ЛАБОРАТОРНА РОБОТА № 2. ДОСЛІДЖЕННЯ ВЛАСТИВОСТЕЙ БЛОКОВОГО СИМЕТРИЧНОГО ШИФРУ AES

Мета роботи: дослідити процеси шифрування за допомогою алгоритму AES на основі навчальної програми CrypTool 2.

Матеріально-технічне забезпечення: ПК зі встановленим програмним забезпеченням CrypTool 2.

Теоретичні відомості

УДОСКОНАЛЕНИЙ СТАНДАРТ ШИФРУВАННЯ AES

У 1997 році Американський інститут стандартизації NIST (National Institute of Standards & Technology) оголосив конкурс на новий стандарт симетричного криптоалгоритму.

Згідно з вимогами конкурсу, алгоритм мав обов'язково:

- ✓ бути симетричним;
- ✓ бути блокових шифром;
- ✓ мати довжину блока 128 біт і підтримувати три довжини ключа: 128, 192 і 256 біт.

2 жовтня 2000 року NIST оголосив переможця. Ним став бельгійський алгоритм RIJNDAEL. У 2001 році алгоритм був затверджений як стандарт шифрування та отримав назву AES – Advanced Encryption Standard (удосконалений стандарт шифрування).

Математична база

Скінченне поле GF(2^8) складається з многочленів вигляду

$$a(x) = a_7x^7 + a_6x^6 + a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0, \text{ де } a_i \in \{0,1\}.$$

У вигляді многочлена $a(x)$ скінченого поля GF(2^8) можна подати будь-який байт, що складається з бітів $a_7a_6a_5a_4a_3a_2a_1a_0$.

<u>Приклад 2.1:</u>

Байт: 01011010.

Многочлен:

$$0 \cdot x^7 + 1 \cdot x^6 + 0 \cdot x^5 + 1 \cdot x^4 + 1 \cdot x^3 + 0 \cdot x^2 + 1 \cdot x^1 + 0 = x^6 + x^4 + x^3 + x.$$

Операції над елементами скінченого поля GF(2^8) вводяться наступним чином.

Додавання

$\forall a(x), b(x) \in GF(2^8)$

$a(x) + b(x) = c(x) = c_7x^7 + c_6x^6 + c_5x^5 + c_4x^4 + c_3x^3 + c_2x^2 + c_1x + c_0,$

де $c_i = a_i \oplus b_i, i = 0,1, \dots,7.$

Приклад 2.2: У двійковій формі:

$$\begin{array}{r} 10110001 \\ 10001111 \\ \hline 00111110. \end{array}$$

Те саме у вигляді многочленів:

$$(x^7 + x^5 + x^4 + 1) + (x^7 + x^3 + x^2 + x + 1) = x^5 + x^4 + x^3 + x^2 + x.$$

Множення

Щоб задати множення у полі GF(2^8), потрібно спочатку зафіксувати нерозкладний многочлен степеня 8 з коефіцієнтами із множини $\{0,1\}$ (нерозкладність означає, що він ділиться лише на себе і на одиницю). Таких многочленів є декілька, автори AES вибрали такий:

$$m(x) = x^8 + x^4 + x^3 + x + 1 = 11B_{16}$$

Два елементи поля GF(2^8) множать за модулем $m(x)$ так:

1) Множать як звичайні многочлени.
2) Проміжний результат ділять на $m(x)$ і за остаточний результат приймають остачу від ділення.

Приклад 2.3:

1) $(x^6 + x^5 + x^4 + x^2) \cdot (x^7 + x^5 + x^4 + x) = x^{13} + x^{11} + x^{10} + x^7 + x^{12} + x^{10} + x^9 + +x^6 + x^{11} + x^9 + x^8 + x^5 + x^9 + x^7 + x^6 + x^3 = x^{13} + x^{12} + x^9 + x^8 + x^5 + x^3.$

2)

$$\begin{array}{l|l} x^{13} + x^{12} + x^9 + x^8 + x^5 + x^3 & x^8 + x^4 + x^3 + x + 1 \\ \hline x^{13} + x^9 + x^8 + x^6 + x^5 & x^5 + x^4 + 1 \\ \hline x^{12} + x^6 + x^3 & \\ x^{12} + x^8 + x^7 + x^5 + x^4 & \\ \hline x^8 + x^7 + x^6 + x^5 + x^4 + x^3 & \\ x^8 + x^4 + x^3 + x + 1 & \\ \hline x^7 + x^6 + x^5 + x + 1 & \end{array} .$$

Звідси

$$(x^{13} + x^{12} + x^9 + x^8 + x^5 + x^3) \ mod \ (x^8 + x^4 + x^3 + x + 1) = x^7 + x^6 + x^5 + x + 1.$$

Алгоритм AES

AES є симетричним ітеративним блоковим алгоритмом шифрування зі 128 довжиною блока та зі змінною довжиною ключа. Довжина ключа може дорівнювати 128, 192 або 256 бітів. На відміну від DES, алгоритм AES не використовує збалансовану мережу Фейстеля. AES базується на архітектурі SQUARE (КВАДРАТ), для якої характерно:

1) представлення блоку у вигляді масиву байтів;
2) шифрування за один раунд всього блоку даних;
3) виконання криптографічних перетворень, як над окремими байтами масиву, так і над його рядками і стовпцями.

Блок проміжного результату називають **станом**. Матриця стану має 4 рядки та 4 стовпці (Nb).

Матриця стану при Nb=4:

$$\begin{pmatrix} s_{0,0} & s_{0,1} & s_{0,2} & s_{0,3} \\ s_{1,0} & s_{1,1} & s_{1,2} & s_{1,3} \\ s_{2,0} & s_{2,1} & s_{2,2} & s_{2,3} \\ s_{3,0} & s_{3,1} & s_{3,2} & s_{3,3} \end{pmatrix}.$$

Основним елементом, яким оперує алгоритм AES, є байт – послідовність 8 біт, що обробляються як єдине ціле.

Задавати значення байта зручно в шістнадцятковій системі числення. Для цього байт ділиться на дві групи з 4-х біт: група старших біт в байті представляється першим шістнадцятковим символом, а група молодших біт – другим. Наприклад, для байта 10101100 отримаємо: 10101100 = 1010 1100 = AC.

Приклад 2.4:

Розглянемо перетворення тексту у матрицю:

Відкритий текст: A SECRET MESSAGE

У шістнадцятковому вигляді: 41 20 53 45 43 52 45 54 20 4D 45 53 53 41 47 45.

Отримаємо:

$$\begin{pmatrix} 41 & 43 & 20 & 53 \\ 20 & 52 & 4D & 41 \\ 53 & 45 & 45 & 47 \\ 45 & 54 & 53 & 45 \end{pmatrix}.$$

Ключ шифру розглядають як матрицю байтів, яка має 4 рядки і кількість стовпців (Nk), що дорівнює довжині ключа, поділеній на 32.

Матриця ключа шифру при *Nk*=4:

$$\begin{pmatrix} k_{0,0} & k_{0,1} & k_{0,2} & k_{0,3} \\ k_{1,0} & k_{1,1} & k_{1,2} & k_{1,3} \\ k_{2,0} & k_{2,1} & k_{2,2} & k_{2,3} \\ k_{3,0} & k_{3,1} & k_{3,2} & k_{3,3} \end{pmatrix}.$$

Вхідні та вихідні дані розглядають як одновимірні масиви з індексами 0,...,*Nb*-1. Елементами масиву є байти. Ці блоки мають довжину 16, 24 або 32 байти.

Кількість циклів шифрування *Nr* залежить від значень *Nk*:

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

Шифрування за алгоритмом AES складається з:

I. Початкового додавання раундового ключа.

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

1. Підстановка байтів;
2. Зсув рядків;
3. Перемішування стовпців;
4. Додавання раундового ключа.

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

Розглянемо кожен з чотирьох етапів детальніше.

Підстановка байтів

Виконується окремо для кожного байта і складається з двох послідовних перетворень.

1. Байт розглядають як елемент поля GF(2^8). Якщо він ненульовий, до нього шукають обернений відносно множення в полі GF(2^8). Якщо ж байт нульовий, оберненого не існує. Тому нульовому байту 00000000 відповідає він сам.

2. Над утвореним байтом виконують таке перетворення:

$$\begin{pmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{pmatrix} \oplus \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}.$$

На основі цих двох перетворень створено спеціальну таблицю замін байтів в шістнадцятковій системі, що називається *S*-боксом (табл. 2.1):

Таблиця 2.1. S-бокс алгоритму AES

		y															
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
x	0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
	1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
	2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
	3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
	4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
	5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
	6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
	7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
	8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
	9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
	a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
	b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
	c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
	d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
	e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
	f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Приклад 2.5:

Отриману матрицю із прикладу 4.4 перетворимо за допомогою *S*-боксу:

$$\begin{pmatrix} 41 & 43 & 20 & 53 \\ 20 & 52 & 4D & 41 \\ 53 & 45 & 45 & 47 \\ 45 & 54 & 53 & 45 \end{pmatrix} \Rightarrow \begin{pmatrix} 83 & 1A & B7 & ED \\ B7 & 00 & E3 & 83 \\ ED & 6E & 6E & A0 \\ 6E & 20 & ED & 6E \end{pmatrix}.$$

Зсув рядків

Рядки стану циклічно зсувають на різні кількості байтів:

Nb	Кількість зсувів...			
	0-го рядка (-)	1-го рядка (*C1*)	2-го рядка (*C2*)	3-го рядка (*C3*)
4	0	1	2	3
6	0	1	2	3
8	0	1	3	4

Обернення етапу зсуву рядків полягає у циклічному зсуві праворуч трьох нижніх рядків на *Nb-C1*, *Nb-C2*, *Nb-C3* байтів відповідно.

Перемішування стовпців

Стовпці стану розглядають як многочлен над полем GF(2^8) та множать за модулем $x^4 + 1$ на фіксований многочлен $c(x)$:

$$c(x) = 03_{16} \cdot x^3 + 01_{16} \cdot x^2 + 01_{16} \cdot x + 02_{16}.$$

Якщо $a(x)$ – стовпець до застосування до нього перемішування, а $b(x)$ – після, то перетворення можна записати так:

$$b(x) = c(x) \otimes a(x),$$

або у матричному вигляді:

$$\begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{pmatrix} = \begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \cdot \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{pmatrix}.$$

Додавання раундового ключа

Побітове додавання за модулем 2 раундового ключа до відповідних бітів, отриманих у попередньому циклі. Раундовий ключ отримують з розширеного ключа шифру. Довжина раундового ключа дорівнює довжині блока *Nb*.

Генерація ключів. *Розширений ключ* – одновимірний масив 4-байтових слів – позначають $W[Nb \cdot (Nr + 1)]$.

Алгоритм розширення ключа при Nk ≤ 6

1. Перші *Nk* 4-байтових слів $W[i]$ послідовно вибираються з ключа шифру: 0-е слово – перші чотири байти, 1-е слово – другі чотири байти і т.д.

2. У слові $W[i-1]$ виконують циклічний зсув байтів за схемою: $(a,b,c,d) \Rightarrow (b,c,d,a)$, де a,b,c,d – байти.

3. Потім до кожного з 4-х байтів одержаного слова застосовують *S*-блок. До результату додають раундову сталу за модулем 2 (табл. 2.2).

Таблиця 2.2. Масив раундових констант Rcon

01	02	04	08	10	20	40	80	1B	36
00	00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00	00

4. Решту слів $W[i]$ визначають за формулою: $W[i] = W[i - Nk] \oplus W[i-1]$

При *Nk* > *6* виконується те саме, за винятком одного: якщо $i - 4$ кратне *Nk*, то перед кроком 4 до кожного байта слова ще раз застосовують *S*-блок.

Дешифрування:

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

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

1. Зсув рядків в зворотному порядку. Байти в останніх трьох рядках матриці зсуваються циклічно вліво на різне число байт.

2. Обернена операція до операції підстановки байтів. Байти матриці замінюються новими значеннями за таблицею зворотної заміни, що є інвертованим *S*-боксом (табл. 2.2).

Таблиця 2.2. Інвертований S-бокс алгоритму AES

x \ y	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	52	09	6a	d5	30	36	a5	38	bf	40	a3	9e	81	f3	d7	fb
1	7c	e3	39	82	9b	2f	ff	87	34	8e	43	44	c4	de	e9	cb
2	54	7b	94	32	a6	c2	23	3d	ee	4c	95	0b	42	fa	c3	4e
3	08	2e	a1	66	28	d9	24	b2	76	5b	a2	49	6d	8b	d1	25
4	72	f8	f6	64	86	68	98	16	d4	a4	5c	cc	5d	65	b6	92
5	6c	70	48	50	fd	ed	b9	da	5e	15	46	57	a7	8d	9d	84
6	90	d8	ab	00	8c	bc	d3	0a	f7	e4	58	05	b8	b3	45	06
7	d0	2c	1e	8f	ca	3f	0f	02	c1	af	bd	03	01	13	8a	6b
8	3a	91	11	41	4f	67	dc	ea	97	f2	cf	ce	f0	b4	e6	73
9	96	ac	74	22	e7	ad	35	85	e2	f9	37	e8	1c	75	df	6e
a	47	f1	1a	71	1d	29	c5	89	6f	b7	62	0e	aa	18	be	1b
b	fc	56	3e	4b	c6	d2	79	20	9a	db	c0	fe	78	cd	5a	f4
c	1f	dd	a8	33	88	07	c7	31	b1	12	10	59	27	80	ec	5f
d	60	51	7f	a9	19	b5	4a	0d	2d	e5	7a	9f	93	c9	9c	ef
e	a0	e0	3b	4d	ae	2a	f5	b0	c8	eb	bb	3c	83	53	99	61
f	17	2b	04	7e	ba	77	d6	26	e1	69	14	63	55	21	0c	7d

3. Процедура, зворотна процедурі перемішування стовпців. Кожен стовпець матриці розглядається як 4-бітовий многочлен над полем GF(2^8) і множиться на фіксований многочлен:

$c^{-1}(x) = 0b_{16} \cdot x^3 + 0d_{16} \cdot x^2 + 09_{16} \cdot x + 0e_{16}$ по модулю многочлена x^4+1.

Таку операцію можна записати в матричному вигляді:

$$\begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{pmatrix} = \begin{pmatrix} 0e & 0b & 0d & 09 \\ 01 & 0e & 0b & 0d \\ 0d & 09 & 0e & 0b \\ 0b & 0d & 01 & 0e \end{pmatrix} \cdot \begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{pmatrix}$$

4. Операція додавання з ключем по модулю 2.

III. Завершальний раунд не містить операцію перемішування стовпців.

Завдання до лабораторної роботи

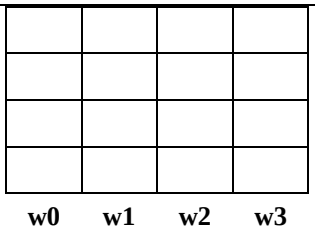
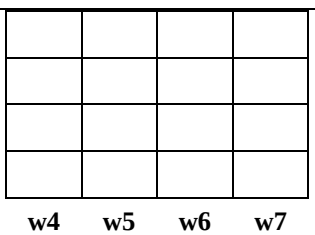
Завдання 1

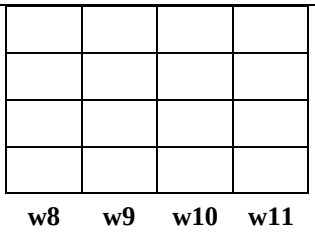
Виконати зашифрування блоку даних відкритого тексту за допомогою алгоритму AES на основі навчальної програми CrypTool 2 (Templates⇒Cryptography⇒ Modern⇒Symmetric⇒AES Visualization) згідно варіанту.

Варіант №	Блок відкритого тексту	Ключ
1.	0102030405060708090101112131415 16	0102030405060708090A0B0C0D0E0F00
2.	1020304050607080901011121314151 60	020406080A0C0E10121416181A1C1E00
3.	0203040506070809101112131415160 1	04080C0014181C2024282C3034383C00
4.	2030405060708091011121314151601 0	0810180028303840485058606870780 0
5.	0304050607080910111213141516010 2	10203000506070809 0A0B0C0D0E0F000
6.	3040506070809101112131415160102 0	20406000A0C0E10121416181A1C1E000
7.	0405060708091011121314151601020 3	4080C1014181C2024282C3034383C000
8.	4050607080910111213141516010203 0	8101820283038404850586068707800 0
9.	0506070809101112131415160102030 4	0203040506070809 0A0B0C0D0E0F0001
10.	5060708091011121314151601020304 0	0406080A0C0E10121416181A1C1E0002
11.	0607080910111213141516010203040 5	080C1004181C2024282C3034383C0004
12.	6070809101112131415160102030405 0	1018200830384048505860687078000 8

1.1. Сформувати раундові ключі для зашифрування даних. У звіті описати зі скріншотами кроки алгоритму генерації ключів згідно схеми:

Генерація ключів

Ключ (128 бітів) у 16-ій системі числення:	
Початковий ключ (128 бітів) у вигляді матриці байтів:	 **w0 w1 w2 w3**
Циклічний зсув **w3**:	
Результат заміни кожного байту **w3** з використанням S-боксу:	
w4 = SubBytes(**w3**) ⊕ Rcon(1) ⊕ **w0**:	
w5 = **w1** ⊕ **w4**:	
w6 = **w2** ⊕ **w5**:	
w7 = **w3** ⊕ **w6**:	
Ключ 1-го раунду (128 бітів) у вигляді матриці байтів:	 **w4 w5 w6 w7**

Ключ 2-го раунду (128 бітів) у вигляді матриці байтів:	
…	
Ключ 10-го раунду (128 бітів) у вигляді матриці байтів:	

Зашифрування блоку

Блок повідомлення (128 бітів) у 16-ій системі числення:	
Блок повідомлення (128 бітів) у вигляді матриці стану:	
Додавання матриці стану з початковим ключем (AddRoundKey):	
Раунд 1	
Підстановка байтів з використанням S-боксу (SubBytes):	
Зсув рядків (ShiftRows):	
Перемішування стовпців (MixColumns):	
Додавання з ключем 1-го раунду (AddRoundKey):	
Результуюча матриця стану 1-го раунду:	
Раунд 2	
Результуюча матриця стану 2-го раунду:	
Раунд 3	
Результуюча матриця стану 3-го раунду:	
…	
Раунд 10	
Підстановка байтів з використанням S-боксу (SubBytes):	
Зсув рядків (ShiftRows):	
Додавання з ключем 10-го раунду (AddRoundKey):	
Результуюча матриця стану 10-го раунду:	
Результат шифрування блоку:	

Контрольні запитання:

1. Опишіть основні кроки зашифрування за алгоритмом AES.
2. Від чого залежить кількість раундів шифрування за алгоритмом AES?
3. Яким чином генеруються ключі в AES?
4. Які особливості дешифрування за алгоритмом AES?
5. Назвіть основні режими роботи блокових симетричних алгоритмів шифрування.