

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА»
Кафедра комп'ютерної інженерії та кібербезпеки

ЗВІТ З ПЕРЕДДИПЛОМНОЇ ПРАКТИКИ

Тема: «Програмна реалізація алгоритму шифрування Калина»

студента IV курсу групи КБ-19-2
спеціальності 125 «Кібербезпека»

Луцевич Марти Олександрівни

(прізвище, ім'я та по-батькові)

Керівник: старший викладач каф. КІ та КБ

Окунькова Оксана Олексіївна

Національна шкала: _____

Кількість балів: _____

Оцінка: ECTS _____

Члени комісії

(підпис)

О.О. Окунькова

(прізвище та ініціали)

(підпис)

В.В. Воротніков

(прізвище та ініціали)

(підпис)

Ю.М. Росінський

(прізвище та ініціали)

Житомир — 2023

		Луцевич М. О			ДУ «Житомирська політехніка».23.125.9.000 – ПП	Арк.
		Окунькова О.О.				1
Змн.	Арк.	№ докум.	Підпис	Дата		

РЕФЕРАТ

Завданням на переддипломну практику була розробка програми для реалізації алгоритму шифрування «Калина».

Пояснювальна записка до переддипломної практики на тему «Програмна реалізація алгоритму шифрування «Калина»» складається зі вступу, двох розділів, висновку, списку використаної літератури.

Текстова частина викладена на 19 сторінках друкованого тексту.

Пояснювальна записка має список використаних джерел, який містить 5 найменувань і займає 1 сторінку. В роботі наведено 5 рисунків. Загальний обсяг роботи – 19 сторінок.

В першому розділі було наведено теоретичні відомості та розглянуто основні особливості протоколу Active Directory в Windows Server. Розглянуто особливості протоколу LDAP його перевагу та різницю між Active Directory.

У другому розділі було створено та налаштовано домен в Active Directory та також створено декілька користувачів для тестування.

Висновок містить в собі результати розробки проєкту програмної реалізації алгоритму шифрування Калина

КЛЮЧОВІ СЛОВА: КАЛИНА, АЛГОРИТМ ШИФРУВАННЯ, ДСТУ 7624:2014

		Луцевич М. О			ДУ «Житомирська політехніка».23.125.9.000 – ПП	Арк.
		Окунькова О.О.				2
Змн.	Арк.	№ докум.	Підпис	Дата		

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ	4
ВСТУП.....	5
РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ АЛГОРИТМУ ШИФРУВАННЯ	6
1.1 Структура алгоритму шифрування ДСТУ 7624:2014 («Калина»)	6
1.2 Опис алгоритму шифрування та розшифрування.....	6
1.3 Аналіз безпеки та стійкості алгоритму	9
1.4 Порівняння з іншими алгоритмами шифрування	10
Висновки до першого розділу	11
РОЗДІЛ 2. ПРОЕКТУВАННЯ	12
2.1 Опис алгоритмів шифрування на прикладах.....	12
2.2 Обґрунтування вибору мови програмування	16
Висновки до другого розділу	16
ВИСНОВКИ.....	17
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	18

		Луцевич М. О			ДУ «Житомирська політехніка».23.125.9.000 – ПП	Арк.
		Окунькова О.О.				3
Змн.	Арк.	№ докум.	Підпис	Дата		

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

XOR — Виключна диз'юнкція (Exclusive or)

AES — Advanced Encryption Standard

DES — Data Encryption Standard

3DES — Triple DES

		Луцевич М. О			ДУ «Житомирська політехніка».23.125.9.000 – ПП	Арк.
		Окунькова О.О.				4
Змн.	Арк.	№ докум.	Підпис	Дата		

ВСТУП

Актуальність теми. Впровадження надійних алгоритмів шифрування є ключовим елементом забезпечення інформаційної безпеки в сучасному світі, де передача даних через відкриті мережі є невід'ємною частиною багатьох галузей. Алгоритм «Калина» — перспективний алгоритм шифрування, розроблений у співпраці Держспецзв'язку, ПАТ «Інститут інформаційних технологій» та провідних українських вчених під керівництвом Горбенка І.Д.

Тому реалізація алгоритму шифрування Калина є актуальною темою курсової роботи, оскільки цей алгоритм може бути застосований у різних сферах, пов'язаних з інформаційною безпекою, ставши важливим кроком у забезпеченні кібербезпеки в Україні. Така робота корисна студентам, які цікавляться криптографією, програмуванням і безпекою даних, а також викладачам, які хочуть залучити студентів до актуальних тем сучасного інформаційного світу.

Метою дослідження є вивчення можливостей та переваг використання алгоритму шифрування «Калина» для забезпечення захисту інформації.

Об'єктом дослідження є процес розробки програмного додатку алгоритму шифрування «Калина».

Предметом дослідження є алгоритм шифрування «Калина».

		Луцевич М. О			ДУ «Житомирська політехніка».23.125.9.000 – ПП	Арк.
		Окунькова О.О.				5
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ АЛГОРИТМУ ШИФРУВАННЯ

1.1 Структура алгоритму шифрування ДСТУ 7624:2014 («Калина»)

Алгоритм шифрування Калина - це блоковий шифр з ключем довжиною 128, 256 або ж 512 біт. Його названо на честь квітки калини, що символізує національність розробників алгоритму — українців.

Алгоритм Калина складається з наступних етапів:

1. Initialization - налагодження даних: таблиці замін, константи
2. Key Expansion - розширення ключа: генерація раундових ключів для кожного раунду шифрування. Для цього використовується алгоритм розширення ключа на основі симетричних шифрів.
3. Encryption Rounds - раунди шифрування, які включають нелінійні заміни та лінійні перестановки бітів з використанням раундових ключів. Кількість раундів залежить від довжини ключа та рівня безпеки, яку необхідно забезпечити.
4. Output Formatting - упорядкування кінцевих даних у певний формат.

Підсумовуючи, структура алгоритму шифрування Калина складається з комбінації лінійних та нелінійних операцій, що забезпечує захист даних.

1.2 Опис алгоритму шифрування та розшифрування

Алгоритм шифрування Калина використовує ключі розміром 128, 256 або 512 біт і повідомлення, розбиті на блоки фіксованого розміру

Калина використовує перестановки, лінійні перетворення та S-блоки для забезпечення безпеки шифрування.

Основні етапи алгоритму шифрування Калина:

1. Розширення ключа

Для створення довшого ключа алгоритм використовує додавання з нульовим ключем по модулю 2^{64}

2. Шифрування:

		Луцевич М. О.			ДУ «Житомирська політехніка».23.125.9.000 – ПП	Арк.
		Окунькова О.О.				6
Змн.	Арк.	№ докум.	Підпис	Дата		

Після розширення ключа використовуються чотири основні функції: SubBytes (підстановка байтів), ShiftRows (зсув рядків), MixColumn (перемішування стовпців), XOR. Ці функції виконуються у циклі, кількість ітерацій якого залежить від довжини ключа.

На кожній ітерації виконуються такі кроки:

- Підстановка байтів: вхідний блок даних проходить через чотири S-блоки ($\pi_0, \pi_1, \pi_2, \pi_3$), кожен з яких замінює частину блока на нове значення за таблицею заміни.
- Зсув рядків: вхідний блок даних проходить через лінійне перетворення, яке змінює його структуру.
- Перемішування стовпців: перетворення стовпців матриці стану шляхом виконання операцій множення і додавання в скінченному полі $GF(2^8)$ за модулем незвідного многочлена $x^8 + x^4 + x^3 + x^2 + 1$
- XOR: побітове додавання раундового ключа до матриці стану за модулем 2.

Після останньої ітерації отримуємо шифротекст.

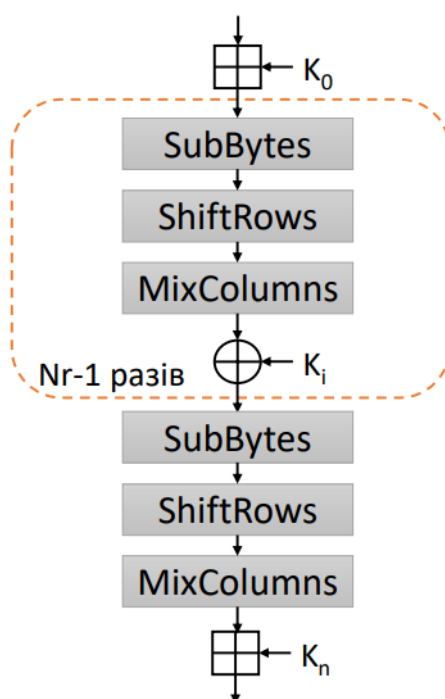


Рисунок 1.1 — Структурна схема алгоритму «Калина» в режимі зашифрування

		Луцевич М. О.			ДУ «Житомирська політехніка».23.125.9.000 – ПП	Арк.
		Окунькова О.О.				7
Змн.	Арк.	№ докум.	Підпис	Дата		

Основні етапи алгоритму розшифрування Калина:

Аналогічно шифруванню, підготовка дешифрування передбачає отримання раундових ключів на основі початкового ключа шифрування. Для цього використовується алгоритм ітераційного розширення ключа, який забезпечує генерацію того ж самого набору раундових ключів, що і при шифруванні.

1. Виконуються операції з п. 2, але на початку замість $\oplus$ (XOR) виконується віднімання по модулю 2^{64} з ключем останнього раунду (InvMixColumns, InvShiftRows, InvSubBytes).
2. Далі використовується чотири основні функції: InvSubBytes (підстановка байтів), ShiftRows (зсув рядків), MixColomn (перемішування стовпців), XOR. Ці функції виконуються у циклі, кількість ітерацій якого залежить від довжини ключа.

На кожній ітерації виконуються такі кроки:

- XOR: побітове додавання раундового ключа до матриці стану за модулем 2.
- Зворотна операція до перемішування стовпців: виконується обернені операції для відновлення початкових значень даних.
- Зсув рядків у зворотному порядку: кожен рядок матриці зсувається вправо на певну кількість позицій, де перший рядок не зсувається, другий рядок зсувається на одну позицію, третій - на дві позиції, а четвертий - на три позиції.
- Обернена операція до підстановки байтів: кожен байт матриці стану замінюється відповідно до оберненої таблиці зворотної заміни

		Луцевич М. О.			ДУ «Житомирська політехніка».23.125.9.000 – ПП	Арк.
		Окунькова О.О.				8
Змн.	Арк.	№ докум.	Підпис	Дата		

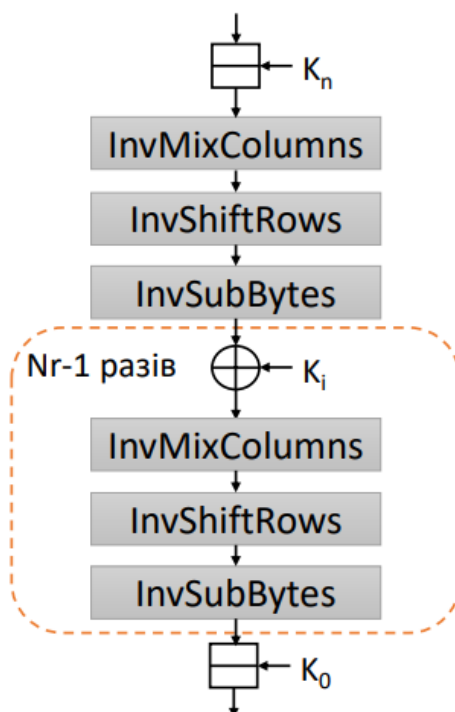


Рисунок 1.2 — Структурна схема алгоритму «Калина» в режимі розшифрування

1.3 Аналіз безпеки та стійкості алгоритму

Однією з головних переваг "Калини" є велика довжина ключа, яка може сягати аж до 512 біт. Це дозволяє збільшити стійкість шифрування і зробити його більш відповідним до сучасних вимог безпеки.

Алгоритм "Калина" використовує операції шифрування, такі як перестановки, змішування та підстановки. Він має складну структуру, яка ускладнює атаки на нього. Крім того, алгоритм відповідає вимогам стандартів безпеки, таких як ISO/IEC 18033-3 та NESSIE, і успішно пройшов багато різних тестів на стійкість і продемонстрував свою високу стійкість до різних типів атак.

Однак, як і у випадку з будь-яким криптографічним алгоритмом, існує можливість знайти уразливості, які можуть бути використані для злому шифрування. Тому, хоча алгоритм "Калина" є досить безпечним, його необхідно регулярно оновлювати та тестувати на наявність можливих уразливостей.

Не можна стверджувати на 100%, що алгоритм "Калина" є абсолютно недоступним для атак. Існують деякі можливі атаки на алгоритм, такі як атака з використанням бічного каналу, деякі атаки на блокові шифри, а також

можливість атак методом перебору, якщо ключ недостатньо довгий. Було виявлено деякі атаки на скорочені варіанти шифру, але вони не є практичними.

Таким чином, можна зробити висновок, що алгоритм Калина є одним з найбільш прогресивних і безпечних блокових шифрів на сьогоднішній день. Його можна використовувати для шифрування даних в різних сферах, включаючи фінанси, медицину, телекомунікації і багато іншого.

1.4 Порівняння з іншими алгоритмами шифрування

Алгоритм "Калина" доволі новий алгоритм (2015 рік), і його ще не так багато досліджували порівняно з іншими популярними алгоритмами шифрування, такими як AES, 3DES і DES.

Однією з основних переваг "Калини" є те, що вона підтримує ключі довжиною до 512 біт, що дозволяє збільшити стійкість шифрування та зробити його більш відповідним до сучасних вимог безпеки. Крім того, "Калина" використовує безпечні операції шифрування, що ускладнює атаки на нього.

Розглянемо основні аспекти алгоритмів:

Швидкодія: алгоритм має гарну швидкої порівнюючи з AES та DES. Особливо це видно при використанні ключа на 256 біт. Проте якщо розглядати ключ на 128 біт, AES є набагато швидшим.

Розмір ключа: «Калина» допускає довжину ключа від 128 до 256 біт, що забезпечує високий рівень стійкості до атак. Однак інші алгоритми, такі як Blowfish/RSA, допускають довжину ключа до 448/4096 біт, що забезпечує вищий рівень стабільності.

Стійкість до атак: "Калина" забезпечує високий рівень стійкості до атак, особливо, при використанні ключів довжиною 256 та 512 біт. Водночас AES також є дуже стійким до атак.

Підводячи підсумок, обираючи алгоритм шифрування, варто звертати увагу на багато факторів: стійкість, швидкодія, доступність. «Калина» є стійким, безпечним алгоритмом та гарним вибором для захисту конфіденційної інформації.

		Луцевич М. О.			ДУ «Житомирська політехніка».23.125.9.000 – ПП	Арк.
		Окунькова О.О.				10
Змн.	Арк.	№ докум.	Підпис	Дата		

Висновки до першого розділу

В даному розділі було описано структуру алгоритму шифрування, представлений опис алгоритму для шифрування та розшифрування, проведено аналіз безпеки та стійкості алгоритму, а також порівняння з іншими алгоритмами.

		Луцевич М. О			ДУ «Житомирська політехніка».23.125.9.000 – ПП	Арк.
		Окунькова О.О.				11
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 2. ПРОЄКТУВАННЯ

2.1 Опис алгоритмів шифрування на прикладах

Розглянемо основні етапи формування ключів, шифрування на прикладах:

1. Формування початкової матриці стану

При формуванні допоміжного ключа, виникає потреба в роз'ясненні моменту формування початкової матриці стану: що за формули і звідки беруться числа. Маючи початковий ключ і умову, почнемо розгляд:

Ключ: «довільний». Потрібно сформувати допоміжний ключ на основі іншого ключа, за довжиною 128 біт.

Згідно з таблицею 2.1, при ключі в 128 біт маємо значення $N_k = 2$. Тоді значення $N_b = 2$.

Таблиця 2.1

Кількість раундів шифрування алгоритму «Калина»

Розмір блоку	Кількість раундів шифрування для різних довжин ключа		
	Довжина ключа 128 бітів ($N_k = 2$)	Довжина ключа 256 бітів ($N_k = 4$)	Довжина ключа 512 бітів ($N_k = 8$)
128 ($N_b = 2$)	10	14	-
256 ($N_b = 4$)	-	14	18
512 ($N_b = 8$)	-	-	18

По формулі $N_b + N_k + 1 = 2 + 2 + 1 = 5$ вираховували, що початкова матриця стану буде мати такий вигляд:

05	00
00	00
00	00
00	00
00	00
00	00
00	00
00	00

		Луцевич М. О.			ДУ «Житомирська політехніка». 23.125.9.000 – ПП	Арк.
		Окунькова О.О.				12
Змн.	Арк.	№ докум.	Підпис	Дата		

2. SubByted (Підстановка байтів)

При операції підстановки байтів кожен байт матриці стану замінюється відповідно до заданої таблиці підстановки. Всього таблиць 4:

Підстановка π_0: <pre> A8 43 5F 06 6B 75 6C 59 71 DF 87 95 17 F0 D8 09 6D F3 1D CB C9 4D 2C AF 79 E0 97 FD 6F 4B 45 39 3E DD A3 4F B4 B6 9A 0E 1F BF 15 E1 49 D2 93 C6 92 72 9E 61 D1 63 FA EE F4 19 D5 AD 58 A4 BB A1 DC F2 83 37 42 E4 7A 32 9C CC AB 4A 8F 6E 04 27 2E E7 E2 5A 96 16 23 2B C2 65 66 0F BC A9 47 41 34 48 FC B7 6A 88 A5 53 86 F9 5B DB 38 7B C3 1E 22 33 24 28 36 C7 B2 3B 8E 77 BA F5 14 9F 08 55 9B 4C FE 60 5C DA 18 46 CD 7D 21 B0 3F 1B 89 FF EB 84 69 3A 9D D7 D3 70 67 40 B5 DE 5D 30 91 B1 78 11 01 E5 00 68 98 A0 C5 02 A6 74 2D 0B A2 76 B3 BE CE BD AE E9 8A 31 1C EC F1 99 94 AA F6 26 2F EF E8 8C 35 03 D4 7F FB 05 C1 5E 90 20 3D 82 F7 EA 0A 0D 7E F8 50 1A C4 07 57 B8 3C 62 E3 C8 AC 52 64 10 D0 D9 13 0C 12 29 51 B9 CF D6 73 8D 81 54 C0 ED 4E 44 A7 2A 85 25 E6 CA 7C 8B 56 80 </pre>	Підстановка π_1: <pre> CE BB EB 92 EA CB 13 C1 E9 3A D6 B2 D2 90 17 F8 42 15 56 B4 65 1C 88 43 C5 5C 36 BA F5 57 67 8D 31 F6 64 58 9E F4 22 AA 75 0F 02 B1 DF 6D 73 4D 7C 26 2E F7 08 5D 44 3E 9F 14 C8 AE 54 10 D8 BC 1A 6B 69 F3 BD 33 AB FA D1 9B 68 4E 16 95 91 EE 4C 63 8E 5B CC 3C 19 A1 81 49 7B D9 6F 37 60 CA E7 2B 48 FD 96 45 FC 41 12 0D 79 E5 89 8C E3 20 30 DC B7 6C 4A B5 3F 97 D4 62 2D 06 A4 A5 83 5F 2A DA C9 00 7E A2 55 BF 11 D5 9C CF 0E 0A 3D 51 7D 93 1B FE C4 47 09 86 0B 8F 9D 6A 07 B9 B0 98 18 32 71 4B EF 3B 70 A0 E4 40 FF C3 A9 E6 78 F9 8B 46 80 1E 38 E1 B8 A8 E0 0C 23 76 1D 25 24 05 F1 6E 94 28 9A 84 E8 A3 4F 77 D3 85 E2 52 F2 82 50 7A 2F 74 53 B3 61 AF 39 35 DE CD 1F 99 AC AD 72 2C DD D0 87 BE 5E A6 EC 04 C6 03 34 FB DB 59 B6 C2 01 F0 5A ED A7 66 21 7F 8A 27 C7 C0 29 D7 </pre>
Підстановка π_2: <pre> 93 D9 9A B5 98 22 45 FC BA 6A DF 02 9F DC 51 59 4A 17 2B C2 94 F4 BB A3 62 E4 71 D4 CD 70 16 E1 49 3C C0 D8 5C 9B AD 85 53 A1 7A C8 2D E0 D1 72 A6 2C C4 E3 76 78 B7 B4 09 3B 0E 41 4C DE B2 90 25 A5 D7 03 11 00 C3 2E 92 EF 4E 12 9D 7D CB 35 10 D5 4F 9E 4D A9 55 C6 D0 7B 18 97 D3 36 E6 48 56 81 8F 77 CC 9C B9 E2 AC B8 2F 15 A4 7C DA 38 1E 0B 05 D6 14 6E 6C 7E 66 FD B1 E5 60 AF 5E 33 87 C9 F0 5D 6D 3F 88 8D C7 F7 1D E9 EC ED 80 29 27 CF 99 A8 50 0F 37 24 28 30 95 D2 3E 5B 40 83 B3 69 57 1F 07 1C 8A BC 20 EB CE 8E AB EE 31 A2 73 F9 CA 3A 1A FB 0D C1 FE FA F2 6F BD 96 DD 43 52 B6 08 F3 AE BE 19 89 32 26 B0 EA 4B 64 84 82 6B F5 79 BF 01 5F 75 63 1B 23 3D 68 2A 65 E8 91 F6 FF 13 58 F1 47 0A 7F C5 A7 E7 61 5A 06 46 44 42 04 A0 DB 39 86 54 AA 8C 34 21 8B F8 0C 74 67 </pre>	Підстановка π_3: <pre> 68 8D CA 4D 73 4B 4E 2A D4 52 26 B3 54 1E 19 1F 22 03 46 3D 2D 4A 53 83 13 8A B7 D5 25 79 F5 BD 58 2F 0D 02 ED 51 9E 11 F2 3E 55 5E D1 16 3C 66 70 5D F3 45 40 CC E8 94 56 08 CE 1A 3A D2 E1 DF B5 38 6E 0E E5 F4 F9 86 E9 4F D6 85 23 CF 32 99 31 14 AE EE C8 48 D3 30 A1 92 41 B1 18 C4 2C 71 72 44 15 FD 37 BE 5F AA 9B 88 D8 AB 89 9C FA 60 EA BC 62 0C 24 A6 A8 EC 67 20 DB 7C 28 DD AC 5B 34 7E 10 F1 7B 8F 63 A0 05 9A 43 77 21 BF 27 09 C3 9F B6 D7 29 C2 EB C0 A4 8B 8C 1D FB FF C1 B2 97 2E F8 65 F6 75 07 04 49 33 E4 D9 B9 D0 42 C7 6C 90 00 8E 6F 50 01 C5 DA 47 3F CD 69 A2 E2 7A A7 C6 93 0F 0A 06 E6 2B 96 A3 1C AF 6A 12 84 39 E7 B0 82 F7 FE 9D 87 5C 81 35 DE B4 A5 FC 80 EF CB BB 6B 76 BA 5A 7D 78 0B 95 E3 AD 74 98 3B 36 64 6D DC F0 59 A9 4C 17 7F 91 B8 C9 57 1B E0 61 </pre>

Рисунок 2.1 — Підстановки алгоритму «Калина»

Отже, маємо довільний початковий ключ

Ключ: 0D0C 1004 181C 2024 282C 3034 383C 0004

Правила такі: До байтів одного рядка поточного стану застосовується одна й та сама підстановка.

$S_{0,i}$	0-рядок	π_0
$S_{1,i}$	1-рядок	π_1
$S_{2,i}$	2-рядок	π_2
$S_{3,i}$	3-рядок	π_3
$S_{4,i}$	4-рядок	π_0
$S_{5,i}$	5-рядок	π_1
$S_{6,i}$	6-рядок	π_2
$S_{7,i}$	7-рядок	π_3

Рисунок 2.2 — Правило підстановки байтів

		Луцевич М. О			ДУ «Житомирська політехніка».23.125.9.000 – ПП	Арк.
		Окунькова О.О.				13
Змн.	Арк.	№ докум.	Підпис	Дата		

Перетворимо перший байт 0D за таблицею π_0 . Отже, на перехресті 0 та D стоїть значення F0. Саме це значення і буде перенесено.

	π_0															
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	A8	43	5F	06	6B	75	6C	59	71	DF	87	95	17	F0	D8	09
1	6D	F3	1D	CB	C9	4D	2C	AF	79	E0	97	FD	6F	4B	45	39
2	3E	DD	A3	4F	B4	B6	9A	0E	1F	BF	15	E1	49	D2	93	C6
3	92	72	9E	61	D1	63	FA	EE	F4	19	D5	AD	58	A4	BB	A1
4	DC	F2	83	37	42	E4	7A	32	9C	CC	AB	4A	8F	6E	04	27
5	2E	E7	E2	5A	96	16	23	2B	C2	65	66	0F	BC	A9	47	41
6	34	48	FC	B7	6A	88	A5	53	86	F9	5B	DB	38	7B	C3	1E
7	22	33	24	28	36	C7	B2	3B	8E	77	BA	F5	14	9F	08	55
8	9B	4C	FE	60	5C	DA	18	46	CD	7D	21	B0	3F	1B	89	FF
9	EB	84	69	3A	9D	D7	D3	70	67	40	B5	DE	5D	30	91	B1
A	78	11	01	E5	00	68	98	A0	C5	02	A6	74	2D	0B	A2	76
B	B3	BE	CE	BD	AE	E9	8A	31	1C	EC	F1	99	94	AA	F6	26
C	2F	EF	E8	8C	35	03	D4	7F	FB	05	C1	5E	90	20	3D	82
D	F7	EA	0A	0D	7E	F8	50	1A	C4	07	57	B8	3C	62	E3	C8
E	AC	52	64	10	D0	D9	13	0C	12	29	51	B9	CF	D6	73	8D
F	81	54	C0	ED	4E	44	A7	2A	85	25	E6	CA	7C	8B	56	80

Рисунок 2.3 — Таблиця π_0

Другий байт 0C вже перетворюється за таблицею π_1 . Маємо результат D2. Третій байт, відповідно, буде перетворюється за таблицею π_2 , четверти — π_3 . П'ятий байт вже буде перетворюватися за таблицею π_0 , згідно рисунку 2.2

Таким чином, отримуємо:

0D	28	→	F0	1F
0C	2C		D2	DF
10	30		4A	A6
04	34		73	40
18	38		79	F4
1C	3C		F5	54
20	00		49	93
24	04		ED	73

3. ShiftPows (Зсув рядків)

Рядки стану циклічно зсувають праворуч на різну кількість байтів, залежно від розміру блоку. Все залежить від типу блоку: 128, 256 чи 512-бітовий блок. Розглянемо на прикладі того ж ключа:

Блок 128-бітів:

0D	28		0D	28
0C	2C		0C	2C
10	30		10	30
04	34		04	34
18	38	→	38	18
1C	3C		3C	1C
20	00		00	20
24	04		04	24

Блок 256-бітів:

0D	28	F0	1F		0D	28	F0	1F
0C	2C	D2	DF		0C	2C	D2	DF
10	30	4A	A6		30	10	4A	A6
04	34	73	40		34	04	73	40
18	38	79	F4	→	79	38	18	F4
1C	3C	F5	54		F5	3C	1C	54
20	00	49	93		93	00	49	20
24	04	ED	73		73	04	ED	24

Блок 512-бітів:

0D	28	F0	1F	01	08	06	07		0D	28	F0	1F	01	08	06	07
0C	2C	D2	DF	05	01	08	06		2C	0C	D2	DF	05	01	08	06
10	30	4A	A6	01	05	01	08		4A	30	10	A6	01	05	01	08
04	34	73	40	01	01	05	01		40	34	73	04	01	01	05	01
18	38	79	F4	04	01	01	05	→	04	38	79	F4	18	01	01	05
1C	3C	F5	54	07	04	01	01		04	3C	F5	54	07	1C	01	01
20	00	49	93	06	07	04	01		04	00	49	93	06	07	04	01
24	04	ED	73	08	06	07	04		04	04	ED	73	08	06	07	24

2.2 Обґрунтування вибору мови програмування

Однією з сильних сторін Python є його простота та легкість використання. Python має простий синтаксис і динамічний тип, що дозволяє швидко створювати прототипи та тестувати код. Це особливо корисно для алгоритмів шифрування, розробка яких може бути складною та трудомісткою.

Python також має велику кількість бібліотек, доступних для криптографії, таких як PyCrypto та Cryptography. Ці бібліотеки надають можливість виконувати криптографічні операції, такі як шифрування та дешифрування, генерація ключів тощо.

Python також підтримує кілька платформ, включаючи Windows, Linux і MacOS, що робить його ідеальним для розробки кросплатформних криптографічних алгоритмів. Крім того, Python є відкритою мовою програмування, яка дозволяє розробникам робити внесок у вдосконалення мови та розширення її можливостей.

Python також має вбудовану підтримку бітових даних, що важливо для реалізації криптографічних алгоритмів. Також Python має вбудовані функції для роботи з хеш-функціями, що корисно для реалізації підтримки різних алгоритмів хешування.

Висновки до другого розділу

В даному розділі було детально розглянуто основні дії формування ключів, шифрування — формування початкової матриці, SubBytes, ShiftRows, MixColumns. Обґрунтовано вибір мови програмування.

		Луцевич М. О.			ДУ «Житомирська політехніка».23.125.9.000 – ПП	Арк.
		Окунькова О.О.				16
Змн.	Арк.	№ докум.	Підпис	Дата		

ВИСНОВКИ

В першому розділі було описано структуру алгоритму шифрування, представлений опис алгоритму для шифрування та розшифрування, проведено аналіз безпеки та стійкості алгоритму, а також порівняння з іншими алгоритмами.

В даному розділі було детально розглянуто основні дії формування ключів, шифрування — формування початкової матриці, SubBytes, ShiftRows, MixColumns. Обґрунтовано вибір мови програмування.

В результаті виконання переддипломної практики отримано поглиблені теоретичні знання та навички з реалізації алгоритму шифрування Калина

		Луцевич М. О			ДУ «Житомирська політехніка».23.125.9.000 – ПП	Арк.
		Окунькова О.О.				17
Змн.	Арк.	№ докум.	Підпис	Дата		

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Щур Н. О. Національний стандарт шифрування ДСТУ 7624:2014 («Калина») [Електронний ресурс] / Наталя Олександрівна Щур. – 2021. – Режим доступу до ресурсу: https://learn.ztu.edu.ua/pluginfile.php/233924/mod_resource/content/1/Лекція7.pdf.
2. Щур Н. О. ЛАБОРАТОРНА РОБОТА № 5. ДОСЛІДЖЕННЯ ОСНОВНИХ ОПЕРАЦІЙ ШИФРУ «КАЛИНА» У ПРОЦЕСІ ФОРМУВАННЯ ДОПОМІЖНОГО КЛЮЧА [Електронний ресурс] / Наталя Олександрівна Щур. – 2021. – Режим доступу до ресурсу: https://learn.ztu.edu.ua/pluginfile.php/189354/mod_resource/content/1/Лаб5.pdf.
3. Щур Н. О. Національний стандарт шифрування ДСТУ 7624:2014 («Калина») [Електронний ресурс] / Наталя Олександрівна Щур. – 2021. – Режим доступу до ресурсу: https://learn.ztu.edu.ua/pluginfile.php/184891/mod_resource/content/1/Лекція6.pdf.
4. Совин Я. Р. ЕФЕКТИВНА РЕАЛІЗАЦІЯ АЛГОРИТМУ БЛОКОВОГО СИМЕТРИЧНОГО ШИФРУВАННЯ ДСТУ 7624:2014 («КАЛИНА») ДЛЯ 8/16/32-БІТОВИХ ВБУДОВАНИХ СИСТЕМ [Електронний ресурс] / Я. Р. Совин, В. І. Отенко, Є. Ф. Штефанюк. – 2017. – Режим доступу до ресурсу: <file:///C:/Users/User/Downloads/1575-Текст%20статті-6052-1-10-20171025.pdf>.
5. СПОСОБИ ГЕНЕРАЦІЇ КЛЮЧІВ АЛГОРИТМІВ ШИФРУВАННЯ НА БАЗІ ЛІНІЙНИХ СТРУКТУР [Електронний ресурс]. – 2018. – Режим доступу до ресурсу: https://ela.kpi.ua/bitstream/123456789/26681/1/Kisilchuk_magistr.pdf.

		Луцевич М. О.			ДУ «Житомирська політехніка». 23.125.9.000 – ПП	Арк.
		Окунькова О. О.				18
Змн.	Арк.	№ докум.	Підпис	Дата		

