Вінницький національний технічний університет

Розробка апаратної платформи для реалізації SHA-алгоритмів на FPGA"

магістерська кваліфікаційна робота

Керівник – к.т.н. доц. Воловик А.Ю.

Розробив студент гр. РТ-19м Прокопчук С.С.

Вінниця ВНТУ 2020

Структурна схема налагоджувальної плати

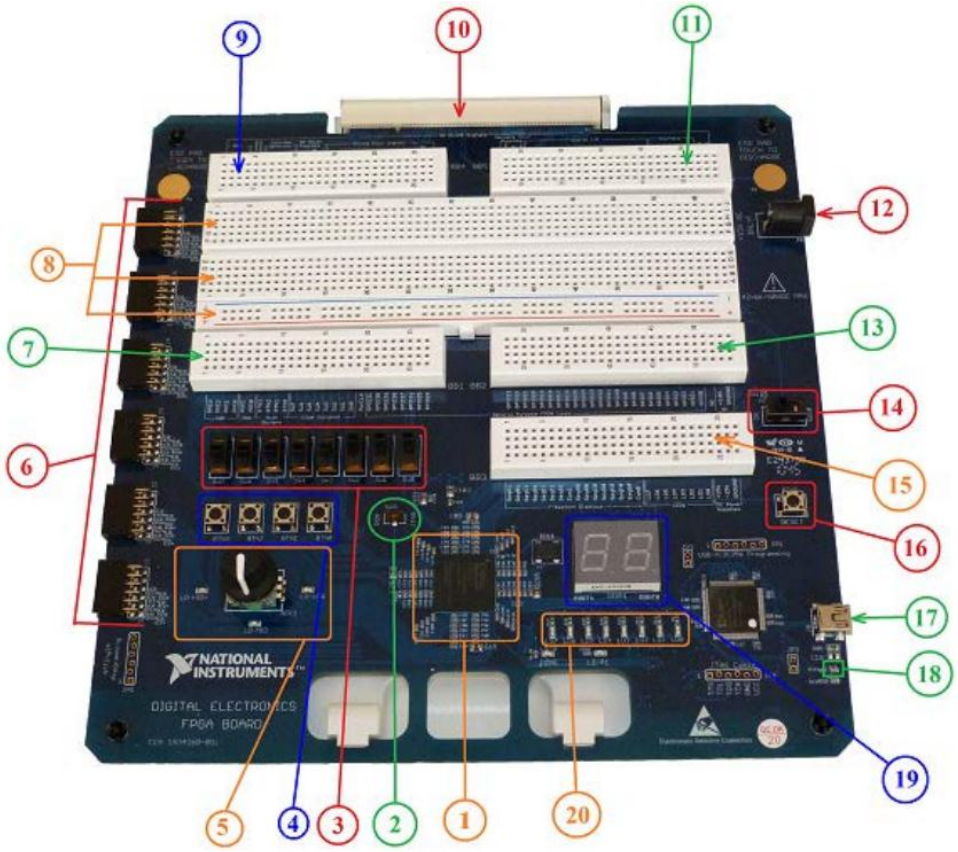


Рисунок Б1 – Налагоджувальна плата NI Digital Electronics FPGA Board

1. ПЛІС XC3S500E Xilinx Spartan - 3E
2. Перемикач SW9
3. Рухомі перемикачі (SW0 - SW7)
4. Кнопки (BTN0 - BTN3)
5. Натискний перемикач
6. Роз'єми Digilent Pmod
7. Зона макетування: сигнальний роз'єм BB1
8. Роз'єми загального призначення
9. Зона макетування: сигнальний роз'єм BB4
10. Роз’єм для підключення до N1 ELVIS II+.
11. Зона макетування: сигнальний роз'єм BB5
12. Роз’єм підключення джерела живлення
13. Зона макетування: сигнальний роз'єм BB2
14. Вимикач живлення
15. Зона макетування: сигнальний роз'єм BB3
16. Кнопка скидання (Reset)
17. Роз'єм USB
18. Світлодіод LD – G
19. Семисегментні індикатори
20. Світлодіоди (LD0 - LD7)

Етапи проектування пристрою в середовищі розробки WebPack ISE

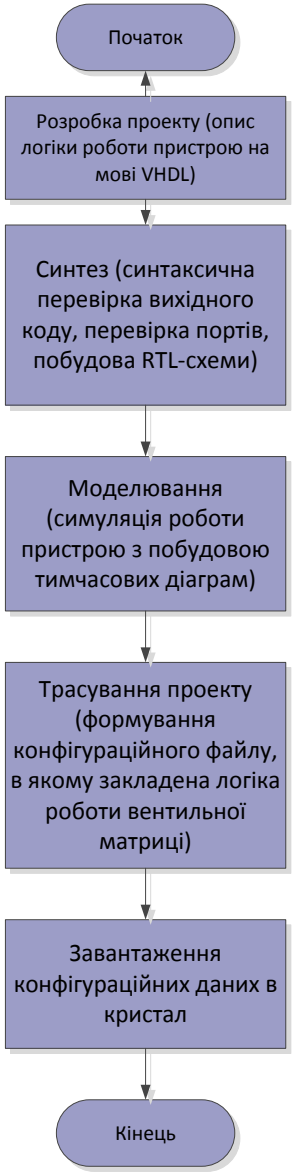
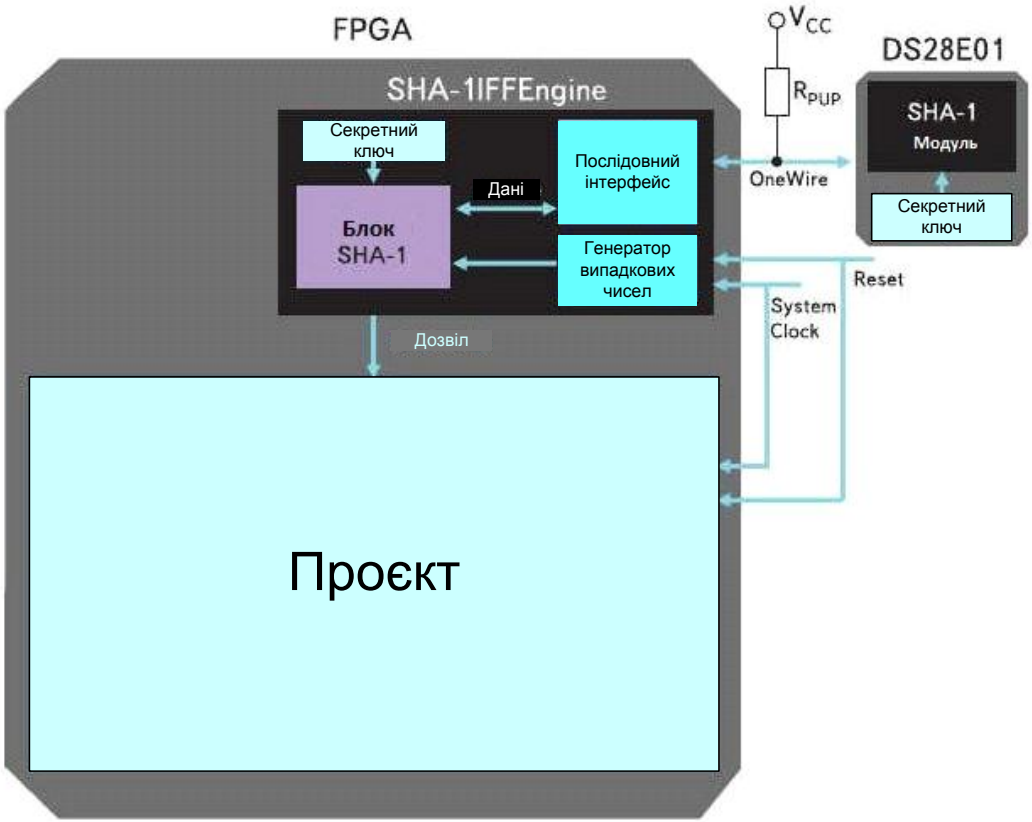


Рисунок В – Етапи проектування пристрою в середовищі розробки WebPack ISE

Реалізація концепції IFF



Рисинок Г1 – Реалізація концепції IFF

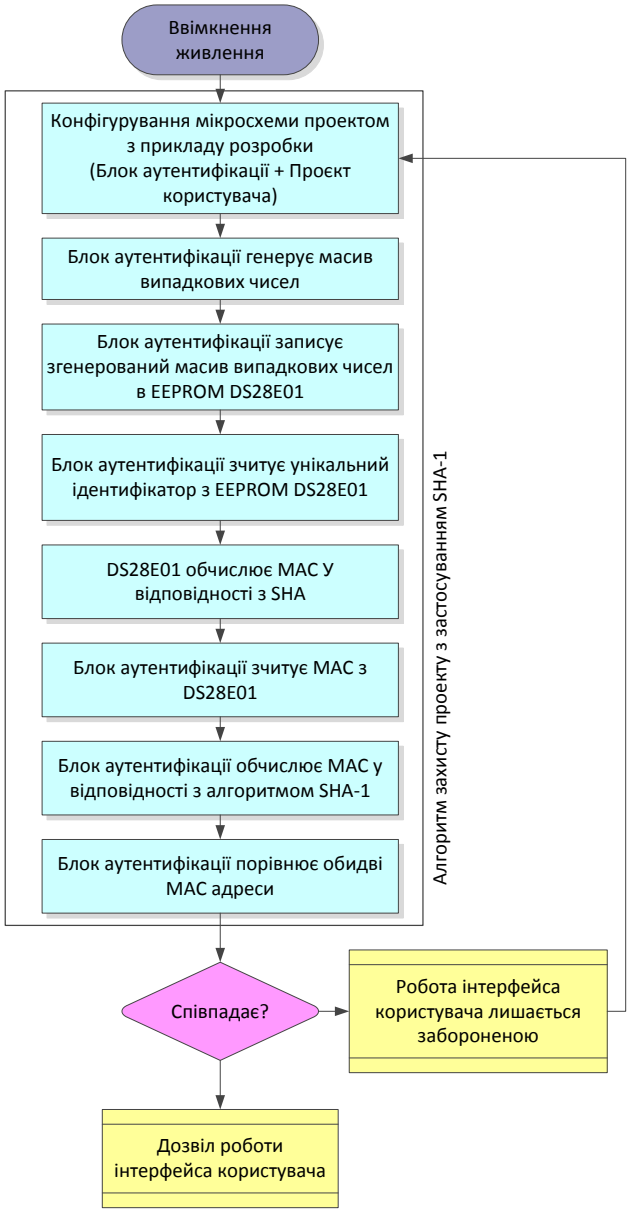


Рисунок Г2 – Алгоритм блоку перевірки при реалізації концепції IFF

Структура алгоритму шифрування. 1

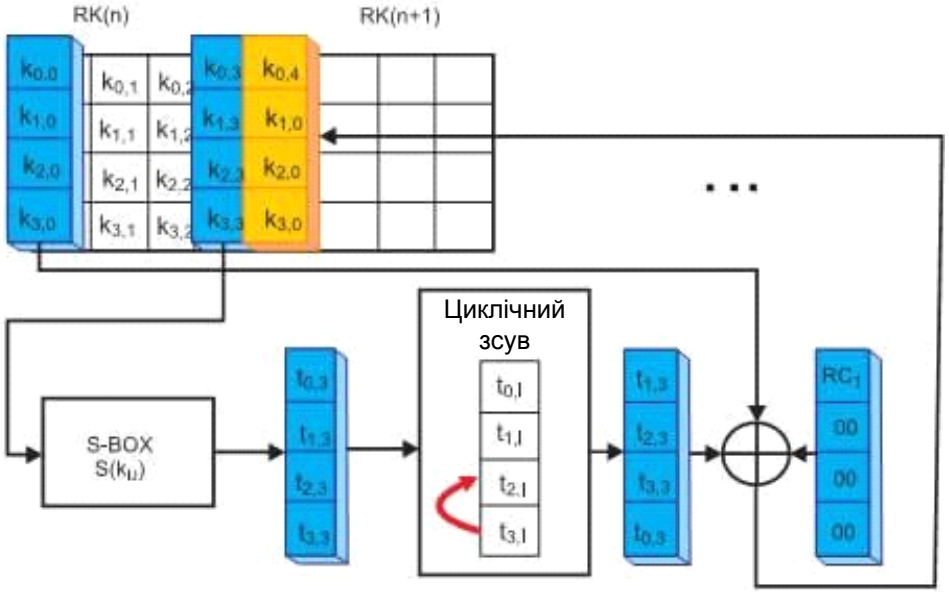


Рисунок Д.1 – Отримання першого стовпця наступного ключа раунду

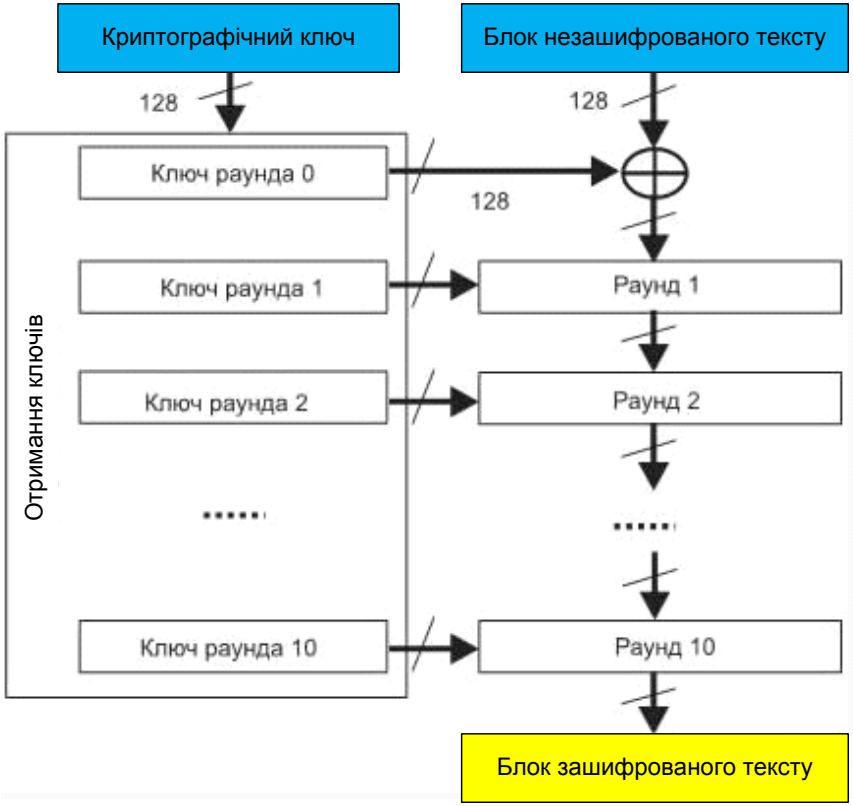


Рисунок Д.2 – Структура алгоритму SHA - 128

Структура алгоритму шифрування. 2

Стан

a_0	a_4	a_8	a_{12}
a_1	a_5	a_9	a_{13}
a_2	a_6	a_{10}	a_{14}
a_3	a_7	a_{11}	a_{15}

Ключ

k_0	k_4	k_8	k_{12}
k_1	k_5	k_9	k_{13}
k_2	k_6	k_{10}	k_{14}
k_3	k_7	k_{11}	k_{15}

Рисунок Д.3 – Структура ключа і стану

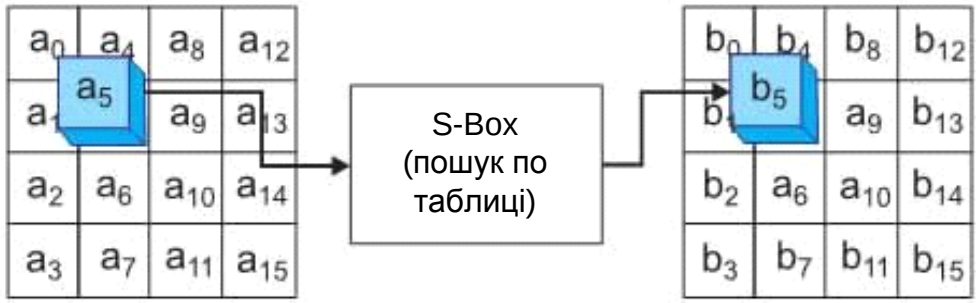


Рисунок Д.5 – Операція заміщення байтів

x \ y	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
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

Рисунок Д.4 – Таблиця S–Box

Структура алгоритму шифрування. 3

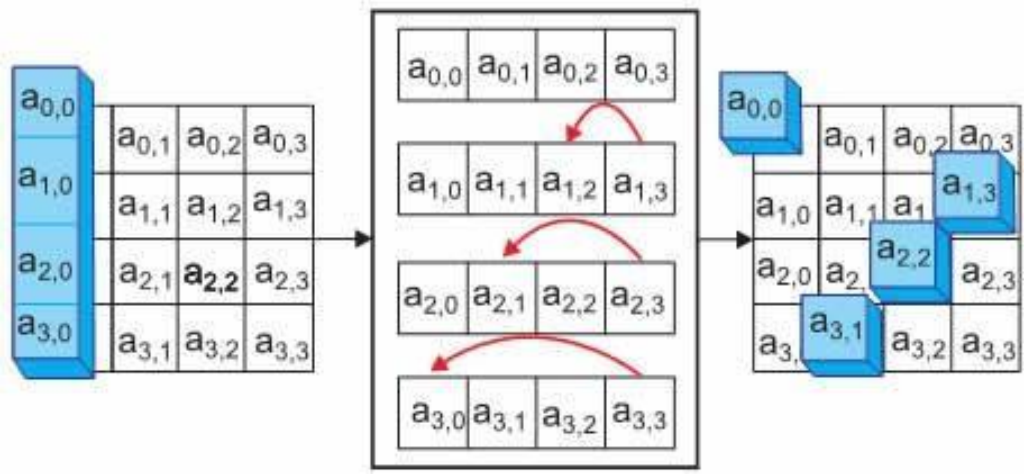


Рисунок Д.6 – Операція зсуву рядків

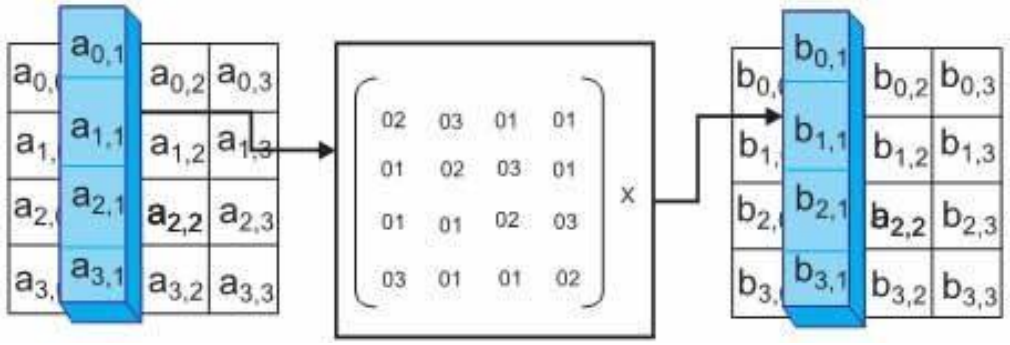


Рисунок Д.7 – Операція перемішування стовпців

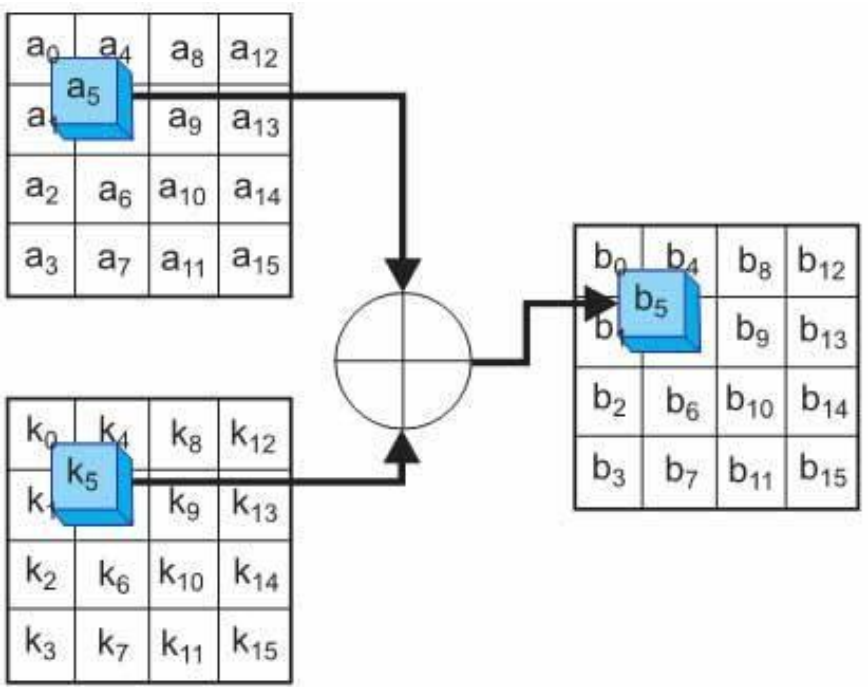


Рисунок Д.8 – Операція додавання ключа раунду

Опис алгоритму модуля аутентифікації

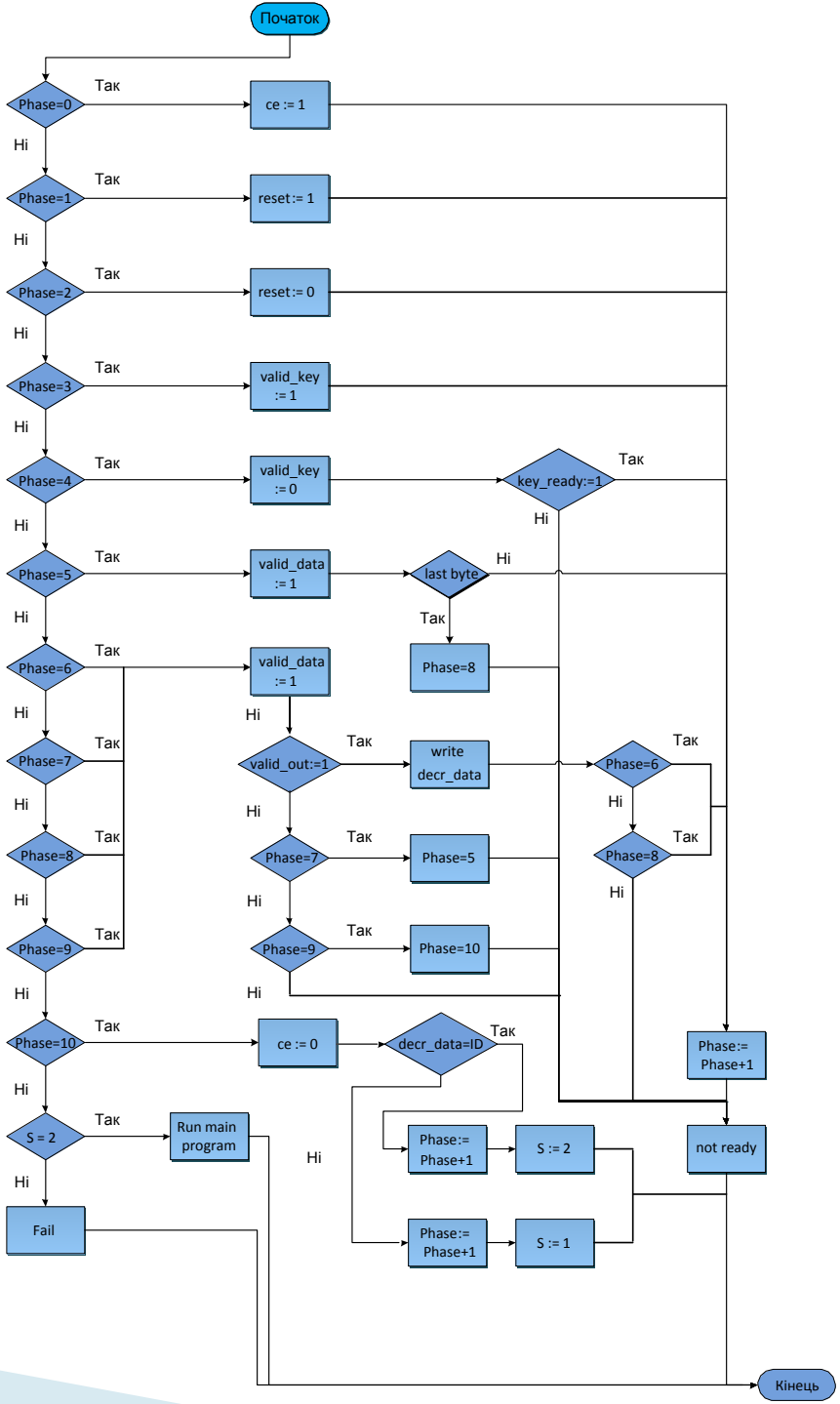


Рисунок Е.1 – Алгоритм аутентифікації серійного номера

Опис перевірки працездатності і результати симуляції. 1

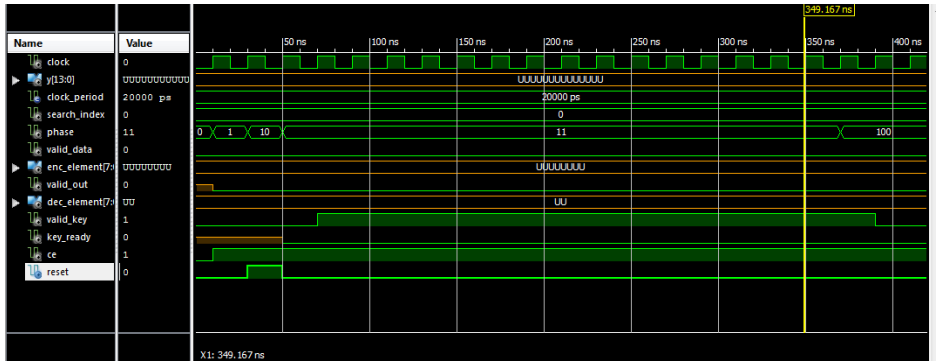


Рисунок Ж.1 – Перші три фази роботи модуля

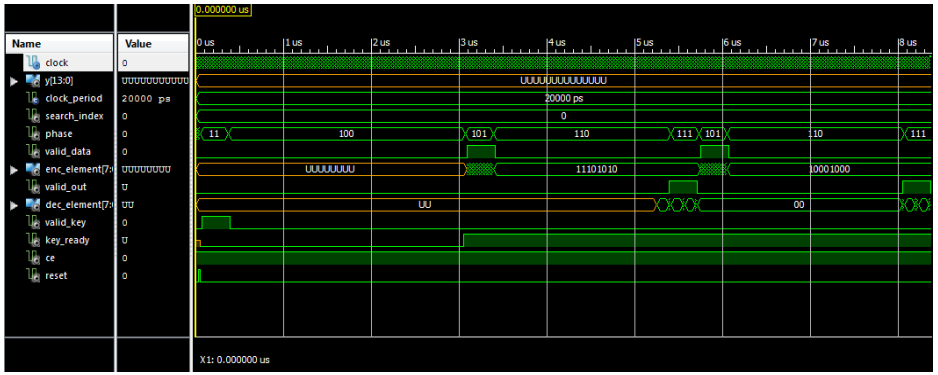


Рисунок Ж.2 – Етапи циклічного запису даних з модуля дешифрування

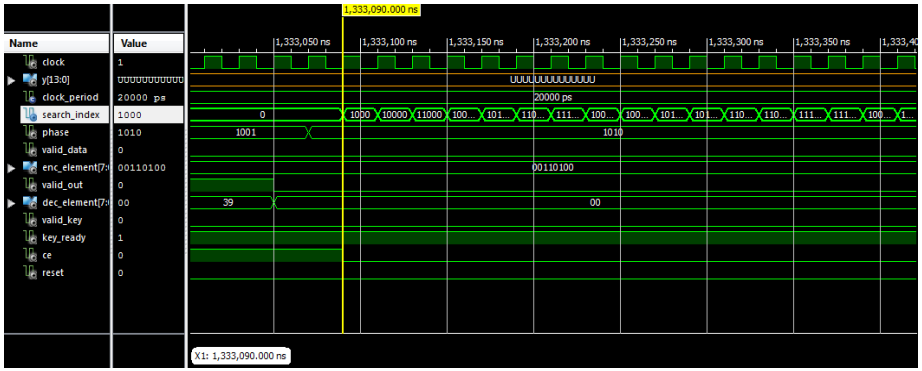


Рисунок Ж.3 – Пошук серійного номера

Опис перевірки працездатності і результати симуляції. 2

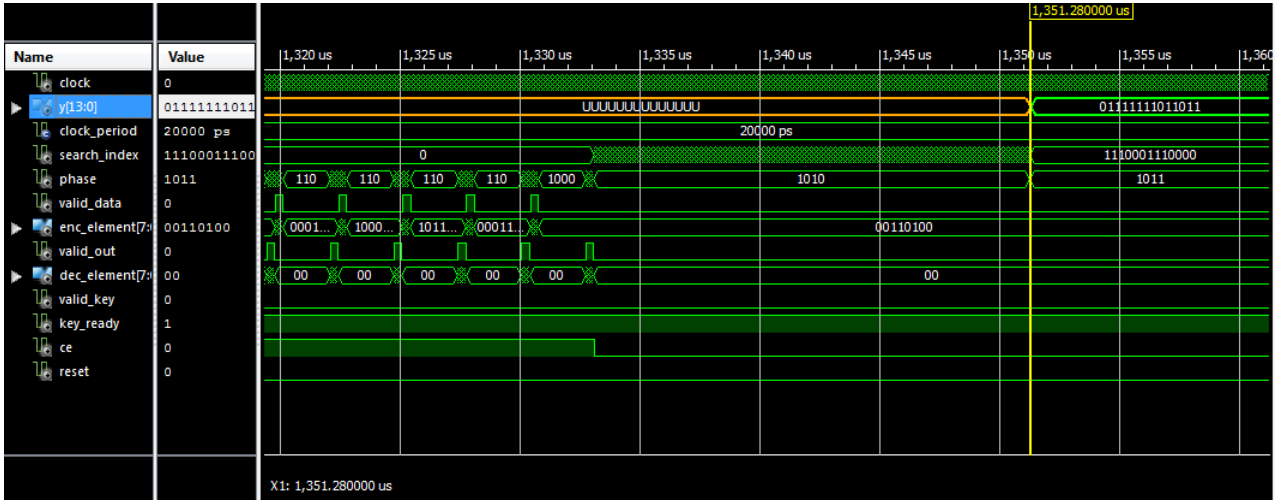


Рисунок Ж.4 – Результат роботи модуля

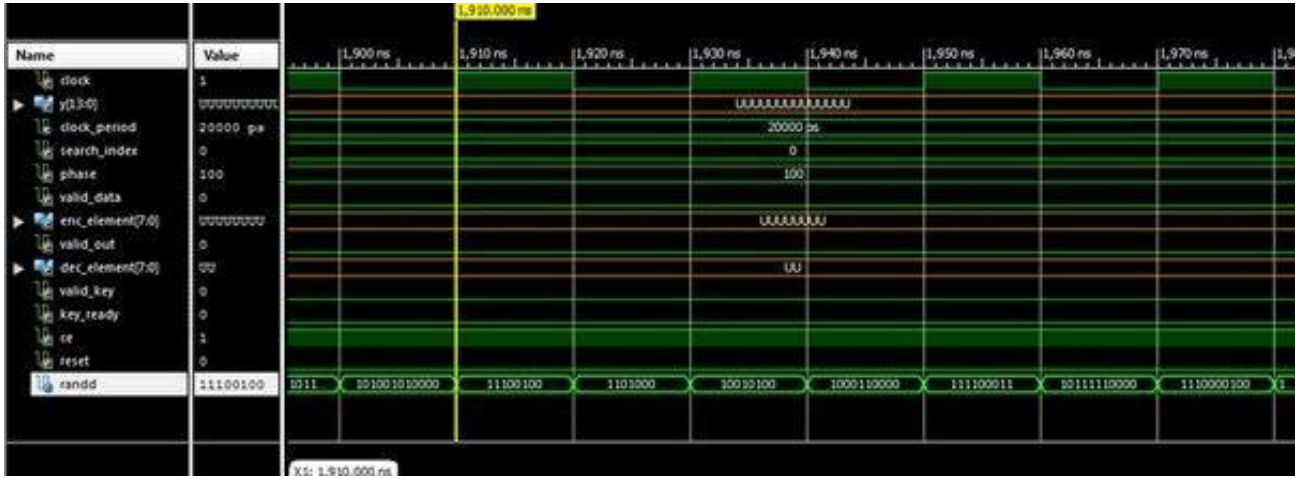


Рисунок Ж.5 – Генерація випадкових чисел

Дякую за увагу!