | 01 | 34 | A2 | 9F | | 2B | F4 | B5 | 56 | | B8 | A0 | 0F | FE | | 24 | DE | FA | 8B |   W28 W29 W30 W31 |
| Ключ 8-го раунду (128 бітів) у вигляді матриці байтів: | |  |  |  |  | | --- | --- | --- | --- | | 30 | 04 | A6 | 39 | | 90 | 64 | D1 | 87 | | 85 | 25 | 2A | D4 | | FF | 21 | DB | 50 |   W32 W33 W34 W35 |
| Ключ 9-го раунду (128 бітів) у вигляді матриці байтів: | |  |  |  |  | | --- | --- | --- | --- | | 3C | 8 | 9E | A7 | | D8 | BC | 6D | EA | | D6 | F3 | D9 | 0D | | ED | CC | 17 | 47 |   W36 W37 W38 W39 |
| Ключ 10-го раунду (128 бітів) у вигляді матриці байтів: | |  |  |  |  | | --- | --- | --- | --- | | 8D | B5 | 2D | 8C | | 0F | B3 | DE | 34 | | 76 | 85 | 5C | 51 | | B1 | 7D | 6A | 2D |   W40 W41 W42 W43 |

Зашифрування блоків

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Блок повідомлення (128 бітів) у 16-ій системі числення: | |  |  |  |  | | --- | --- | --- | --- | | 28 | 48 | 49 | 29 | | 20 | 40 | 41 | 21 | | 58 | B8 | 79 | 18 | | 50 | D1 | 51 | 10 | |
| Блок повідомлення (128 бітів) у вигляді матриці стану: | |  |  |  |  | | --- | --- | --- | --- | | 0F | C4 | 3E | 2E | | 2D | F0 | 5A | B5 | | 0F | 65 | 50 | A2 | | 6C | 7E | A6 | 96 | |
| Додавання матриці стану з початковим ключем (AddRoundKey): | |  |  |  |  | | --- | --- | --- | --- | |  |  |  |  | |  |  |  |  | |  |  |  |  | |  |  |  |  | |
| Раунд 1 | |
| Підстановка байтів з використанням Sбоксу (SubBytes): | |  |  |  |  | | --- | --- | --- | --- | | 34 | 52 | 3B | A5 | | B7 | 09 | 83 | FD | | 6A | 6C | B6 | AD | | 53 | 3E | D1 | CA | |
| Зсув рядків (ShiftRows): | |  |  |  |  | | --- | --- | --- | --- | | 34 | 52 | 3B | A5 | | 09 | 83 | FD | B7 | | B6 | AD | 6A | 6C | | CA | 53 | 3E | D1 | |
| Перемішування стовпців (MixColumns): | |  |  |  |  | | --- | --- | --- | --- | | 0F | 2D | 0F | 6C | | C4 | F0 | 65 | FE | | 3E | 5A | 50 | A6 | | 2E | B5 | A2 | 96 | |
| Додавання з ключем 1-го раунду  (AddRoundKey): | |  |  |  |  | | --- | --- | --- | --- | | 57 | B4 | 06 | 7E | | 81 | 6C | 96 | 09 | | 74 | 26 | 48 | C1 | | 29 | 7B | C3 | F3 | |
| Результуюча матриця стану 1-го раунду: | |  |  |  |  | | --- | --- | --- | --- | | 5B | 8D | 06 | 7E | | 81 | 6C | 96 | 09 | | 74 | 26 | 4B | C1 | | 29 | 7B | C3 | F3 | |
| Раунд 2 | |
| Результуюча матриця стану 2-го раунду: | |  |  |  |  | | --- | --- | --- | --- | | F8 | 77 | 6E | 30 | | 38 | 9B | E1 | C7 | | 61 | 19 | 32 | 78 | | 14 | 35 | 60 | A9 | |
| Раунд 3 | |
| Результуюча матриця стану 3-го раунду: | |  |  |  |  | | --- | --- | --- | --- | | C7 | 38 | 19 | 17 | | 6F | 50 | 6 | 7C | | 57 | 6C | 5C | 75 | | 02 | 26 | 16 | BA | |
| Раунд 4 | |
| Результуюча матриця стану 4-го раунду: | |  |  |  |  | | --- | --- | --- | --- | | 0D | F3 | C6 | C1 | | CA | 80 | A2 | FB | | 4D | 0F | 20 | 6C | | 61 | 3D | 66 | D1 | |
| Раунд 5 | |
| Результуюча матриця стану 5-го раунду: | |  |  |  |  | | --- | --- | --- | --- | | C1 | C4 | 60 | 21 | | 66 | E1 | 78 | 05 | | F7 | 59 | BB | 5C | | 35 | 20 | 42 | 67 | |
| Раунд 6 | |
| Результуюча матриця стану 6-го раунду: | |  |  |  |  | | --- | --- | --- | --- | | C6 | 5E | 7A | F8 | | E1 | 62 | 97 | 53 | | 3C | 96 | 1E | 69 | | EA | 1C | C3 | E9 | |
| Раунд 7 | |
| Результуюча матриця стану 7-го раунду: | |  |  |  |  | | --- | --- | --- | --- | | AA | 78 | 62 | 12 | | F9 | 1B | E0 | CC | | C3 | B3 | EA | 01 | | 20 | 76 | 74 | 86 | |
| Раунд 8 | |
| Результуюча матриця стану 8-го раунду: | |  |  |  |  | | --- | --- | --- | --- | | 6B | A4 | 26 | 59 | | 14 | A2 | C3 | 93 | | 62 | C7 | FA | D9 | | 6B | E9 | 0A | 00 | |
| Раунд 9 | |
| Результуюча матриця стану 9-го раунду: | |  |  |  |  | | --- | --- | --- | --- | | CE | AE | 98 | 00 | | 8F | 51 | 7E | 95 | | 3F | A9 | 6C | DB | | AF | 93 | E4 |  | |
| Раунд 10 | |
| Підстановка байтів з використанням Sбоксу (SubBytes): | |  |  |  |  | | --- | --- | --- | --- | | D0 | 3F | 35 | 0F | | 8F | FE | B7 | C1 | | 88 | 6F | F2 | 9E | | 07 | 1A | D4 | F8 | |
| Зсув рядків (ShiftRows): | |  |  |  |  | | --- | --- | --- | --- | | D0 | 3F | 35 | 0F | | FE | B7 | C1 | 8F | | F2 | 9E | 88 | 6F | | F8 | 07 | 1A | D4 | |
| Додавання з ключем 10-го раунду  (AddRoundKey): | |  |  |  |  | | --- | --- | --- | --- | | 5D | 8A | 1E | 83 | | F1 | 04 | 1F | BB | | 84 | 1B | D4 | 3E | | 49 | 7A | 70 | F9 | |
| Результуюча матриця стану 10-го раунду: | |  |  |  |  | | --- | --- | --- | --- | | D0 | 3F | 35 | 0F | | FE | B7 | C1 | 8F | | F2 | 9E | 88 | 6F | | F8 | 07 | 1A | D4 | |
| Результат шифрування блоку: | D0 FE F2 F8 3F B7 9E 07 35 C1 88 1A 0F 8F 6F D4 |

**Контрольні запитання:**

1) Опишіть основні кроки зашифрування за алгоритмом AES.

Шифрування за алгоритмом AES складається з:

I. Початкового додавання раундового ключа.

II. Nr-1 раундів, кожен з яких складається з чотирьох етапів:

* Підстановка байтів;
* Зсув рядків;
* Перемішування стовпців;
* Додавання раундового ключа;

III. Завершального раунду Nr, в якому пропускається перемішування стовпців.

2) Від чого залежить кількість раундів шифрування за алгоритмом AES?

Кількість циклів шифрування Nr залежить від значень Nk:

|  |  |  |  |
| --- | --- | --- | --- |
|  | Nk (довжина ключа) | Nb (Довжина блоку) | Nr (Кількість раундів) |
| AES-128 | 4 (125) | 4 (128) | 10 |
| AES-192 | 6 (192) | 12 |
| AES-256 | 8 (256) | 14 |

3) Яким чином генеруються ключі в AES?

У стандартному шифру AES (Advanced Encryption Standard) ключі

генеруються на основі введених користувачем початкових ключів (які можуть бути 128, 192 або 256 бітами). Алгоритм генерації ключів в AES передбачає

кілька етапів:

- Розширення ключа (Key Expansion): Початковий ключ розширюється до

більш довгого ключа, що використовується для раундів шифрування. У

кожному раунді шифрування використовується окремий підключ, який

формується з початкового ключа.

- Key Schedule (Розкладка ключів): Початковий ключ розкладається на багато

раундових ключів, які використовуються на кожному раунді шифрування.

- Раундові ключі (Round Keys): Початковий ключ розбивається на раундові

ключі, які використовуються для кожного раунду шифрування. Цей процес включає додавання раундових констант та здійснення операцій над бітами ключа для отримання кінцевих раундових ключів.

4) Які особливості дешифрування за алгоритмом

4) Які особливості дешифрування за алгоритмом AES?

I. Перед першим раундом дешифрування виконується операція додавання з ключем.

II. Потім виконується 9 раундів дешифрування, кожен з яких здійснює такі

операції:

- Зсув рядків в зворотному порядку. Байти в останніх трьох рядках матриці

зсуваються циклічно вліво на різне число байт.

- Обернена операція до операції підстановки байтів. Байти матриці

замінюються новими значеннями за таблицею зворотної заміни, що є

інвертованим S-боксом.

- Процедура, зворотна процедурі перемішування стовпців. Кожен стовпець

матриці розглядається як 4-бітовий многочлен над полем GF(28 ) і множиться

на фіксований многочлен.

- Операція додавання з ключем по модулю 2.

III. Завершальний раунд не містить операцію перемішування стовпців.

5) Назвіть основні режими роботи блокових симетричних алгоритмів

шифрування.

− Electronic Codebook (ECB) – режим електронної кодової книги;

− Cipher Block Chaining (CBC) – режим зчеплення блоків зашифрованого тексту;

− Cipher Feedback (CFB) – режим зворотного зв’язку за зашифрованим текстом;

− Output Feedback (OFB) – режим зворотного зв’язку за виходом;

− Counter Mode (CTR) – режим лічильника.