Міністерство освіти і науки України
Харківського національного університету імені В.Н. Каразіна
Навчально-наукового інституту комп'ютерних наук та штучного інтелекту
Спеціальність 125 «Кібербезпека»
Освітня програма «Кібербезпека»

В.о. зав. кафедрою КІСМіТ

Марина ЄСІНА

"Допущено до захисту"

« »_____2025р.

Пояснювальна записка

до кваліфікаційної роботи бакалавра

на тему: «Порівняння аналогового метода криптографічного перетворення даних з цифровим та розробка пропозицій щодо їх сумісної програмної реалізації»

оцінка «_____»

Голова ЕК

Мичуда Л.З.

Керівник: к.т.н. Громико І.О.

Рецензент: к.т.н. Шостак О.В.

Виконавець: студент групи КБ42

Біловус О.С.

Харків – 2025

РЕФЕРАТ

Пояснювальна записка до проєкту бакалавра містить 60 сторінки, 17 рисунків, 5 таблиць, додаток А з лістингом коду програми, додаток Б з таблицями, 22 посилання на джерела.

Мета роботи полягає в дослідженні, систематизації та розробці технічних вимог, програмних операцій і адаптаційних механізмів для цифрового, аналогового та гібридного шифрування.

Об’єкт дослідження – процеси цифрового, аналогового та гібридного шифрування.

Предмет дослідження – технічні вимоги, програмні операції та адаптаційні механізми, які використовуються в цифровому, аналоговому та гібридному шифруванні.

Основними методами дослідження є аналіз і порівняння існуючих криптографічних технологій, розробка моделей адаптаційних рішень, а також тестування ефективності гібридних підходів до шифрування.

У роботі досліджено: сучасні методи цифрового, аналогового та гібридного шифрування, сформовано узагальнену модель криптографічних методів, проведено аналіз адаптаційних рішень та здійснено тестування ефективності гібридних шифрувальних підходів.

Результати роботи можуть бути використані у сфері інформаційної безпеки, для удосконалення засобів захисту даних, а також як наукове підґрунтя для подальших досліджень у галузі криптографії.

Ключові слова: ЦИФРОВЕ ШИФРУВАННЯ, АНАЛОГОВЕ ШИФРУВАННЯ, КРИПТОГРАФІЧНІ АЛГОРИТМИ, БЕЗПЕКА ДАНИХ, ГІБРИДНЕ ШИФРУВАННЯ, АДАПТАЦІЯ КРИПТОГРАФІЇ, ТЕСТУВАННЯ ШИФРУВАННЯ.

ABSTRACT

The explanatory note to the bachelor's project contains 60 pages, 17 figures, 5 tables, Appendix A with the listing of the program code, Appendix B with the tables, 22 references list.

The purpose of the work is to study, systematise and develop technical requirements, software operations and adaptation mechanisms for digital, analogue and hybrid encryption.

The object of research is the processes of digital, analogue and hybrid encryption.

The subject of research is technical requirements, software operations and adaptation mechanisms used in digital, analogue and hybrid encryption.

The main research methods are analysis and comparison of existing cryptographic technologies, development of models of adaptation solutions, and testing the effectiveness of hybrid encryption approaches.

The paper investigates: modern methods of digital, analogue and hybrid encryption, develops a generalised model of cryptographic methods, analyses adaptation solutions and tests the effectiveness of hybrid encryption approaches.

The results of the work can be used in the field of information security, to improve data protection, and as a scientific basis for further research in the field of cryptography.

Keywords: DIGITAL ENCRYPTION, ANALOGUE ENCRYPTION, CRYPTOGRAPHIC ALGORITHMS, DATA SECURITY, HYBRID ENCRYPTION, CRYPTOGRAPHY ADAPTATION, ENCRYPTION TESTING.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

GSM – Global System for Mobile Communications

LTE – Long-Term Evolution

NLP – Natural Language Processing

NCDP – Neuro Color Dynamic Programming

FHSS – Frequency Hopping Spread Spectrum

AES – Advanced Encryption Standard

WPA2 – Wi-Fi Protected Access 2

3DES – Triple Data Encryption

DES – Data Encryption Standard

RSA – Rivest-Shamir-Adleman

ECC – Elliptic Curve Cryptography

TLS – Transport Layer Security

PGP – Pretty Good Privacy

DAC – Digital-to-Analog Converter

IDE – Integrated Development Environment

RC – Remote Control

ШІМ – Широтно-імпульсна модуляція

HC-SR04 – Ультразвуковий датчик відстані

IoT – Internet of Things

ВСТУП

У сучасному інформаційному просторі, де обсяги переданих та збережених даних постійно зростають, питання їх захисту набуває критичного значення. Шифрування як основний метод забезпечення конфіденційності та цілісності інформації відіграє ключову роль у сфері кібербезпеки. Історично склалося, що процеси шифрування розвивалися як у цифровому, так і в аналоговому форматах. Попри домінування цифрових технологій у сучасному світі, аналогові методи також залишаються актуальними — зокрема, в умовах спеціалізованих технічних середовищ або систем з обмеженими цифровими ресурсами.

Незважаючи на досягнення у цифровій криптографії, виключно дискретний підхід має низку обмежень. Він передбачає роботу з вже оцифрованою інформацією, залишаючи за межами захисту аналогові ділянки сигналу - такі як інтонація мови, форма хвиль або аналогові параметри зображення, що передаються [1]. Ці елементи можуть нести як службову, так і приховану інформацію, що робить їх потенційно вразливими. Крім того, цифрові методи схильні до атакуючих впливів, заснованих на частотному аналізі, шаблонах повторень і вразливості в алгоритмах, відомих з відкритих джерел.

У цьому контексті аналогова криптографія стає особливо привабливою та важливою. Вона оперує безперервними сигналами та параметрами, які складніше формалізувати та передбачити. Застосування функцій з безперервним аргументом, хаотичних сигналів, а також динамічних перетворень форми сигналу дозволяють створити додатковий рівень складності, який практично не піддається класичному криптоаналізу.

Аналогові методи добре маскують факт передачі захищеної інформації, особливо у багатоканальних та шумових середовищах.

На мою думку, перспективним напрямом на сьогоднішній день вважається гібридна криптографія, яка поєднує переваги цифрового та аналогового підходів. Гібридні системи дозволяють шифрувати зміст повідомлення і форму його уявлення, перетворюючи текстову чи цифрову інформацію на безперервні графічні образи, які можна легко впроваджувати в аналоговий потік сигналу.

Проблема адаптації аналогових методів до цифрових технологій частково висвітлена у науково-технічній літературі. Дослідники криптографії, такі як К. Шеннон, У. Діффі та М. Хеллман, заклали основи сучасної криптографії, використовуючи принципи класичних методів шифрування [1]. Подальші дослідження у цій сфері спрямовані на покращення стійкості алгоритмів та їхню адаптацію до сучасних цифрових систем. Однак питання інтеграції аналогових принципів у цифрову криптографію залишається недостатньо вивченим, що зумовлює необхідність подальших досліджень.

Ця робота присвячена всебічному аналізу існуючих методів шифрування, зокрема цифрових і аналогових, їхньому порівнянню та визначенню ефективних підходів до їх адаптації. Особливу увагу мною приділено розробці гібридної системи аналого-цифрового шифрування, яка поєднує переваги обох підходів. У ході дослідження розглядаються теоретичні основи криптографії, технічні вимоги до шифрувальних систем, принципи реалізації ключових операцій, а також практичні аспекти адаптації аналогових методів у цифровому середовищі.

Об’єктом дослідження є процеси шифрування інформації в контексті інформаційної безпеки. Предметом дослідження є аналіз аналогових методів шифрування та їх адаптація до цифрових технологій.

Метою роботи є дослідження можливостей застосування аналогових методів у цифровій криптографії, визначення їхніх переваг і недоліків, а також розробка підходів до їх ефективної інтеграції.

1 АНАЛІЗ ПРОЦЕСІВ ШИФРУВАННЯ

1.1 Основи криптографії та її класифікація

Криптографія є наукою про методи захисту інформації шляхом її шифрування, що передбачає перетворення даних у форму, яку неможливо зрозуміти без відповідного ключа. Основна мета криптографії полягає у забезпеченні конфіденційності, цілісності, автентичності та відмінності інформації. Протягом століть методи криптографії розвивалися від простих шифрів до складних алгоритмів, здатних захищати навіть найчутливішу інформацію. Одним із найдавніших методів є шифр Цезаря, який полягав у зсуві літер у тексті на певну кількість позицій. Сучасна криптографія значно ускладнилася, використовуючи складні математичні операції та алгоритми, що гарантують високий рівень захисту.

По-перше, криптографічні методи можна розрізнити за типом даних - цифрова криптографія працює з двійковими кодами, тоді як аналогова криптографія застосовується до аналогових сигналів. Аналогове шифрування використовується, зокрема, для захисту голосових сигналів у телефонних системах, а також в радіокомунікаціях [2].

По-друге, відповідно до алгоритмічного підходу, криптографію можна поділити на класичну, що охоплює історичні методи, такі як шифр Віженера, та сучасну, яка включає потужні алгоритми, такі як AES, RSA і ECC. Сучасні методи включають також постквантову криптографію, що розробляється для протидії загрозам з боку квантових комп’ютерів.

Розглянемо діаграму (див. Рис 1.1), яка ієрархічно класифікує шифри, розділяючи їх на класичні та сучасні методи шифрування. Вона демонструє різноманіття криптографічних підходів, що використовувалися в історії та

застосовуються в сучасних цифрових системах [3].

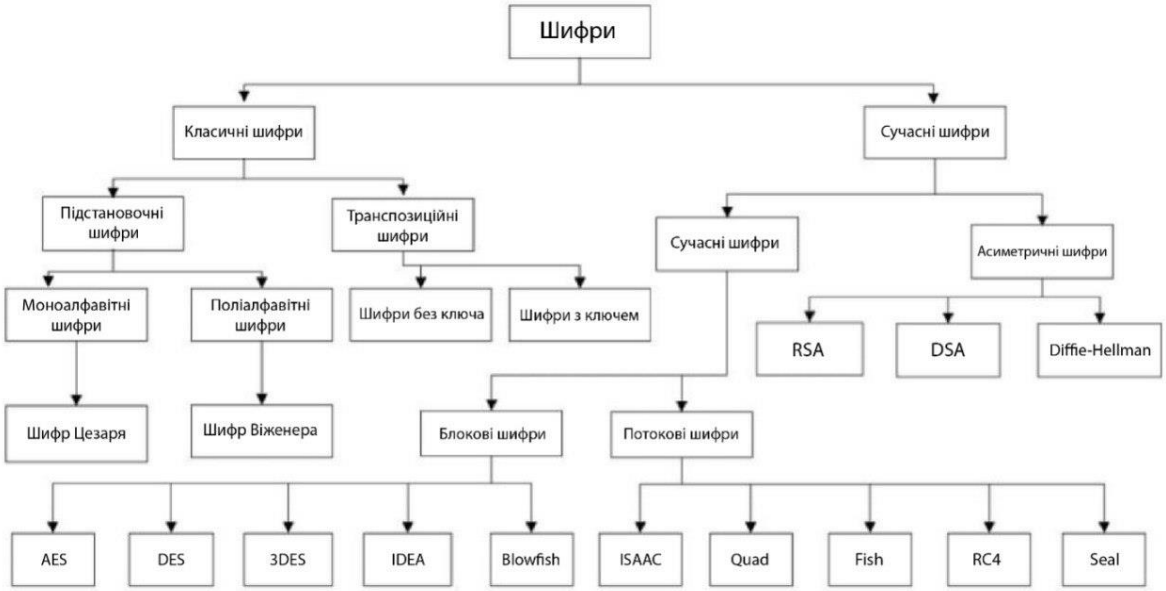


Рисунок 1.1 - Класифікація криптографії [3].

Класичні шифри поділяються на підстановочні та перестановочні. Підстановочні шифри, у свою чергу, розділяються на моноалфавітні та поліалфавітні методи. Прикладом першої групи є шифр Цезаря, який виконує заміну літер алфавіту шляхом їх зсуву. До другої групи належить шифр Віженера, що застосовує змінний ключ для шифрування тексту [3].

Перестановочні шифри також можуть бути безключовими або ключовими. Безключові перестановочні шифри передбачають фіксовану зміну розташування символів у повідомленні, тоді як ключові шифри базуються на використанні ключа для визначення перестановки символів [3].

Також, сучасна криптографія, згідно з діаграмою, поділяється на симетричні та асиметричні шифри (див. рис 1.1). Симетричні алгоритми передбачають використання одного і того ж ключа для шифрування і розшифрування. Вони поділяються на блочні та потокові шифри. До блочних шифрів належать AES, DES, 3DES, IDEA та Blowfish, тоді як потокові шифри включають ISAAC, Quad, Fish, RC4 та Seal.

Асиметричні шифри, на відміну від симетричних, використовують два різні ключі: відкритий для шифрування та закритий для розшифрування. Прикладами таких алгоритмів є RSA, DSA та протокол обміну ключами Діффі-Геллмана.

Таким чином, наведена схема чітко демонструє еволюцію криптографічних методів, що еволюціонували від простих підстановок і перестановок до складних алгоритмів симетричного та асиметричного шифрування, які є основою сучасної інформаційної безпеки.

1.2 Обґрунтування важливості цифрового методу та його недоліки

Цифрове шифрування є фундаментальним компонентом сучасної інформаційної безпеки, забезпечуючи конфіденційність, цілісність та автентичність даних у цифровому середовищі. Його основні принципи базуються на використанні математичних алгоритмів для перетворення відкритого тексту в зашифрований, що унеможливлює несанкціонований доступ до інформації [4].

Цифровий метод — це сукупність інструментів і підходів, що базуються на комп’ютерній обробці даних, математичному моделюванні, цифрових алгоритмах і автоматизації процесів. Його застосування охоплює майже всі сфери життя: від медичної діагностики до систем штучного інтелекту, від цифрової освіти до державного управління. Однак, попри очевидні переваги, цифровий метод не позбавлений недоліків, які слід враховувати в процесі його широкого впровадження.

Розглянемо в чому важливість цифрового методу шифрування. Цифрові методи дозволяють опрацьовувати великі обсяги даних з високою швидкістю та точністю [4]. Наприклад, в інженерії або медицині комп’ютерні моделі допомагають точно прогнозувати наслідки певних рішень або діагностувати захворювання на ранніх етапах. Це значно

зменшує кількість помилок, зумовлених людським фактором, і підвищує ефективність роботи.

Також, варто не забувати, що завдяки цифровим технологіям стало можливим масштабування процесів без втрати якості. Онлайн-освіта, хмарні сервіси, цифрові архіви — усе це приклади того, як цифровий метод дає змогу охопити широку аудиторію без фізичних обмежень. Цифрові методи сприяють автоматизації рутинних процесів, що економить час, людські та фінансові ресурси. У виробництві автоматизовані системи контролю якості, у банківській справі — цифрові транзакції та аналітика, у сфері послуг — чат-боти і CRM-системи.

Застосування цифрових моделей дозволяє швидше приймати обґрунтовані рішення. Наприклад, у бізнесі алгоритми штучного інтелекту аналізують ринок у реальному часі, прогнозують зміни попиту, поведінку клієнтів тощо.

Але чим більше суспільство покладається на цифрові методи, тим сильніше воно вразливе до технічних збоїв, кібератак чи втрати даних. Відмова системи в банку, лікарні чи урядовій установі може мати серйозні наслідки.

Автоматизація процесів нерідко супроводжується скороченням робочих місць. Це створює соціальну напругу, особливо серед людей, які не мають цифрових навичок або не готові до перекваліфікації. Часто цифрові рішення позбавляють взаємодію людського елементу. Наприклад, у сфері охорони здоров’я надмірна автоматизація може зменшити емпатію лікаря до пацієнта, а в освіті — знизити якість живого спілкування між учителем і учнем.

Цифрові методи часто пов’язані з великим обсягом персональних даних. Їх неналежне використання або зберігання створює загрозу для конфіденційності та порушення прав людини. Також виникає етична дилема щодо рішень, які ухвалюють алгоритми без людського втручання.

Цифровий метод — безперечно потужний інструмент, що відкриває нові горизонти для розвитку науки, економіки, медицини та суспільства загалом. Його здатність підвищувати ефективність, точність, швидкість і доступність процесів робить його надзвичайно важливим у сучасному світі. Однак, водночас не можна ігнорувати його недоліки: від залежності від технологій до соціальних і етичних викликів [2].

1.3 Обґрунтування важливості аналогового методу та його недоліки

Класична криптографія, започаткована Клодом Шенноном, базується на дискретних елементах — символах, числах, бітових послідовностях. Шеннон сам зазначав, що його дослідження мають обмеження, пов'язані з їх "дискретною природою" [5]. У той час це було доцільно - передача інформації зводилася до цифр і символів. Однак сучасні інформаційні потоки часто мають аналогову природу — інтонації, варіації сигналів, зображення, що змінюються у часі. Відмова враховувати ці компоненти — це обмеження захисту, яке залишає аналогові сліди відкритими для перехоплення [5].

Таким чином, ми повертаємось до аналогового шифрування, яке, на відміну від цифрового, працює з неперервними сигналами, використовуючи методи фазового, амплітудного або частотного маскування, а також хаотичні системи. Одним із класичних прикладів аналогового шифрування є скремблювання, яке використовується в радіозв’язку та телебаченні для обмеження доступу до контенту. Інший підхід полягає у використанні хаотичних сигналів, які важко передбачити, що ускладнює їх розшифрування сторонніми особами. Для забезпечення безпеки аналогові методи можуть бути адаптовані до цифрових середовищ, що дозволяє створювати гібридні підходи до шифрування. Такі методи використовуються, наприклад, у квантовій криптографії, де оптичні сигнали застосовуються для генерації випадкових криптографічних ключів.

Однією з головних переваг аналогових методів є те, що вони менш вразливі до цифрових атак. Візьмемо скремблювання — це спотворення сигналу таким чином, щоб його неможливо було розпізнати без спеціального обладнання. Такий метод складніше дешифрувати за допомогою стандартних цифрових алгоритмів, особливо у випадках, коли змінюються характеристики сигналу в реальному часі [6].

У ситуаціях, де недоступні складні цифрові системи або де важлива швидкість передавання без складної обробки, аналогові методи дають змогу забезпечити базовий рівень захисту. Наприклад, під час воєнних операцій чи в польових умовах, де цифрова інфраструктура обмежена або легко порушується, аналогові системи залишаються надійними.

Не менш важливими є технології розширеного спектру, які використовуються в аналоговій криптографії, дозволяють передавати сигнал у вигляді широкого діапазону частот. Це робить сигнал менш помітним і стійким до перешкод. Такі методи використовуються в радіозв'язку та спецслужбах для прихованого передавання інформації. Додавання штучного шуму до основного сигналу унеможливлює його перехоплення без точного знання алгоритму демодуляції. Це робить маскування ефективним методом у високочутливих комунікаціях, де необхідно сховати сам факт передавання даних.

У багатьох випадках, особливо в системах старшого покоління, використовуються аналогові пристрої, які не підтримують цифрову обробку. Аналогові методи криптографії ідеально інтегруються з такими технологіями без потреби у складній модернізації [5].

На жаль, аналогові методи складніше адаптувати під нові вимоги або оновити [7]. Зміна параметрів скремблера або частотного діапазону вимагає фізичного втручання в обладнання, що у цифрових системах вирішується простим оновленням програмного забезпечення.

Також, аналоговий сигнал схильний до спотворень під впливом атмосферних явищ, електромагнітних перешкод або завад у середовищі передачі. Це знижує стабільність і якість комунікації порівняно з цифровими системами, які можуть використовувати корекцію помилок. У разі передачі складної інформації, наприклад аудіо або відео високої якості, аналогові методи можуть призводити до втрати частини даних через погіршення сигналу або спотворення під час передавання [8].

Попри домінування цифрових технологій, на мою думку, аналоговий метод продовжує залишатися актуальним у низці специфічних сфер, де потрібна швидкість, низький рівень цифрового втручання та фізична стійкість системи. Аналогова криптографія, як і цифрова, не є ідеальною — обидві мають свої вразливості, які можуть бути використані для несанкціонованого доступу до переданої інформації [8]. З огляду на це, доцільно розглядати підхід гібридної аналогово-цифрової криптографії, який поєднує переваги обох методів: гнучкість аналогових рішень у реальному часі з високим рівнем захисту, який забезпечують цифрові алгоритми шифрування. Тому, я вважаю, комбіновані, гібридні методи, що поєднують кілька способів шифрування, є перспективними [5].

1.4 Концепція гібридної (цифро-аналогової) криптографії

Гібридна криптографія, синтез цифрових та аналогових методів, являє собою не просто технічну альтернативу, а й філософський зсув. Вона визнає, що інформація не завжди обмежується дискретними бітами та логічними елементами. Іноді вона існує в рівнях напруги форми хвилі, кривій функції, ширині імпульсу модульованого сигналу або навіть в очевидній випадковості аналогового шуму. У той час як цифрова криптографія перевершує алгоритмічну силу та повторюваність, аналогові методи пропонують непередбачуваність, неясність та стійкість до традиційного аналізу сигналів [5].

Приймаючи цю подвійність, гібридні системи можуть приховувати не лише вміст повідомлення, але й його структуру, час та сигнатуру сигналу. Перехід від теорії до реалізації відкриває нам ще більші перспективи. Ця концептуальна основа створює умови для глибшого технічного дослідження — такого, яке інтегрує відомі стандарти цифрового шифрування з інноваційними методами аналогового маскування.

Практично така система спирається на ідею багаторівневого кодування, де аналоговий етап забезпечує маскування фізичної форми сигналу, а цифровий — криптографічну трансформацію вмісту. Поєднання цих підходів дозволяє ускладнити як математичний аналіз сигналу, так і його фізичну інтерпретацію сторонніми спостерігачами.

У практичному контексті, мені здається, ефективним рішенням є використання аналогового методу як первинного захисного шару. Воно змінить структуру сигналу таким чином, щоб він залишався формально "аналоговим", але втратив читабельність або розпізнаваність для стандартних методів прийому. Проте, слід пам’ятати, аналогові методи не забезпечують високого рівня криптографічної стійкості, оскільки може бути вразливим до методів спектрального чи статистичного аналізу.

Для подолання цієї вразливості доцільним є використання цифрового шифрування. Це дозволяє розробити уніфіковану архітектуру гібридного шифрування, в якій аналоговий метод працює як "фізичний бар'єр", а цифровий забезпечує "логічне зашифрування". Для подальшого ускладнення структури гібридної криптографічної системи, доцільним є включення додаткового етапу математичного перетворення сигналу. Зокрема, йдеться про використання безперервних функцій, таких як логарифмічні або тригонометричні, з метою створення нелінійних сигнальних деформацій [5]. Наприклад, логарифмічне перетворення може бути використане для нелінійної модуляції амплітуди сигналу, тоді як тригонометричні функції, зокрема синусоїда, здатні вводити періодичні

варіації, які приховують структуру сигналу на рівні фізичного носія (див рис.1.4). Після проходження сигналу через скремблер, його можна трансформувати за допомогою функцій:

- $y = \log_a x$— для нелінійної деформації амплітуди, що особливо ускладнює визначення початкових меж кадру або символьної структури [5].
- $y = \sin(x)$— для періодичного модуляційного спотворення. Наприклад, зміна фази чи амплітуди відповідно до синусоїдального закону створює "псевдохвильову" структуру [5].

Включення таких математичних кривих у структуру гібридного шифрування дозволяє зруйнувати залишкову впорядкованість даних і підвищити ентропію, унеможливлюючи проведення ефективного зворотного аналізу без точного знання функціональної форми. Крім того, динамічне перемикання або зміна параметрів функцій перетворення у реальному часі здатне створити додаткову непередбачуваність, що істотно посилює криптографічну стійкість системи загалом [5].

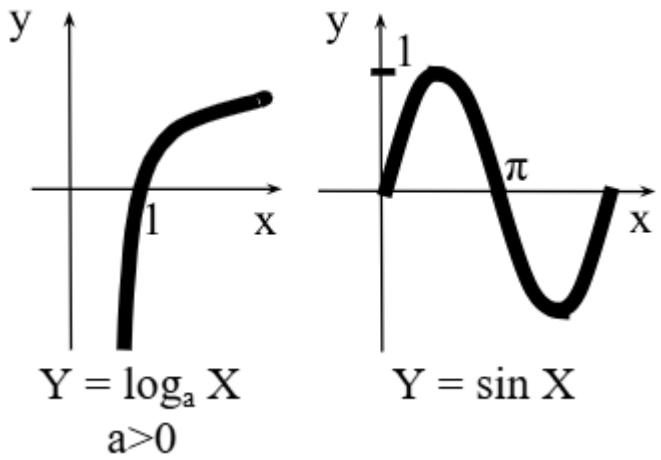


Рисунок 1.4 - Приклади графіків безперервних функцій

Таким чином, використання математичних безперервних функцій як елементів сигнало-генерації чи деформації дозволяє вивести гібридну криптографічну систему на якісно новий рівень. Воно розширює

традиційну модель шифрування, додаючи нелінійні, непередбачувані, і водночас оборотні перетворення**,** які значно ускладнюють криптоаналіз і роблять систему практично недоступною для атак за допомогою класичних цифрових методів [5].

У гібридному підході ключем виступає інформація про розміщення, форму, тип функцій, і динаміку сигналу. Такий ключ може бути переданий як окремим аналоговим сигналом (криптосигналом), або в цифровій формі. Розрізняють:

- Динамічний ключ — передається разом із повідомленням;
- Статичний ключ — передається раніше або окремо [5].

Ключ у нашій гібридній системі не лише шифрує — він керує всією логікою захисту, створюючи фундамент для синергетичного поєднання аналогових і цифрових методів шифрування. Його компрометація веде до повного порушення цілісності захисту, тоді як його правильне використання гарантує багаторівневу криптографічну стійкість.

2 ТЕХНІЧНІ ВИМОГИ ТА ПРОГРАМНІ ОПЕРАЦІЇ В ПРОЦЕСІ ШИФРУВАННЯ

2.1 Визначення технічних вимог та важливих програмних операцій у цифровому шифруванні

Як ми вже казали, цифрове шифрування є фундаментальним елементом сучасної кібербезпеки, забезпечуючи конфіденційність, цілісність та автентичність інформації. Для досягнення цих цілей нам необхідно чітко визначити технічні вимоги та розуміти ключові програмні операції, що лежать в основі криптографічних процесів.

Однією з фундаментальних вимог до сучасних криптографічних алгоритмів є їхня стійкість до криптоаналізу. Іншими словами, навіть якщо зловмиснику відомий сам алгоритм шифрування, цього недостатньо для розкриття змісту зашифрованих даних без наявності відповідного ключа [9]. Така стійкість досягається завдяки використанню складних математичних перетворень, а також достатньої довжини ключів, що ускладнює проведення атак методом повного перебору або інших форм аналітичного зламу. Водночас, важливим аспектом, який безпосередньо впливає на ефективність криптографічних систем, є управління ключами [9]. Саме ефективне генерування, зберігання, передача та утилізація криптографічних ключів гарантує, що доступ до зашифрованої інформації можуть отримати лише авторизовані особи. Без належного управління ключами навіть найнадійніший алгоритм шифрування може виявитися вразливим.

Не менш значущою є і продуктивність алгоритмів шифрування. У сучасних інформаційних системах, особливо при обробці великих обсягів даних, важливо забезпечити високу швидкість шифрування та дешифрування без суттєвого зниження загальної продуктивності [9]. Таким чином, криптографічні рішення повинні бути оптимізованими не лише з

точки зору безпеки, але й з урахуванням апаратних і програмних ресурсів системи. Крім того, однією з вимог до сучасних систем цифрового шифрування є сумісність. Вона передбачає здатність алгоритмів інтегруватися з різноманітними платформами та мережевими протоколами, що особливо важливо для великих організацій, які використовують комплексні інфраструктури безпеки. Високий рівень сумісності дозволяє уникнути фрагментації системи та забезпечує безперебійну роботу між різними компонентами[10].

Нарешті, у динамічному середовищі кіберзагроз критичне значення має адаптивність криптографічних алгоритмів. Можливість їх оновлення та вдосконалення у відповідь на появу нових вразливостей і методів атак є запорукою довгострокової ефективності та надійності захисту. Здатність алгоритмів швидко еволюціонувати відповідно до змін у сфері інформаційної безпеки забезпечує сталість захисних механізмів упродовж часу.

Програмні операції в свою чергу цифрового шифрування є основою для захисту даних. Основними серед них є шифрування та дешифрування, які забезпечують конфіденційність інформації шляхом її перетворення у зашифрований вигляд і зворотного розшифрування [10]. Важливу роль відіграє генерація ключів — процес створення криптографічних ключів з використанням генераторів псевдовипадкових чисел. Від якості цих ключів залежить стійкість системи до зламу. Ще однією ключовою операцією є хешування — перетворення даних у фіксований хеш-код для перевірки цілісності та автентичності. Управління ключами охоплює безпечне зберігання, передавання та оновлення ключів, часто з використанням інфраструктури відкритих ключів (PKI) і протоколів обміну.[10] Аутентифікація далі перевіряє особу чи систему перед наданням доступу, зазвичай за допомогою цифрових сертифікатів чи підписів. Завершує перелік управління сертифікатами — процес видачі, перевірки та

відкликання цифрових сертифікатів, що підтверджують справжність користувачів та їхніх ключів.

Усі ці операції утворюють єдину систему, яка забезпечує надійний захист інформації в цифровому середовищі.

2.2. Визначення технічних вимог та важливих програмних операцій у аналоговому шифруванні

Аналогове шифрування залишається актуальним у сферах, де необхідна висока швидкість передачі та захищеність від цифрового аналізу. Його ключові технічні вимоги включають захист від перехоплення, перешкодостійкість та сумісність із сучасними технологіями. Основні програмні операції, такі як модуляція, фазове маніпулювання, спектральне розширення та хаотичні сигнали, забезпечують ефективність аналогових методів шифрування у критичних системах комунікації [8].

Аналогові сигнали можуть бути легко перехоплені та розшифровані за допомогою спектрального аналізу або іншого обладнання. Тому важливо використовувати методи маскування сигналу, частотну або фазову модуляцію для ускладнення аналізу.

Оскільки аналогові сигнали схильні до шумів та спотворень, алгоритми шифрування повинні мінімізувати вплив сторонніх сигналів і підвищувати чіткість переданої інформації. Для ефективного кодування та декодування сигналів необхідно забезпечити точне налаштування частот, амплітуд і фазових характеристик передавача та приймача. Також, системи аналогового шифрування повинні інтегруватися з наявними комунікаційними технологіями, такими як телефонні лінії, радіозв’язок або супутникові системи.

Тепер розглянемо, важливі програмні операції у аналоговому шифруванні. Один із найпоширеніших способів кодування інформації – це зміна параметрів сигналу (амплітуди або частоти) відповідно до

закладеного коду. Далі, спектральне розширення сигналу - метод, що дозволяє розподіляти інформацію по широкому діапазону частот, що робить сигнал менш помітним для стороннього перехоплення. Аналогові хаотичні системи та шумове маскування сигналу дозволяють створювати криптографічно стійкі системи без визначеного патерну сигналу.

Розуміння та впровадження цих технічних вимог та програмних операцій є критично важливим для забезпечення надійного захисту інформації у аналоговому середовищі.

2.3. Порівняння цифрового та аналогового підходів до шифрування

Цифрове шифрування значно випереджає аналогове завдяки високій криптографічній стійкості та широкій гнучкості. Однак аналогові методи все ще залишаються актуальними у певних сферах, таких як радіозв'язок або військові системи, де цифрові методи можуть бути неефективними через обмеженість обчислювальних ресурсів [8]. Вибір між цими підходами залежить від вимог до безпеки, швидкості передачі даних та можливих загроз у конкретному середовищі (див. табл. Б.2.3.1).

Отже, ми можемо зробити висновок, що обидва методи — аналоговий і цифровий — мають свою унікальну цінність і актуальність. Аналогове шифрування зберігає значення в умовах, де потрібна оперативність, стійкість до виявлення і мінімальна цифрова інфраструктура. Натомість цифрове шифрування забезпечує найвищий рівень захисту в глобальних інформаційних мережах і системах. У сучасному світі ці підходи не конкурують, а радше доповнюють один одного, формуючи комплексну систему інформаційної безпеки, здатну адаптуватися до найрізноманітніших викликів.

3 АНАЛІЗ ТА АДАПТАЦІЯ АНАЛОГОВОГО МЕТОДА ДО ЦИФРОВОГО ШИФРУВАННЯ

3. 1 Підбір аналогового метода для адаптації

3.1.1 Огляд класичних аналогових методів шифрування

Аналогові методи шифрування відігравали ключову роль у забезпеченні конфіденційності інформації до появи цифрових технологій. Вони базувалися на механічних, електромагнітних або оптичних принципах та використовували різноманітні алгоритми для перетворення вихідного повідомлення в зашифрований формат. Аналогові методи шифрування використовувалися для захисту голосового зв'язку, радіопередач і інших аналогових сигналів до широкого впровадження цифрових технологій. Характеристики сигналу змінювалися так, щоб без спеціального ключа або алгоритму відновлення інформація була малозрозумілою для стороннього спостерігача.

Скремблювання є одним із методів аналогового шифрування, що використовується для тимчасового приховування інформації шляхом зміни структури сигналу таким чином, щоб без спеціального ключа відновлення інформація ставала нерозбірливою. Цей метод знайшов широке застосування в різних сферах, включаючи захист телефонних розмов, телевізійних передач і радіозв'язку [6].

Основна ідея скремблювання полягає у зміні певних характеристик сигналу, таких як часова послідовність, частота або фаза, щоб унеможливити або ускладнити його перехоплення та дешифрування сторонніми особами. На відміну від криптографічних методів, скремблювання зазвичай не гарантує абсолютної безпеки, але забезпечує достатній рівень захисту в умовах, коли важлива оперативність передачі інформації.

Існує декілька основних методів скремблювання сигналу, кожен з яких має свої особливості та використовується у різних сферах [6].

1) Часове скремблювання

При часовому скремблюванні вихідний аналоговий сигнал розбивається на невеликі часові сегменти, які переставляються в певному порядку згідно з ключем [6]. Без знання цього ключа отриманий сигнал буде хаотичним і нечитабельним. Наприклад, у військовому телефонному зв'язку часові перестановки використовувалися для запобігання підслуховуванню розмов.

Формульно цей процес можна виразити як [6]:

$$S'(t) = S(f(t))S'(t) \ = \ S(f(t))$$

де S(t)— початковий сигнал, S'(t) — скрембльований сигнал, а f(t) — функція перестановки часових фрагментів.

2) Частотне скремблювання

Частотне скремблювання передбачає зміну частотного спектру сигналу відповідно до секретного алгоритму. Вхідний сигнал перетворюється в частотній області, а потім відновлюється на приймальному кінці за допомогою зворотного перетворення. Цей метод широко застосовувався у захищених радіокомунікаціях.

Формульно частотне скремблювання можна виразити наступним рівнянням [6]:

$$S`(t) = \ \sum_{\text{i}} A_i * cos(2\pi f_i't + \varphi_i),$$

де f_i' – змінена частота відповідно до алгоритму шифрування.

Графічно такий метод можна зобразити через спектрограму до і після перетворення (див. табл. Б.3.1.1.1).

3) Фазове скремблювання

При фазовому скремблюванні змінюється фаза сигналу, що значно ускладнює його розшифровку без знання алгоритму перетворення.

Використання випадкових фазових зсувів дозволяє ефективно приховати інформацію в аналогових каналах.

Формула фазового скремблювання [6]:

$$S'(t) = Acos(2\pi ft + \varphi)$$

де φ — випадковий фазовий зсув, що змінюється за певним алгоритмом.

4) Комбіноване скремблювання

Цей метод використовує одночасно кілька підходів, наприклад часове та частотне скремблювання, що підвищує рівень захисту. Такий підхід застосовується у високозахищених урядових та військових системах зв'язку.

Реалізація систем скремблювання вимагає дотримання певних технічних умов.

По-перше, це синхронізація між передавачем і приймачем. Оскільки сигнал модифікується, отримувач повинен точно знати алгоритм зворотного перетворення. Для цього використовуються спеціальні системи синхронізації, що мінімізують часові зсуви і втрати даних[6].

По-друге - високоточне обладнання. Прилади для скремблювання повинні мати низький рівень внутрішнього шуму і високу точність роботи, щоб не допускати спотворень, які можуть зробити сигнал нерозбірливим навіть після зворотного декодування.

Дуже важливою є стійкість до шуму та перешкод. Оскільки сигнал може передаватися в умовах радіоперешкод або слабкого сигналу, необхідно враховувати ефективність скремблювання навіть у таких умовах. Використання адаптивних алгоритмів корекції помилок допомагає зберігати якість передачі. Деякі методи скремблювання (наприклад, часове переставлення) можуть викликати затримки у передачі даних, що є критичним для реального часу, такого як телефонні розмови або

радіозв’язок військового призначення. Системи повинні бути оптимізовані для мінімізації таких затримок.

Просте скремблювання може бути легко зламане методами аналізу сигналу, тому застосовуються комбіновані методи і випадкові зміни ключів, що підвищують рівень безпеки.

Скремблювання знайшло широке застосування у різних сферах. Одним з перших його використань була захищена телефонія у військових операціях. Наприклад, під час Другої світової війни США застосовували систему "SIGSALY" для захисту комунікацій між союзниками [12]. Ця система використовувала складне частотне та фазове скремблювання, що робило її майже неможливою для розшифрування противником.

Військові комунікації широко використовують частотне і фазове скремблювання для забезпечення безпечного зв’язку [11]. Супутниковий зв’язок використовує фазове шифрування для запобігання втручанню та несанкціонованому доступу. Наприклад, у системах GPS сигнал шифрується фазовими методами для захисту від спуфінгу (підміни сигналу).

У сучасних умовах скремблювання активно застосовується в цифровому телебаченні та мобільному зв’язку. Наприклад, кабельні оператори використовують скремблювання для шифрування преміального контенту, обмежуючи доступ для неавторизованих користувачів. Крім того, авіаційна та морська навігація використовують методи частотного скремблювання для захисту радіозв’язку від перехоплення.

У комерційній сфері скремблювання застосовується в корпоративних системах зв’язку, щоб забезпечити конфіденційність внутрішніх переговорів. Це особливо важливо для фінансових установ, де витік інформації може призвести до значних збитків.

Скремблювання залишається ефективним методом тимчасового приховування інформації в аналогових та цифрових комунікаціях. Хоча

його криптографічна стійкість не є абсолютною, правильно реалізовані алгоритми дозволяють значно ускладнити несанкціоноване перехоплення даних. Сучасні технології продовжують розвивати методи скремблювання, забезпечуючи нові рівні захисту в умовах постійного розвитку кіберзагроз.

Наступним методом, який ми розглянемо буде аналогове спектральне розсіювання - ефективний методом захисту інформаційних сигналів, що базується на розподілі сигналу на широкому спектрі частот. Це дозволяє ускладнити його перехоплення, ідентифікацію та відновлення без знання алгоритму розсіювання [11]. Головна ідея цього підходу полягає в тому, що замість передачі сигналу у вузькій частотній смузі він розсіюється на широкий діапазон частот за певним законом, що забезпечує високу завадостійкість та прихованість передачі.

На рис. 3.1 зображено залучення функціоналів в процесах NLP та NCDP. Згідно з даними Громико Ігоря Олексійовича , метод розширеного спектру може ефективно працювати в синергії з NCDP через структури обробки різних характеристик сигналу [13].

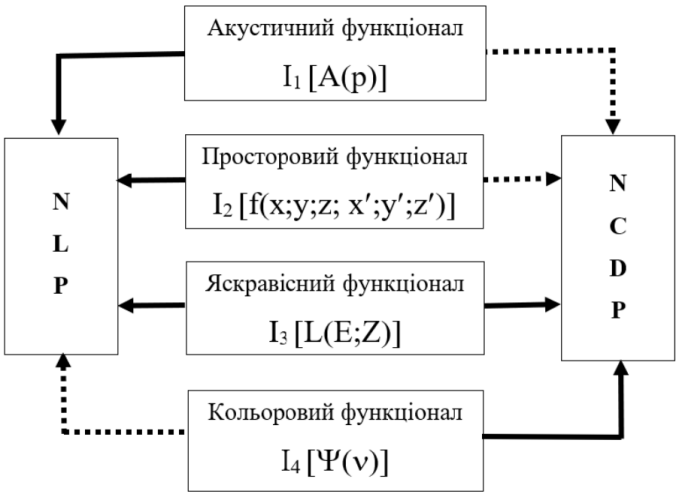


Рисунок 3.1 - Задіяність функціоналів в NLP та NCDP

Зокрема, акустичний функціонал $I_1[A(p)]$ може бути використаний для попереднього аналізу вхідного звукового сигналу перед модуляцією

спектру. Просторовий функціонал $I_2[f(...)]$ в свою чергу може дозволити визначити топологію сигналу в багатовимірному просторі — важливо для правильного формування та фільтрації сигналу в широкому спектрі [13].

Таким чином, вставлення коду розширеного спектру(див рис.3.2) може бути реалізовано шляхом перетворення функціоналів у сигнальну надбудову, яка змінює спектральні характеристики каналу. Вона може розглядатися як структурна модель реалізації NCDP через метод розширеного спектру, де функціонали виступають ключовими модулями для формування, перетворення та декодування даних у нейроорієнтованих системах [11].

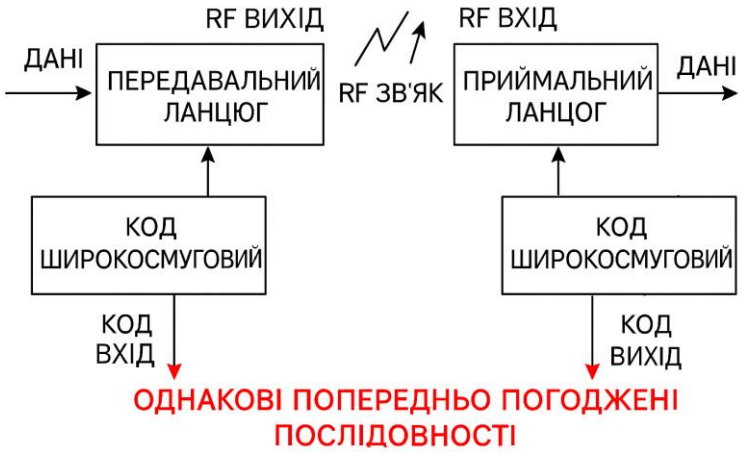


Рисунок 3.2 - Система зв'язку з розширеним спектром

Існує кілька основних методів аналогового спектрального розсіювання. Одним з найпоширеніших є частотне розсіювання з використанням псевдовипадкової зміни несучої частоти. У цьому методі частота сигналу постійно змінюється за певним законом, що робить його малопомітним для сторонніх спостерігачів. Наприклад, якщо сигнал передається у вузькому частотному діапазоні 1000–1100 Гц, при спектральному розсіюванні він буде переміщатися у ширшому діапазоні, скажімо, 500–2000 Гц відповідно до псевдовипадкової послідовності.

Іншим поширеним методом є фазове спектральне розсіювання, яке полягає в застосуванні випадкових фазових зсувів до переданого сигналу. Це дозволяє значно зменшити можливість ідентифікації сигналу за його спектральними характеристиками.

Також важливим методом є амплітудне спектральне розсіювання, де змінюється амплітуда сигналу за псевдовипадковим законом. Це ускладнює можливість дешифрування сигналу без наявності відповідного ключа.

Реалізація аналогового спектрального розсіювання вимагає дотримання певних технічних умов. Зокрема, необхідно забезпечити високу точність генерації псевдовипадкових послідовностей для керування параметрами сигналу [11]. Важливим аспектом є синхронізація передавача і приймача, оскільки навіть невеликі відхилення можуть призвести до втрати інформації. Також слід враховувати енергетичну ефективність передачі, оскільки широкий спектр сигналу може призводити до збільшеного споживання потужності.

Практичне застосування аналогового спектрального розсіювання охоплює різні сфери, включаючи військовий зв’язок, супутникові комунікації та спеціальні системи зв’язку. Наприклад, у військових радіосистемах цей метод використовується для захисту передачі команд і розвідувальної інформації від ворожого перехоплення та радіозаглушення. Супутникові системи зв’язку також активно застосовують цей метод для забезпечення стійкості сигналу до атмосферних завад і навмисного глушіння.

Третій метод - маскування сигналу шумом також є одним із ефективних методів захисту інформації в аналогових і цифрових системах зв'язку [14]. Його суть полягає у змішуванні корисного сигналу зі штучним шумом таким чином, щоб для стороннього спостерігача сигнал здавався випадковим або нечитабельним (див. рис 3.3). Лише за допомогою

спеціального фільтра або ключа можна відновити початковий сигнал, що забезпечує високу прихованість переданих даних.

Рисунок 3.3 - Система маскування сигналів шумом

Одним із ключових аспектів методу є використання спеціально створеного шуму, який повинен відповідати певним характеристикам, щоб ефективно маскувати сигнал. Наприклад, можна використовувати білий шум, псевдовипадкові послідовності або спеціально сформовані спектральні компоненти, які забезпечують складність перехоплення і декодування сигналу [14].

Основними видами маскування сигналу шумом є адитивне, мультиплікативне та адаптивне маскування. При адитивному маскуванні до корисного сигналу додається випадковий шум, який генерується синхронно на передавальній і приймальній стороні. Формульно цей процес можна описати рівнянням [15]:

$$S'(t) = S(t) + N(t),$$

де S(t)— корисний сигнал, N(t)— шум, а S'(t) — переданий сигнал. На приймальному кінці за допомогою кореляційного аналізу або спеціального фільтра шум видаляється, відновлюючи оригінальний сигнал.

Мультиплікативне маскування передбачає модуляцію корисного сигналу випадковим шумовим процесом. У цьому випадку сигнал набуває змінної амплітудної або частотної характеристики, що ускладнює його

аналіз без знання параметрів шумового сигналу. Формула для цього процесу [15]:

$$S'(t)=S(t)\times N(t)$$

Адаптивне маскування є найбільш досконалим методом, при якому параметри шуму змінюються залежно від характеристик сигналу або навколишнього середовища, що робить процес дешифрування надзвичайно складним.

Реалізація систем маскування сигналу шумом вимагає високоточних генераторів шуму, синхронізації передавача і приймача, а також складних алгоритмів фільтрації. Основними технічними вимогами є висока кореляція між шумами на передавальному і приймальному кінцях, широкий динамічний діапазон шуму, а також низький рівень власних перешкод системи.

Метод маскування шумом широко використовується в конфіденційному радіозв'язку, особливо в урядових та військових системах. Наприклад, у військовій авіації цей метод застосовувався для приховування переговорів між пілотами та командними пунктами від ворожого перехоплення. Також цей метод знаходить застосування у супутниковому зв’язку, де важливо забезпечити захист інформації від перехоплення та аналізу сигналів розвідкою.

Окрім військових застосувань, маскування сигналу шумом використовується в комерційних і корпоративних системах зв’язку, забезпечуючи захист телефонних розмов і передачі даних. Наприклад, банківські установи застосовують подібні методи для безпечного передавання голосових і цифрових повідомлень.

Таким чином, маскування сигналу шумом є способом захисту інформації, який використовується в різних сферах, забезпечуючи прихованість сигналів у складних умовах комунікації. Його вдосконалення та поєднання з іншими методами криптографічного захисту дозволяє

створювати високонадійні системи безпеки для сучасних комунікаційних технологій.

Таким чином, аналогові методи шифрування відігравали важливу роль у захисті інформації до поширення цифрових технологій. Вони дозволяли тимчасово захистити інформацію від стороннього доступу, однак їх стійкість була обмеженою. Саме тому з розвитком цифрових систем зв'язку вони поступилися місцем сучасним криптографічним методам, заснованим на математичних алгоритмах і комп'ютерних технологіях.

Розуміння цих аналогових методів шифрування є важливим для їх подальшої адаптації до цифрових технологій. Багато сучасних криптографічних алгоритмів базуються на принципах, закладених ще в аналогових системах, таких як підстановки, перестановки та використання динамічних ключів. Подальший аналіз їхньої стійкості дозволить визначити, які саме методи можуть бути адаптовані для сучасного цифрового середовища.

3.1.2 Аналіз стійкості та відбір аналогового метода

Аналогові методи шифрування, такі як скремблювання, аналогове спектральне розсіювання та маскування сигналу шумом, відіграли значну роль у забезпеченні безпеки інформаційних каналів. Однак їх стійкість залежить від низки факторів, зокрема можливості несанкціонованого дешифрування, впливу шумів та перешкод, а також технологічного розвитку засобів розвідки сигналів.

Скремблювання є одним із найпростіших методів аналогового шифрування, що змінює часову, частотну або фазову структуру сигналу. Основним його недоліком є вразливість до методів спектрального аналізу та синхронного дешифрування, особливо за наявності потужних обчислювальних ресурсів. Просте скремблювання, наприклад часове переставлення сегментів сигналу, може бути зламане за допомогою

кореляційного аналізу. Для підвищення стійкості використовуються комбінаційні методи, що включають випадкове переставлення із секретним ключем.

Аналогове спектральне розсіювання є одним із найстійкіших методів, оскільки він маскує корисний сигнал, розподіляючи його на широкому частотному діапазоні. Це ускладнює виявлення сигналу противником, особливо при використанні динамічних схем розсіювання. Проте сучасні методи аналізу спектральної густини дозволяють виявити прихований сигнал за допомогою довготривалого накопичення енергії та аналізу ймовірних схем модуляції. Тому підвищення стійкості передбачає використання псевдовипадкових сигналів та адаптивних методів змін частотного розподілу.

Маскування сигналу шумом є ефективним методом захисту, оскільки додає штучний шум, що робить сигнал нерозбірливим без відповідного фільтра або ключа. Однак його стійкість залежить від якості генерації шуму та можливості його відокремлення. Зокрема, якщо шум має певні закономірності або відносно низьку енергетичну щільність порівняно з корисним сигналом, його можна видалити за допомогою спеціалізованих алгоритмів обробки сигналу. Для підвищення захисту використовують адаптивні методи змішування сигналу із змінними характеристиками шуму.

Таким чином, стійкість аналогових методів шифрування визначається складністю алгоритму перетворення, використанням випадкових або псевдовипадкових змінних, а також рівнем розвитку засобів аналізу сигналів. Комбіновані методи, що поєднують кілька підходів, можуть значно підвищити рівень захисту, забезпечуючи ефективний захист інформації навіть у сучасних умовах розвитку технічних засобів розвідки [16].

Аналіз стійкості трьох основних аналогових методів шифрування дозволяє нам оцінити їхню ефективність у сучасних умовах інформаційної

безпеки [16]. Кожен із цих методів має свої переваги та недоліки, які впливають на їхню придатність для застосування в умовах сучасних загроз(див. табл. Б.3.1.2.1).

У сучасних умовах інформаційної безпеки оптимальним рішенням є комбіноване використання декількох методів, де аналогові методи виступають як додатковий рівень захисту перед основним цифровим шифруванням. Це дозволяє створювати багаторівневу систему безпеки, яка здатна протистояти як технічному, так і аналітичному дешифруванню.

Аналіз показує, що жоден із методів не є універсальним і придатним для всіх випадків використання. Найбільш стійкими до перехоплення та аналізу є аналогове спектральне розсіювання та маскування сигналу шумом. Вони забезпечують найвищий рівень безпеки, однак їхня складність реалізації та вимоги до апаратного забезпечення можуть бути значними обмеженнями.

З іншого боку, скремблювання є найпростішим у реалізації, але його стійкість до аналізу низька. Зловмисники можуть відновити оригінальний сигнал, використовуючи методи спектрального або часово-частотного аналізу. Частотне та фазове шифрування є компромісним варіантом, який поєднує середню стійкість із помірною складністю реалізації, що робить його привабливим для військового та спеціального зв’язку.

Для створення гібридного аналогово-цифрового шифрування найкращим вибором є аналогове спектральне розсіювання, оскільки воно дозволяє значно ускладнити виявлення сигналу [18]. У поєднанні з цифровими методами шифрування цей підхід забезпечує високий рівень безпеки навіть у разі перехоплення даних. Однак, його впровадження вимагає високоточного обладнання та складних алгоритмів синхронізації, що може обмежувати його застосування в масових комунікаціях.

Отже, в умовах даної роботи ми приймаємо рішення адаптувати метод скремблювання для використання в цифрових системах шифрування. Це

означає, що ми плануємо інтегрувати простий та швидкий аналоговий метод маскування сигналу з потужними цифровими алгоритмами, щоб створити багаторівневу систему захисту. Такий підхід дозволить використати переваги скремблювання як попереднього етапу, який забезпечує базове маскування даних, а потім застосувати цифрове шифрування для забезпечення високої стійкості до криптоаналізу, що є критично важливим у сучасних умовах інформаційної безпеки[18]. Обрана стратегія допоможе компенсувати недоліки скремблювання, зокрема його низьку стійкість до аналізу, за рахунок застосування потужних цифрових методів. Таким чином, адаптація скремблювання до цифрового шифрування дозволяє нам створити систему, яка поєднує швидкість і простоту реалізації аналогового методу з високою безпекою та стійкістю сучасних цифрових технологій, що робить цей підхід оптимальним для використання в умовах обмежених ресурсів

3.2 Підбір цифрового метода для адаптації

3.2.1 Огляд сучасних цифрових методів шифрування

Сучасні цифрові методи шифрування є основою безпечного зберігання та передачі інформації в цифровому світі. Вони розробляються для захисту даних від несанкціонованого доступу, забезпечуючи конфіденційність, цілісність і автентичність інформації. Залежно від принципу роботи, цифрові методи шифрування поділяються на симетричні та асиметричні алгоритми, а також гібридні підходи, які поєднують переваги обох категорій.

Симетричні алгоритми використовують один і той самий ключ як для шифрування, так і для дешифрування даних. Основною перевагою цих методів є висока швидкість обробки інформації, що робить їх ефективними для захисту великих обсягів даних. Однак головним недоліком є

необхідність безпечного розповсюдження ключів між комунікуючими сторонами.

Симетричні методи шифрування використовують один і той самий ключ для шифрування і дешифрування даних. Найвідомішим представником цього підходу є AES. AES застосовується у багатьох державних, комерційних і фінансових системах завдяки високій швидкості роботи та потужній безпеці. Наприклад, у бездротових мережах стандарт WPA2 використовує AES для захисту передачі даних, що демонструє його здатність ефективно обробляти великі обсяги інформації [17]. У свою чергу, DES був популярним у минулому, проте його коротка довжина ключа (56 біт) зробила його вразливим до сучасних атак, тому його поступово замінили більш стійким алгоритмом 3DES, який застосовує тричі послідовне шифрування даних. Проте, через зростання обчислювальних можливостей сучасних комп'ютерів, навіть 3DES сьогодні вважається менш ефективним порівняно з AES [17].

Асиметричні алгоритми використовують пару ключів: відкритий і закритий. Відкритий ключ використовується для шифрування, а закритий – для дешифрування. Основна перевага цього підходу – відсутність необхідності передавати секретний ключ по незахищеним каналам. Однак цей метод значно повільніший за симетричне шифрування через високу обчислювальну складність.

Асиметричні методи шифрування ґрунтуються на використанні пари ключів – відкритого та закритого, що дозволяє безпечно обмінюватися інформацією без потреби в попередньому встановленні спільного секрету. RSA є найвідомішим прикладом такого підходу. Його безпека базується на складності факторизації великих чисел, і при використанні ключів довжиною 2048 або 4096 біт він забезпечує високий рівень захисту. RSA часто використовується в цифрових підписах, електронній пошті та інших протоколах для встановлення безпечного з'єднання. У порівнянні з RSA,

алгоритм ECC дозволяє досягти аналогічного рівня безпеки, використовуючи набагато менші розміри ключів завдяки використанню властивостей еліптичних кривих. Це робить ECC ідеальним для мобільних пристроїв та інших ресурсозалежних систем, де важлива ефективність обчислень. Інший приклад асиметричного алгоритму – ElGamal, який застосовується в різноманітних криптографічних протоколах, де безпека забезпечується через складність обчислення дискретного логарифму. Хоча ElGamal менш популярний, він знаходить своє застосування у спеціалізованих системах, де необхідна додаткова криптографічна гнучкість.

Оскільки асиметричне шифрування є повільнішим за симетричне, на практиці часто використовуються гібридні схеми, де асиметричні алгоритми застосовуються для обміну ключами, а для подальшого шифрування даних використовується симетричний алгоритм.

Гібридні методи шифрування об’єднують переваги симетричного та асиметричного підходів, що дозволяє ефективно вирішувати проблему розподілу ключів при збереженні високої швидкості обробки даних. Протокол TLS є класичним прикладом гібридного шифрування. Він використовує асиметричне шифрування для встановлення безпечного з’єднання та обміну ключами, після чого симетричні алгоритми, такі як AES, використовуються для шифрування основного трафіку. Це дозволяє забезпечити як швидкість, так і безпеку передачі даних в Інтернеті. Аналогічно, система PGP для захисту електронної пошти комбінує обидва підходи: асиметричне шифрування використовується для захисту симетричного ключа, а самі повідомлення шифруються симетричним алгоритмом. Такий підхід дозволяє користувачам легко обмінюватися зашифрованими повідомленнями, не турбуючись про безпечну передачу секретного ключа через незахищені канали.

3.2.2 Аналіз стійкості та відбір цифрового метода

Сучасна криптографія є наріжним каменем інформаційної безпеки у глобальній мережі, де захист даних від несанкціонованого доступу набуває критичного значення. Розробка ефективних цифрових методів шифрування орієнтована на забезпечення конфіденційності, цілісності та автентичності даних, незважаючи на стрімке зростання обчислювальних потужностей і розвиток методів криптоаналізу. Основними категоріями сучасних методів шифрування є симетричні, асиметричні та гібридні алгоритми. Їхня стійкість залежить не лише від математичних властивостей, але й від правильної організації протоколів обміну ключами, що дозволяє протистояти сучасним загрозам, включаючи потенційний вплив квантових комп'ютерів.

Симетричні алгоритми, такі як AES, забезпечують високий рівень безпеки завдяки довгим ключам (128, 192 або 256 біт) та здатності швидко обробляти великі обсяги даних. Вони є оптимальними для захисту даних у внутрішніх мережах або в закритих системах, де ключі можуть бути безпечно розповсюджені між сторонами [19]. Проте, проблема безпечної передачі секретного ключа залишається суттєвим викликом, оскільки навіть найсильніший симетричний алгоритм може бути скомпрометований, якщо секретний ключ потрапить до рук зловмисника.

Асиметричні алгоритми, зокрема RSA та ECC, використовують пару ключів – відкритий і закритий, що усуває необхідність передачі секретного ключа через незахищені канали. RSA, базуючись на складності факторизації великих чисел, широко застосовується для цифрових підписів і встановлення безпечних з'єднань. Проте, високі обчислювальні витрати роблять його менш ефективним для шифрування великих обсягів даних. ECC вирізняється тим, що забезпечує аналогічний рівень безпеки при значно менших розмірах ключів, що є критичним для мобільних пристроїв і систем з обмеженими ресурсами. Однак, як і всі асиметричні методи, вони

можуть стати вразливими у разі появи квантових комп'ютерів, тому сучасні дослідження зосереджені на розробці квантово-стійких алгоритмів.

Гібридні методи шифрування поєднують переваги симетричного та асиметричного підходів, що дозволяє вирішити проблему безпечного обміну ключами без втрати ефективності. Протокол TLS є класичним прикладом, де асиметричне шифрування використовується для встановлення з'єднання та обміну симетричним ключем, після чого основний трафік шифрується алгоритмом AES. Такий підхід забезпечує високий рівень безпеки та швидкість обробки, що робить його незамінним для захисту інтернет-з'єднань.

Для більш наочного порівняння основних цифрових методів шифрування наведемо таблицю, що відображає ключові параметри кожного з них (див. табл. Б.3.2.2.1).

Аналіз даних показує нам, що вибір конкретного цифрового методу шифрування має залежати від специфічних умов застосування. Симетричні алгоритми є незамінними для систем, де критично важлива швидкість обробки великих обсягів даних, але їхня ефективність обмежується проблемами безпечного обміну ключами. Асиметричні алгоритми, навпаки, забезпечують зручний механізм встановлення безпечного з'єднання, але вимагають значних обчислювальних ресурсів, що робить їх менш придатними для реального часу в системах високої навантаженості. Гібридні методи, які поєднують обидва підходи, демонструють найвищу стійкість до атак та оптимальне співвідношення між швидкістю і безпекою.

У підсумку, для створення системи аналогово-цифрового шифрування в умовах обмежених ресурсів, тоді як аналоговий метод використовується скремблювання, оптимальним вибором є симетричне шифрування, зокрема алгоритм AES [19]. Це пов'язано з тим, що AES забезпечує високу швидкість обробки даних і відмінну криптографічну стійкість при відносно невисоких обчислювальних витратах, що є

критичним у середовищах із обмеженою апаратною потужністю. Завдяки своїй ефективності, AES здатен швидко обробляти великі обсяги даних, що дозволяє компенсувати потенційні недоліки скремблювання, яке, хоч і забезпечує базовий рівень маскування сигналу, може бути вразливим до спеціалізованих методів аналізу [19]. Крім того, симетричні методи, як правило, легше інтегруються в гібридні схеми шифрування, де аналогова частина (скремблювання) доповнюється цифровою обробкою, що дозволяє створити багаторівневу систему захисту. Таким чином, використання AES у поєднанні зі скремблюванням дозволить нам досягти оптимального співвідношення між ефективністю, швидкістю і рівнем безпеки, що робить цей підхід найкращим для застосування в умовах з обмеженими ресурсами.

3.3 Способи реалізації обраних методів шифрування

3.3.1 Способи реалізації гібридного шифрування

Теоретично гібридна система спирається на ідею багаторівневого кодування, де аналоговий етап забезпечує маскування фізичної форми сигналу, а цифровий — криптографічну трансформацію вмісту. Поєднання цих підходів дозволяє ускладнити як математичний аналіз сигналу, так і його фізичну інтерпретацію сторонніми спостерігачами.

У практичному контексті ефективним рішенням є використання аналогового скремблювання як первинного захисного шару. Скремблювання змінює структуру сигналу таким чином, щоб він залишався формально "аналоговим", але втратив читабельність або розпізнаваність для стандартних методів прийому. Проте скремблювання саме по собі не забезпечує високого рівня криптографічної стійкості, оскільки може бути вразливим до методів спектрального чи статистичного аналізу.

Для подолання цієї вразливості доцільним є використання цифрового симетричного шифрування, зокрема алгоритму AES. AES відомий своєю високою продуктивністю, криптостійкістю та ефективною реалізацією

навіть на обмежених апаратних платформах (наприклад, вбудованих системах, IoT-пристроях). Завдяки своїй швидкодії AES здатен швидко обробляти великі обсяги даних, що критично в системах реального часу, де затримки неприпустимі.

З теоретичної точки зору, симетричні шифри легше синхронізуються з аналоговими компонентами системи, оскільки не вимагають складного управління ключами, як це відбувається в асиметричних схемах. Це дозволяє розробити уніфіковану архітектуру гібридного шифрування, в якій аналогове скремблювання працює як "фізичний бар'єр", а AES забезпечує "логічне зашифрування".

Таким чином, застосування AES у поєднанні зі скремблюванням дозволяє реалізувати нам в цій роботі оптимальну систему захисту

У цьому розділі ми розглянемо практичні підходи до реалізації обраних методів шифрування, що включають як алгоритмічні рішення, так і використання наявної апаратної платформи. Основна ідея полягає у створенні системи, де аналогові методи, такі як скремблювання, інтегровані з цифровими алгоритмами шифрування, що дозволяє забезпечити багаторівневий захист даних. Скремблювання, як метод попереднього захисту сигналу, передбачає зміну часових, частотних або фазових характеристик для маскування його змісту. Реалізація цього методу може здійснюватися різними підходами, що забезпечують як програмну гнучкість, так і апаратну простоту.

3.3.2 Використання ELEGO UNO R3 ChipKit з Arduino IDE для реалізації аналогового шифрування

В сучасних умовах інтеграції цифрових технологій у систему керування та обробки сигналів важливим аспектом є можливість створення аналогового сигналу з використанням доступної апаратної платформи. ELEGO UNO R3 ChipKit, сумісний з Arduino IDE, є чудовим прикладом

такої техніки, оскільки дозволяє реалізувати подачу аналогових сигналів через використання методів, заснованих на цифровому керуванні. Хоча більшість мікроконтролерів цього типу не мають вбудованого цифрово-аналогового перетворювача, існує ефективний підхід до імітації аналогових сигналів – це генерація імпульсно-модуляційного сигналу, який після відповідного фільтрування перетворюється в стабільне аналогове значення.

Основним принципом є те, що PWM-сигнал представляє собою послідовність цифрових імпульсів, ширина яких змінюється згідно з заданою величиною – так званою скважністю. Зміна скважності дозволяє варіювати середню напругу на виході, що еквівалентно аналоговому значенню. Для отримання гладкого аналогового сигналу цей цифровий імпульсний сигнал проходить через низькочастотний фільтр, зазвичай побудований на основі резистора та конденсатора (RC-фільтр). Завдяки цьому компонент фільтра усереднює коливання і видає постійне або плавно змінне напруження, яке можна використовувати для керування аналоговими пристроями, як-от світлодіоди, двигуни або аудіопідсилювачі.

На платформі ELEGO UNO R3 ChipKit за допомогою Arduino IDE розробник має доступ до бібліотек та функцій, що спрощують керування PWM-виходами. Наприклад, стандартна функція «analogWrite()» дозволяє задати значення скважності для конкретного цифрового виводу, який підтримує PWM. Відповідно, зміна параметру, переданого у функцію, змінює середнє значення напруги на виході, що після додаткового RC-фільтрування стає аналоговим сигналом. Цей підхід є надзвичайно гнучким, оскільки дозволяє програмно керувати сигналом, здійснювати його плавне регулювання та адаптувати алгоритми керування до конкретних умов експлуатації.

Таким чином, використання ELEGO UNO R3 ChipKit у поєднанні з Arduino IDE для генерації аналогового сигналу за допомогою PWM є ефективним і доступним рішенням, яке дозволяє перевести цифрове

керування в аналоговий формат. Це дає змогу створювати інтегровані системи з високою функціональністю, де простота реалізації поєднується з гнучкістю та адаптивністю до змінних умов експлуатації, що робить даний підхід оптимальним для широкого спектра практичних застосувань.

Сучасні мікроконтролерні системи надають широкі можливості для створення електронних пристроїв. Одним із популярних рішень є мікроконтролерна плата ELEGO UNO R3 ChipKit, яка є сумісною з Arduino UNO. В її основі лежить мікроконтролер ATmega328P, що забезпечує підтримку великої кількості бібліотек та модулів Arduino [22]. Це робить її зручною для використання як у навчальних, так і в професійних проектах.

Одним із корисних модулів для роботи з мікроконтролером є ультразвуковий датчик відстані HC-SR04. Принцип його роботи заснований на випромінюванні та прийомі звукових хвиль. Він дозволяє з високою точністю визначати відстань до об’єкта, що є необхідним у багатьох застосуваннях, таких як робототехніка, системи безпеки та автоматизація.

Функціонування HC-SR04 базується на вимірюванні часу, за який відбитий сигнал повертається до приймача. Відстань до об’єкта можна обчислити за формулою [22]:

$$d = \frac{t \times v}{2},$$

де d – відстань, t – час проходження сигналу, а v – швидкість звуку в повітрі (приблизно 343 м/с).

Для генерації аналогового сигналу застосовується широтно-імпульсна модуляція. Мікроконтролер формує сигнал, частота та заповнення якого змінюються залежно від виміряної відстані. Це дозволяє використовувати датчик у проектах, де потрібна динамічна зміна параметрів керування на основі відстані до об’єкта.

Цей код дозволяє отримувати дані про відстань, а також генерувати ШІМ-сигнал, значення якого пропорційне виміряній відстані. Завдяки

використанню функції analogWrite() можна динамічно змінювати параметри системи, залежно від отриманих даних.

Таким чином, поєднання мікроконтролера ELEGO UNO R3 ChipKit та ультразвукового датчика HC-SR04 дозволяє створювати ефективні рішення для вимірювання відстані. Це відкриває широкі можливості для автоматизації та розробки інтелектуальних систем, що реагують на зміну навколишнього середовища.

3.3.3 Використання сучасних алгоритмів для імітації аналогового метода

Один із сучасних підходів полягає в застосуванні алгоритмічних моделей для цифрової імітації аналогових процесів скремблювання. За допомогою математичного моделювання можна розбивати вхідний сигнал на сегменти та застосовувати до них псевдовипадкове переставлення або зміну характеристик, що імітує поведінку аналогового скремблювання. Цей метод дозволяє точно налаштовувати параметри процесу: регулювати тривалість сегментів, частоту перестановок і ступінь змін у сигналі, що забезпечує високий рівень адаптивності системи.

Завдяки додаванню випадкового відхилення у значення ШІМ-сигналу, система отримує ефект динамічного скремблювання. Це дозволяє усунути можливі перешкоди або спотворення при використанні датчика, а також підвищує стійкість до завад. Такий підхід може бути корисним у розробці інтелектуальних адаптивних систем, які працюють у складних умовах середовища.

Рядок analogWrite(PWM_OUT, pwmValue + random(-10, 10)); відправляє ШІМ-сигнал зі змінним значенням заповнення імпульсу (duty cycle), що коливається в межах випадкового зсуву ±10 одиниць (див. Додаток А). Це означає, що ширина імпульсів сигналу змінюється в межах відхилень від основного значення pwmValue.

На вихідному піні PWM_OUT генерується ШІМ-сигнал з робочим циклом, який змінюється в межах випадкового розсіювання. Наприклад, якщо pwmValue = 150, то фактичне значення, передане у функцію analogWrite(), буде в діапазоні [140, 160] (див. Додаток А).

Такий підхід має кілька важливих переваг. По-перше, зниження перешкод та резонансних ефектів, які можуть виникати в системах з повторюваними ШІМ-сигналами. Додавання невеликого випадкового шуму зменшує ймовірність стабільних гармонік, що покращує якість сигналу. По-друге, імітація природних варіацій є корисною у випадках керування освітленням або звуковими ефектами, оскільки додавання випадкових змін робить перехід між рівнями більш плавним і природним. По-третє, у комунікаційних або криптографічних застосуваннях додавання випадкових варіацій може ускладнювати розпізнавання та перехоплення сигналу, що підвищує рівень безпеки переданих даних.

На приймаючій стороні сигнал може бути оброблений різними методами. Фільтрація середнього значення дозволяє усунути шум шляхом усереднення кількох останніх вимірювань. Аналіз спектра сигналу дає змогу розрізняти корисний сигнал від випадкових змін і, таким чином, забезпечувати стабільність роботи системи. Застосування алгоритмів адаптивної фільтрації, таких як фільтр Калмана, дає можливість прогнозувати справжнє значення сигналу, що підвищує точність системи управління.

Динамічна зміна ШІМ-сигналу є ефективним інструментом керування електронними пристроями, що дозволяє адаптувати їхню роботу до змінних умов. Додавання випадкового зсуву сигналу допомагає знизити перешкоди, зробити управління більш плавним і природним, а також забезпечити додатковий рівень безпеки у цифрових комунікаціях. Це робить ШІМ незамінною технологією в сучасних мікроконтролерних системах, які потребують точного та надійного керування.

3.3.4 Способи реалізації цифрового методу

Алгоритм AES є сучасним стандартом симетричного шифрування, що забезпечує високий рівень безпеки і ефективність обробки даних (див. рис 3.4). Реалізація AES може здійснюватися як у програмному, так і в апаратному середовищі. Програмна реалізація полягає у використанні готових бібліотек і фреймворків, які підтримують шифрування і дешифрування даних за допомогою AES [20]. Це дозволяє нам інтегрувати алгоритм у різноманітні додатки, серверні та клієнтські програми, забезпечуючи захист даних у мережевих з'єднаннях, базах даних і файлових системах. Окрім цього, апаратна реалізація AES здійснюється за допомогою спеціалізованих криптографічних модулів, що вбудовуються у мікроконтролери або процесори [20]. Таке рішення значно підвищує швидкість обробки даних, зменшує затримки і знижує ризик витоку ключів, оскільки апаратні модулі важче модифікувати або атакувати. Інтеграція апаратної реалізації AES в комплексну систему захисту дозволяє створити багаторівневу систему шифрування, де цифрове шифрування на основі AES стає останнім рубежем оборони при спробах перехоплення або аналізу даних.

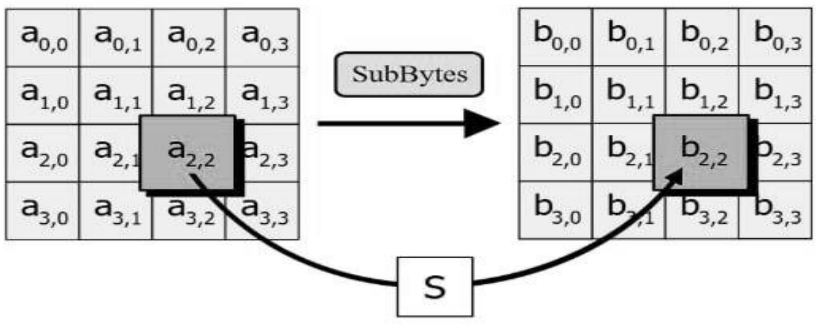


Рисунок 3.4 - Схема роботи AES [20]

Таким чином, розглянуті нами способи реалізації обраних методів шифрування демонструють можливості адаптації як цифрових, так і

аналогових підходів. Використання сучасних алгоритмічних рішень для скремблювання забезпечує гнучкість і адаптивність системи, а застосування доступної апаратної платформи дозволяє швидко розробляти і тестувати прототипи.

ШІМ-сигнал використовується в цій роботі для передавання аналогової інформації через цифровий канал. Змінюючи робочий цикл сигналу, можна кодувати дані, які зчитує приймальна сторона. Однак у традиційних системах передача такого сигналу може бути вразливою для атак через передбачуваність параметрів сигналу. Додавання випадкового зсуву у analogWrite() створює хаотичність у сигналі, що ускладнює його аналіз, а AES-шифрування гарантує, що навіть у разі перехоплення сигналу зловмисник не зможе отримати справжні дані без відповідного ключа (див. Додаток А).

Процес передачі даних у такій системі відбувається у кілька етапів. Спочатку передані дані шифруються за допомогою AES, перетворюючи інформацію у псевдовипадковий набір бітів. Далі отримані бітові значення використовуються для зміни параметрів ШІМ-сигналу, наприклад, зміни його робочого циклу або частоти імпульсів. Додаткове внесення випадкових коливань у signalWrite() допомагає маскувати корисний сигнал від аналізу. На приймальній стороні здійснюється зворотний процес: фільтрація ШІМ-сигналу, виділення бітової послідовності та розшифрування даних за допомогою AES(див. Додаток А).

Перевагою нашого підходу є підвищена стійкість до атак. Навіть якщо зловмисник отримає сигнал, випадкові варіації у ШІМ зроблять його аналіз складнішим. Окрім того, криптографічний захист AES гарантує, що без відповідного ключа отримана інформація залишиться нерозпізнаною. Це може бути корисним у системах бездротового зв'язку, керуванні дронами, захищених системах зв'язку та інших галузях, де важливо забезпечити безпечну передачу даних.

Таким чином, поєднання динамічного ШІМ-сигналу з AES-шифруванням забезпечує ефективний механізм захисту інформації, підвищуючи її стійкість до аналізу та атак. Це відкриває нові можливості для безпечної передачі даних у вбудованих системах та бездротових мережах для наукового товариства.

3. 4 Використання гібридного метода шифрування

Основою нашої гібридної системи є мікроконтролер, наприклад, Arduino UNO, який генерує ШІМ-сигнал і керує його параметрами. Ультразвуковий датчик HC-SR04 використовується для визначення відстані до об'єкта, що дозволяє змінювати характеристики сигналу залежно від вимірюваних даних. Для правильного підключення потрібні резистори та з'єднувальні проводи, а також виконавчий пристрій, такий як світлодіод або двигун, що отримуватиме сигнал і змінюватиме свій стан відповідно до змін параметрів ШІМ.

Наступний код демонструє реалізацію динамічного керування ШІМ-сигналом на платформі Arduino(див. Додаток А). Він змінює значення широтно-імпульсного сигналу залежно від показань ультразвукового датчика HC-SR04. Для реалізації AES-шифрування на платформі Arduino можна використати бібліотеку Crypto [22]. Ось приклад коду, який шифрує дані перед передачею через ШІМ(див. Додаток А). Вираз analogWrite(PWM_OUT, pwmValue + random(-10, 10)); додає випадковий зсув до вихідного сигналу (див. Додаток А). Це означає, що значення ШІМ не є абсолютно стабільним, а має невеликі випадкові коливання у діапазоні ±10 одиниць.

Таким чином, у ході нашого дослідження було здійснено аналіз аналогових та цифрових методів шифрування, що дозволило підібрати оптимальні підходи для захищеної передачі даних. Розглянуто класичні аналогові методи та сучасні цифрові алгоритми шифрування, включаючи

AES, що забезпечує високий рівень безпеки. Аналіз стійкості методів дозволив визначити доцільність використання комбінації аналогових і цифрових підходів, зокрема застосування скремблювання у ШІМ-сигналі для ускладнення аналізу переданих даних.

Ми запропонували способи шифрування на основі обраних методів, включаючи використання плати ELEGO UNO R3 ChipKit для генерації аналогового сигналу, а також програмну реалізацію AES-алгоритму для шифрування даних перед передачею. Розглянули варіанти застосування сучасних алгоритмів для імітації аналогового методу та їх комбінування у гібридному підході.

Запропонована нами методика дозволяє підвищити захищеність систем зв'язку та передачі даних, особливо у бездротових середовищах, де існує високий ризик перехоплення інформації. Завдяки використанню випадкових варіацій ШІМ-сигналу та AES-шифрування можна значно ускладнити аналіз переданих даних зловмисниками. Отримані результати можуть бути використані для подальших досліджень та розробки більш складних методик захищеної передачі даних у вбудованих та IoT-системах.

4 РОЗРОБКА ГІБРИДНОЇ СИСТЕМИ АНАЛОГО-ЦИФРОВОГО ШИФРУВАННЯ

4.1 Опис програмної середи та застосованої техники

Програмна середа Arduino - Arduino Integrated Development Environment або Arduino IDE є офіційним інструментом для розробки, компіляції та завантаження програмного коду (скетчів) на мікроконтролери сімейства Arduino [21]. Вона була створена з метою забезпечення зручного середовища для розробників, студентів та початківців, які працюють з мікроконтролерами, електронікою та робототехнікою (див. рис. 4.1).

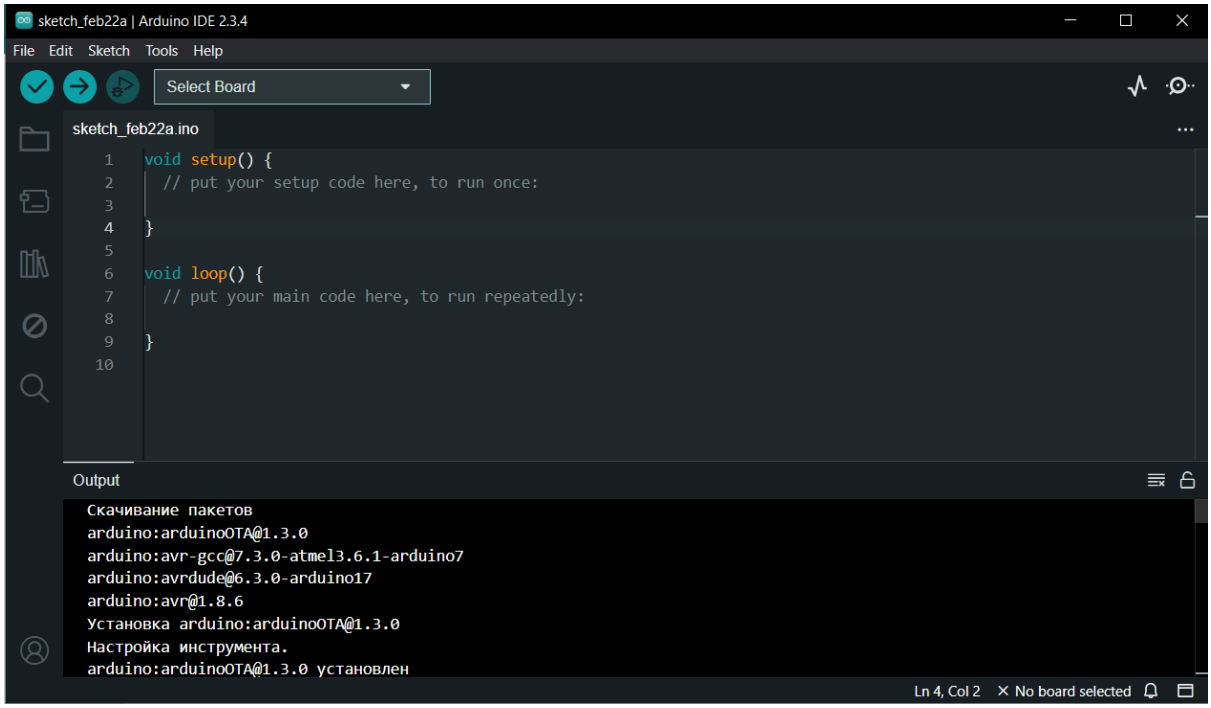


Рисунок 4.1 - Програмна середа Arduino

Програмування в Arduino IDE базується на двох основних функціях:

- void setup() – функція ініціалізації, яка виконується один раз після завантаження програми на плату. У ній зазвичай задаються режими пінів (входи/виходи), ініціалізація дисплеїв, датчиків тощо [21].

- void loop() – головна функція, яка виконується безперервно. Вона містить основну логіку програми, наприклад зчитування значень з датчиків, обробку сигналів або управління пристроями [21].

При розробці використовуються також бібліотеки – готові модулі коду, які розширюють функціональність середовища (наприклад, для роботи з дисплеями, датчиками, сервоприводами тощо).

Arduino IDE підтримує широкий спектр плат: від стандартних Uno, Nano, Mega до розширених моделей типу Due, MKR, а також сумісних плат (наприклад, Elegoo, NodeMCU тощо). Вибір плати здійснюється через меню Інструменти > Плата, а вибір порту – через Інструменти > Порт [21].

Користувач також може встановлювати додаткові ядра та бібліотеки для роботи з нестандартним обладнанням за допомогою Менеджера плат та Менеджера бібліотек.

Програмна середа Arduino IDE є ефективним інструментом для навчання, прототипування та розробки вбудованих систем. Її простота, функціональність і гнучкість роблять її однією з найпопулярніших платформ у сфері електроніки та STEM-освіти. Вона слугує мостом між апаратним забезпеченням і програмною логікою, надаючи користувачам можливість швидко та інтуїтивно реалізовувати проекти будь-якої складності.

Застосована техніка, описана в таблиці (див. табл. Б.4.1.1), базується на апаратному забезпеченні з комплекту "Arduino Starter Kit", а саме — з використанням мікроконтролера Arduino Uno R3, який є основним елементом керування всієї системи..

4.2 Реалізація гібридного перетворення даних

У нашому проєкті шифрування цифрових даних (виміряної відстані) здійснюється за допомогою алгоритму AES, після чого зашифроване

значення використовується для керування широтно-імпульсним сигналом. Завдяки випадковому зсуву в межах ±10 одиниць, сигнал PWM набуває невеликих коливань (див. рис. 4.2). Такий підхід створює умовну подобу аналогового шифрованого сигналу, де змінний вихід відображає зашифровану інформацію у вигляді "аналогоподібної" модуляції.

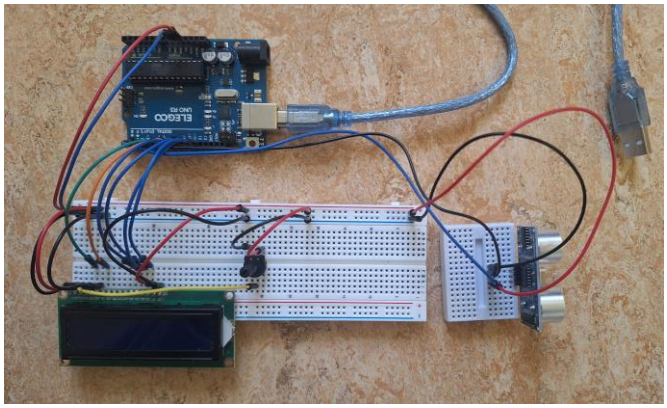


Рисунок 4.2 - Реалізація гібридного шифрування

Як центральний керуючий елемент використовується плата Elegoo Uno R3, яка повністю сумісна з Arduino Uno (див. рис. 4.3). Живлення до плати подається через USB-кабель, підключений до комп'ютера. Крім подачі живлення, USB-інтерфейс використовується також для прошивки мікроконтролера і моніторингу даних через послідовний порт. На платі є світлодіодний індикатор, який свідчить про подачу живлення і роботу пристрою.

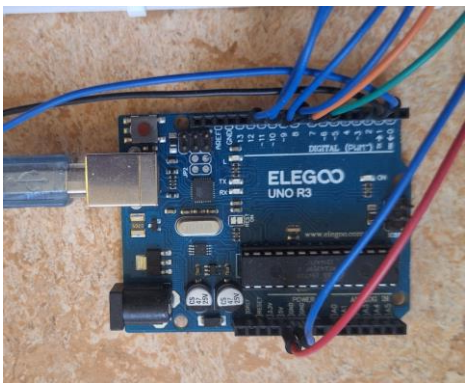


Рисунок 4.3 - Elegoo Uno R3

У збірці задіяні дві макетні плати. На основній макетній платі розміщено два компоненти. Перший - LCD-дисплей 16x2 символу- відображає числові дані, отримані від ультразвукового датчика (див. рис. 4.4). Підключення здійснюється безпосередньо через цифрові піни, унаслідок чого використовується щонайменше шість дротів для передавання команд і даних. Підключені сигнальні лінії RS, E, D4, D5, D6 і D7. Другий - потенціометр, використовується для регулювання контрастності дисплея. Він має три виводи: один під'єднаний до напруги живлення (5 В), другий - до землі, а третій - до виводу V0 дисплея.

Живлення і земля від мікроконтролера під'єднані до бічних шин макетної плати (червона - VCC, синя - GND), звідки живлення розподіляється на всі інші компоненти.

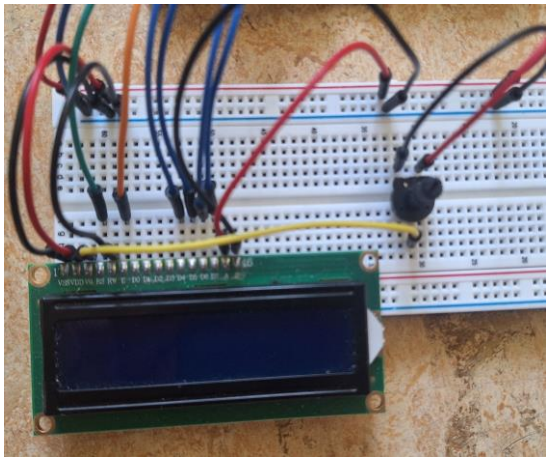


Рисунок 4.4 - LCD-дисплей 16x2 символу

На окремій невеликій макетній платі розташовано ультразвуковий далекомір HC-SR04, який призначений для вимірювання відстані до об'єктів на основі принципу ехолокації (див. рис. 4.5). Пристрій має чотири виводи: VCC - живлення (5 В), GND - земля, Trig - вхідний сигнал (активація вимірювання), Echo - вихідний сигнал (відбитий імпульс).

Підключення Trig і Echo здійснюється до цифрових пінів мікроконтролера, призначення яких вказується в програмному коді.

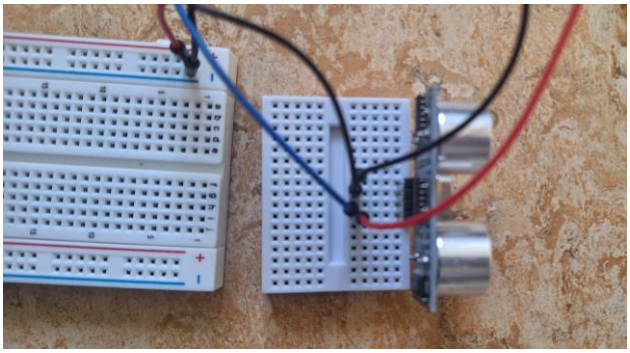


Рисунок 4.5 - Ультразвуковий далекомір HC-SR04

У проекті застосовуються перемички DuPont типу "тато-мама", що дає змогу зручно з'єднувати контакти модулів з макетною платою і мікроконтролером. Розподіл проводів такий: червоні дроти використовуються для подачі живлення (5 В), чорні дроти для підключення до землі; сині, зелені та помаранчеві дроти - для сигнальних з'єднань між мікроконтролером і модулями (LCD і HC-SR04).

Дроти під'єднані до цифрових пінів Arduino відповідно до логіки бібліотеки керування дисплеєм і датчиком.

У результаті ми реалізуємо функціональний модуль, здатний вимірювати відстань до об'єкта, що знаходиться перед ультразвуковим датчиком, і виводити відповідну інформацію на РК-дисплей (див. рис. 4.6). Принцип дії ґрунтується на надсиланні ультразвукового імпульсу та вимірюванні часу його повернення, що дає змогу обчислити відстань на основі швидкості звуку.

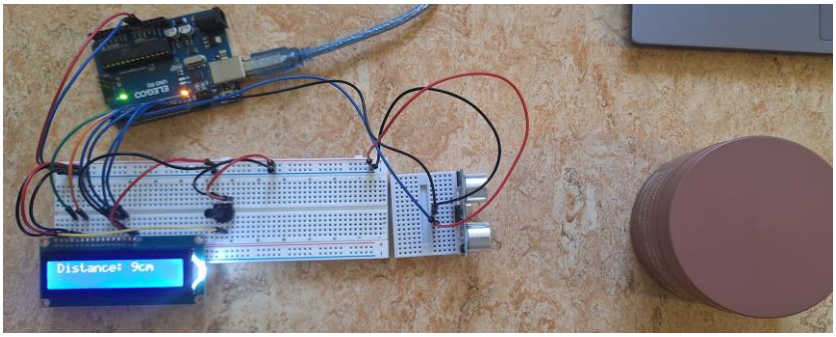


Рисунок 4.6 - Функціональний модуль

Діапазон дальності його вимірювання становить від 2 до 400 см [22]. У комплект модуля з HC SR04 також входять ресивер і трансмітер. Якщо подати на вихід Trig імпульс тривалістю 10 мкс, то в ультразвуковому далекомірі HC-SR04 відбудеться перетворення сигналу на 8 імпульсів із частотою 40 кГц, які через випромінювач будуть надіслані вперед [22]; Коли імпульси дійдуть до перешкоди, вони відіб'ються від неї та будуть прийняті приймачем R, що забезпечить наявність вхідного сигналу на виході Echo; На стороні контролера отриманий сигнал за допомогою формул слід перевести у відстань.

AESLib aesLib відповідає за створення об’єкта бібліотеки AES для доступу до методів шифрування (див. Додаток А).

Строка byte aes_key[16] = {0x01, 0x02, ..., 0x10} потрібна для встановлення 128-бітного ключа шифрування AES (16 байтів), який буде використано для шифрування блоку даних (див. Додаток А).

Перший наш крок це, коли ультразвуковий датчик HC-SR04 вимірює відстань до об'єкта (в см). Це цифрове значення (наприклад, 35 см) передається далі. Отримане значення відстані перетворюється на байтовий масив (тобто набір чисел для обробки). Далі цей масив шифрується за допомогою цифрового алгоритму AES — одного з найнадійніших методів шифрування. В результаті виходить новий набір байтів, у якому первинна інформація (відстань) більше не читається напряму.

Наступний крок - один байт із зашифрованого набору (перший) використовується для керування широтно-імпульсною модуляцією (PWM), тобто сигналом, що змінюється по ширині імпульсів. Це імітує аналоговий вихід. До значення ШІМ-сигналу додається випадковий зсув ±10 одиниць. Цей шум робить сигнал менш передбачуваним, і візуально або електрично він виглядає як слабкий "зашумлений" аналоговий сигнал, який несе зашифровану інформацію.

Таким чином, ми отримуємо приклад цифрового-аналогового перетворення даних.

4.3 Тестування базових елементів аналого-цифрового перетворення даних

На дисплеї ми бачимо виміряну відстань 2 см (див. рис. 4.7). Поруч розташований об'єкт, що знаходиться на відповідній відстані від ультразвукового датчика, що підтверджує точність вимірювання.

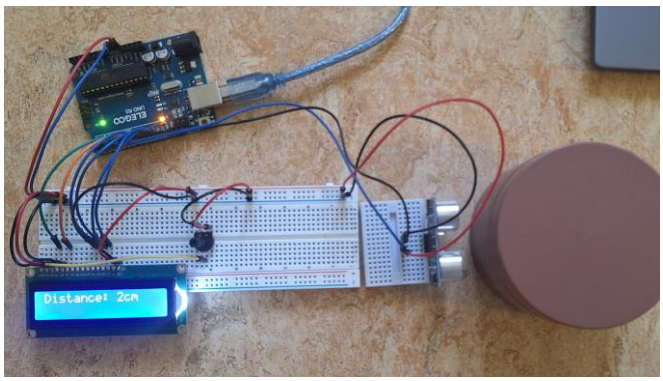


Рисунок 4.7 - Функціональний модуль, вимір 2 см

На наступному графіку зображено поведінку PWM-сигналу на виході Arduino, коли відстань, виміряна ультразвуковим датчиком, становить 2 см (див. рис. 4.8). Значення відстані було зашифроване з використанням AES, і один з байтів шифрованих даних (у нашому прикладі — близько 150) використовувався для генерації сигналу широтно-імпульсної модуляції.

Рисунок 4.8 - Поведінка PWM-сигналу, вимір 2 см

Оскільки до цього значення додається випадкове коливання у межах ±10 одиниць за допомогою функції random(-10, 10), сигнал на виході стає "зашумленим" (див. Додаток А). Це видно на графіку — жовта крива коливається навколо сірого пунктирного рівня (базове значення). Такі флуктуації роблять сигнал непостійним, і ми отримуємо аналогову змінну амплітуду.

Далі протестуємо наше цифрово-аналогове перетворення для відстанні, яка поступово зменшується (див. рис. 4.9-4.10).

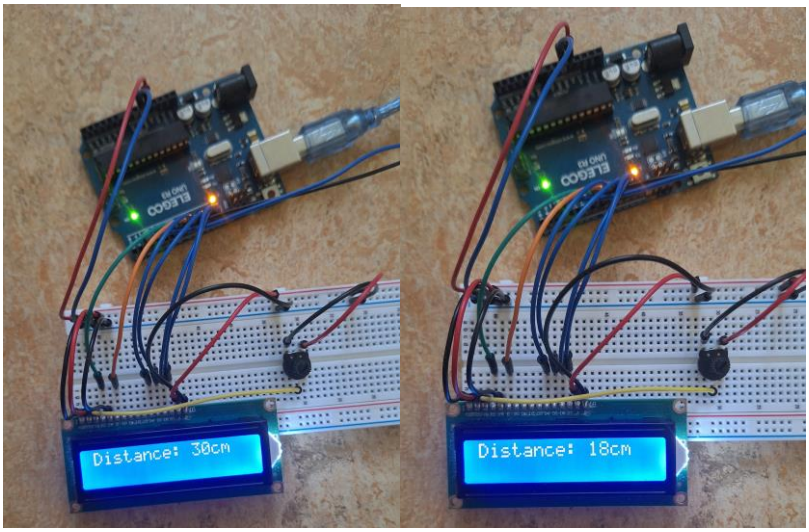


Рисунок 4.9-4.10 - Функціональний модуль, вимір від 30 до 18 см

На дисплеї, як ми бачимо, відображено зміну відстані від 30 до 18 см у процесі наближення об’єкта до ультразвукового датчика. Положення об’єкта відповідає показникам на екрані, що демонструє правильну роботу системи вимірювання в динаміці.

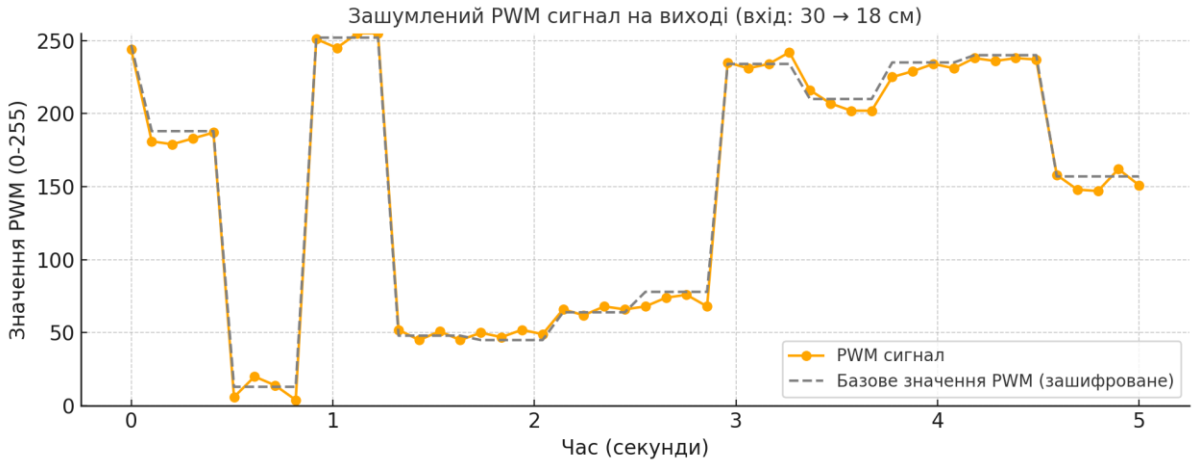


Рисунок 4.11 - Поведінка PWM-сигналу, вимір 30-18 см

На цьому графіку зображено, як змінюється PWM-сигнал на виході Arduino, коли ультразвуковий датчик вимірює відстань, що поступово зменшується від 30 см до 18 см (див. рис. 4.11). Отримане значення відстані шифрується за допомогою алгоритму AES, і з отриманого зашифрованого блоку береться перший байт (ciphertext[0]), який використовується як базове значення для формування PWM-сигналу (див. Додаток А). Сіра пунктирна лінія: показує базове значення PWM, яке відповідає одному з байтів AES-зашифрованого результату. Жовта крива з точками: показує реальний PWM-сигнал, який отримується після додавання випадкового шуму у межах ±10 одиниць.

В результаті, у ході дослідження було проаналізовано поведінку широтно-імпульсного сигналу (PWM), сформованого на базі зашифрованих даних від ультразвукового датчика відстані. Основною метою експерименту було оцінити вплив шифрування (алгоритм AES-128 у режимі ECB) на форму вихідного PWM-сигналу, а також вивчити ефект додаткового шуму, що вводиться для ускладнення зворотної інтерпретації даних.

Перший графік демонструє ситуацію з фіксованою відстанню (2 см), де вихідний PWM-сигнал коливається навколо певного значення (~150), що

відповідає одному з байтів AES-зашифрованого блоку. На графіку чітко видно, що доданий шум у межах ±10 одиниць створює флуктуації, що робить сигнал змінним у часі навіть за незмінного вхідного параметра.

Другий графік моделює зміну відстані у діапазоні від 30 до 18 см. Зашифровані значення та відповідний PWM-сигнал демонструють відсутність прямої кореляції між відстанню і вихідним значенням PWM. Це є характерною властивістю блочного шифрування AES, де навіть незначна зміна у вхідному блоці призводить до суттєвих змін у шифротексті. Додатковий шум ще більше маскує структуру сигналу, підвищуючи його стійкість до аналізу.

Таким чином, дослідження підтвердило, що використання AES-шифрування у поєднанні зі скремблюванням широтно-імпульсного сигналу забезпечує надійне маскування переданої інформації. Метод ефективно унеможливлює зворотну ідентифікацію вхідних значень (відстані) на основі аналізу PWM-сигналу, навіть при наявності доступу до фізичного каналу передачі. Отримані результати можуть бути використані у системах безпечної аналогової передачі даних, зокрема для сенсорних або вбудованих пристроїв.

ВИСНОВКИ

У ході даної дипломної роботи мною було здійснено повний цикл дослідження процесів шифрування інформації в контексті інформаційної безпеки; аналіз аналогових методів шифрування та пропозиції щодо їх адаптація до цифрових технологій; мною було проведено дослідження можливостей застосування аналогових методів у цифровій криптографії, визначення їхніх переваг і недоліків; було розроблено теоретичну модель, реалізації та тестування практичної моделі гібридного шифрування, яка поєднує в собі цифровий та аналоговий методи захисту інформації в контексті вбудованих мікропроцесорних систем на базі Arduino. Таким чином мета цієї дипломної роботи була досягнута.

Для цього мною була створена функціональна система, яка здійснює зчитування відстані за допомогою ультразвукового датчика HC-SR04, перетворює отримані дані у зашифровану форму за допомогою симетричного алгоритму AES, а потім передає ці дані у вигляді широтно-імпульсного сигналу з додаванням випадкового шуму. Застосування AES дозволило гарантувати високий рівень криптографічного захисту, тоді як додаткове псевдовипадкове зміщення в PWM-сигналі ускладнило можливість прямого дешифрування чи аналізу сигналу за аналоговими характеристиками. Таким чином, система одночасно реалізує захист на двох рівнях: цифровому — через алгоритмічне шифрування, та аналоговому — через фізичну модифікацію сигналу.

У процесі реалізації моделі мною було також проведено спостереження за поведінкою системи при різних значеннях вхідних даних, включаючи як фіксовані, так і змінні відстані. На дисплеї виводились відповідні вимірювання, що дозволяло верифікувати правильність роботи датчика, AES-шифрування, а також коректність відображення у вигляді PWM-сигналу. Для повноти аналізу результати були також представлені у

графічній формі, що дозволило візуалізувати ефект додавання шуму та вплив змін вхідних параметрів на вихідний зашифрований сигнал.

Таким чином, результатом стало створення узагальненої адаптивної моделі криптографічного захисту для сенсорних пристроїв, яка інтегрує цифрові алгоритми з аналоговими методами маскування. Ця модель довела свою ефективність у контексті простих апаратних засобів і є перспективною для подальшого використання в інтернеті речей, робототехнічних системах та автономних сенсорних мережах, де критично важливим є не лише шифрування даних, але й запобігання їхньому перехопленню або зчитуванню на фізичному рівні.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Shannon C.E. 'Communication Theory of Secrecy Systems'. Bell System Technical Journal, 1949 / [Електронний ресурс] - Режим доступу: https://pages.cs.wisc.edu/~rist/642-spring-2014/shannon-secrecy.pdf , 656 С.

2. Горбенко І. Д. Прикладна криптологія. Теорія. Практика. Застосування : монографія. / І. Д. Горбенко, Ю. І. Горбенко//, Харків : Форт, 2012. - 868 с.

3. A Survey and Analysis of the Image Encryption Methods / ResearchGate. – Режим доступу: https://www.researchgate.net/figure/Classification-of-Cryptography-16_fig1_322277374 (дата звернення: 16.05.2025).

4. Громико І. О. Криптографія у загальній парадигмі захисту інформації. Варіант виходу із квантової кризи // Захист інформації. INSIDE. - 2016. - №6. - С.48-56.

5. Громико І.О. «Криптографія нового покоління: інтегральні рівняння як альтернатива методології алгебри» К., / Броншпак Г.Г. Громико І. О., Доценко С. І., Перчик Е. Л. // Всеукраїнська зб. «Радіотехніка», 2014

6. A Review of Analog Speech Scrambling for Secure Communication [Електронний ресурс] // ResearchGate. – Режим доступу: https://www.researchgate.net/publication/294682428_A_Review_of_Analog_Speech_Scrambling_for_Secure_Communication (дата звернення: 15.05.2025).

7. Громико І.О. Постквантова криптографія у ракурсі загальної парадигми захисту інформації // Інформаційні системи та технології: матеріали 5-ї Міжнародної НТК. Х: Типографія Мадрид, 2016 – 240 с. – С. 292-293.

8. Analog vs. Digital Signals [Електронний ресурс] // Allelco Electronics. – Режим доступу: https://www.allelcoelec.com/blog/analog-vs.digital-signals.html (дата звернення: 16.05.2025).

9. Криптографічні методи [Електронний ресурс] //VPN Unlimited. – Режим доступу: https://www.vpnunlimited.com/ua/help/cybersecurity/cryptographic-techniques?utm_source=chatgpt.com (дата звернення: 16.04.2025).

10. Шифрування: Типи та алгоритми. Що це і який тип шифрування кращий? [Електронний ресурс] //hostkoss blog. – Режим доступу: https://hostkoss.com/b/uk/encryption-types-algorithms/?utm_source=chatgpt.com (дата звернення: 15.04.2025).

11. An Introduction to Spread-Spectrum Communications [Електронний ресурс] // Analog Devices. – Режим доступу: https://www.analog.com/en/resources /technical-articles/introduction-to-spreadspectrum-communications--maxim-integrated.html (дата звернення: 14.05.2025).

12. SIGSALY [Електронний ресурс] // Wikipedia. – Режим доступу: https://en.wikipedia.org/wiki/SIGSALY (дата звернення: 16.05.2025).

13. Громико І.О. «NCDP - НЕЙРОКОЛЬОРОВОДИНАМІЧНЕ ПРОГРАМУВАННЯ // Interdisciplinary research: scientific horizons and perspectives SECTION 12 // INFORMATION TECHNOLOGIES AND SYSTEMS С. 64 -70 (дата звернення: 20.05.2025).

14. A highly secure stream cipher based on analog-digital hybrid chaotic system [Електронний ресурс] // ScienceDirect. – Режим доступу: https://www.sciencedirect.com/science/article/abs/pii/S0020025521012512 (дата звернення: 16.05.2025).

15. Analog–Digital Combined High-Secure Optical Communication System Based on Chaotic Circuit Driving [Електронний ресурс] // MDPI Photonics. – Режим доступу: https://www.mdpi.com/2304-6732/9/9/669 (дата звернення: 16.05.2025).

16. NIST to Standardize Encryption Algorithms That Can Resist Attack by Quantum Computers [Електронний ресурс] // National Institute of Standards and Technology (NIST). – Режим доступу: https://www.nist.gov/news-events/news/2023/08/nist-standardize-encryption-algorithms-can-resist-attack-quantum-computers (дата звернення: 16.05.2025).

17. Encryption: It's Not About Good and Bad Guys, It's About All of Us [Електронний ресурс] // Center for European Policy Analysis (CEPA). – Режим доступу: https://cepa.org/comprehensive-reports/encryption-its-not-about-good-and-bad-guys-its-about-all-of-us (дата звернення: 16.05.2025).

18. How ADC and DAC Converters Work: Everything You Need to Know – [Електронний ресурс] // Режим доступу: https://en.hwlibre.com/How-ADC-and-DAC-converters-work%3A-everything-you-need-to-know/ (дата звернення: 18.05.2025).

19. Advanced Encryption Standard [Електронний ресурс] // Wikipedia. – Режим доступу: https://uk.wikipedia.org/wiki/Advanced_Encryption_Standard (дата звернення: 18.05.2025).

20. Advanced Encryption Standard [Електронний ресурс] // TechTarget – Режим доступу: https://www.techtarget.com/searchsecurity/definition/Advanced-Encryption-Standard (дата звернення: 18.05.2025).

21. Arduino IDE [Електронний ресурс] // Arduino Режим доступу: https://www.arduino.cc/en/software/ (дата звернення: 18.04.2025).

22. UNO R3 [Електронний ресурс] // Arduino Режим доступу: https://docs.arduino.cc/hardware/uno-rev3/ (дата звернення: 20.04.2025).

Додаток А – Вихідний код

```
#include <AESLib.h>

#define TRIG_PIN 9
#define ECHO_PIN 10
#define PWM_OUT 6

AESLib aesLib;

byte aes_key[16] = {0x01, 0x02, 0x03, 0x04, 0x05, 0x06, 0x07, 0x08, 0x09,
0x0A, 0x0B, 0x0C, 0x0D, 0x0E, 0x0F, 0x10};

void setup() {
    pinMode(TRIG_PIN, OUTPUT);
    pinMode(ECHO_PIN, INPUT);
    pinMode(PWM_OUT, OUTPUT);
    Serial.begin(9600);
}

void loop() {
    digitalWrite(TRIG_PIN, LOW);
    delayMicroseconds(2);
    digitalWrite(TRIG_PIN, HIGH);
    delayMicroseconds(10);
    digitalWrite(TRIG_PIN, LOW);

    long duration = pulseIn(ECHO_PIN, HIGH);
    int distance = duration * 0.034 / 2;

    byte plaintext[16] = {distance, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0};
    byte ciphertext[16];

    aesLib.encryptBlock(ciphertext, plaintext, aes_key);

    int pwmValue = ciphertext[0] % 256;
    pwmValue = constrain(pwmValue, 0, 255);

    analogWrite(PWM_OUT, pwmValue + random(-10, 10));

    Serial.print("Encrypted PWM Value: ");
    Serial.println(pwmValue);
    delay(100);
}
```

Додаток Б – Таблиці

Таблиця 2.3.1 - Основні принципи цифрового та аналогового шифрування

Критерій	Аналогове шифрування	Цифрове шифрування
Принцип роботи	Змінює параметри аналогового сигналу (амплітуда, частота, фаза) для його маскування.	Використовує математичні алгоритми для перетворення даних у закодовану форму.
Тип даних	Голос, радіосигнали, відео, аналогові імпульси.	Текст, файли, цифровий голос, цифрове відео.
Стійкість до злому	Менш стійке, оскільки залежить від приховування сигналу.	Висока стійкість при використанні сучасних алгоритмів.
Спосіб передачі	Використовує аналогові носії: радіохвилі, телефонні лінії.	Використовує цифрові мережі: інтернет, мобільний зв’язок.
Перешкодостійкість	Вразливе до шумів та природних спотворень сигналу.	Менш чутливе до шумів, оскільки працює з дискретними даними.
Гнучкість	Важко адаптується до змін, вимагає фізичних змін у пристроях.	Легко оновлюється шляхом зміни алгоритмів або програмного забезпечення.
Приклади	Фазова модуляція (PSK), амплітудна модуляція (AM), шумове маскування.	AES, RSA, ECC, DES, цифрові підписи.

Таблиця 3.1.1.1 – Перетворення в наслідок частотного скремблювання

Частота (Гц)	Вихідний сигнал	Скрембльований сигнал
300	+	-
1000	+	+
5000	-	+

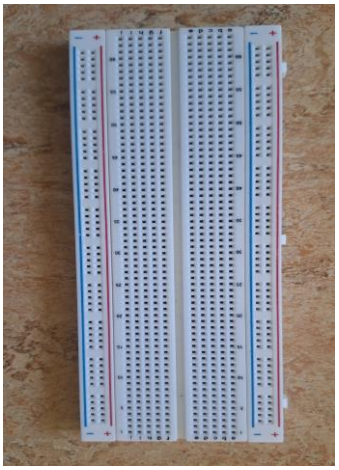
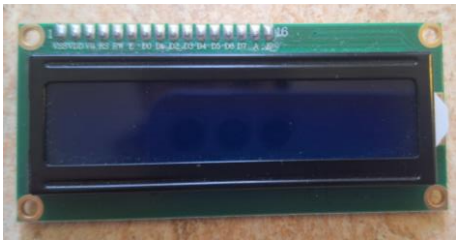
Таблиця 3.1.2.1 – Аналіз аналогових методів

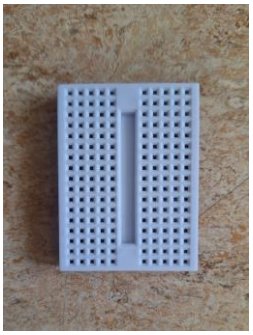
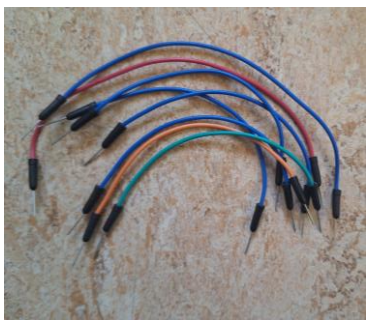
Метод	Стійкість до перехоплення	Стійкість до аналізу	Складність реалізації	Вразливість до шуму	Застосування
Скремблювання	Середня	Низька	Низька	Висока	Телефонія, радіозв’язок
Аналогове спектральне розсіювання	Висока	Висока	Дуже висока	Низька	Військові та супутникові комунікації
Маскування сигналу шумом	Висока	Висока	Висока	Висока	Захищений урядовий зв’язок

Таблиця 3.2.2.1 – Аналіз цифрових методів

Метод	Стійкість до атак	Швидкість	Основні обмеження	Основне застосування
Симетричне (AES)	Висока	Дуже висока	Проблема безпечного обміну ключами	Захист великих обсягів даних
Асиметричне (RSA)	Висока	Низька	Високі обчислювальні витрати	Цифрові підписи, обмін ключами
Асиметричне (ECC)	Висока	Помірна	Залежність від реалізації алгоритму	Мобільні пристрої, IoT
Гібридне (TLS, PGP)	Дуже висока	Висока	Складність впровадження	Захист інтернет-з'єднань, електронна пошта

Таблиця 4.1.1 - Опис застосованої техники

Назва компоненту	Зображення компоненту	Призначення
USB-кабель для підключення до комп'ютера		Підключення мікроконтролера (Arduino) до комп'ютера для завантаження скетчів (програм) та живлення [22].
Макетна плата (breadboard) на 830 точок		Безпайкове збирання електронних схем.
LCD-дисплей 1602		Виведення текстової інформації — значення з датчиків, повідомлення тощо.
Потенціометр 10 кОм		Регулювання рівня напруги (наприклад, для налаштування контрасту дисплея або введення значення) [22].

Макетна плата (breadboard) на 120 точок		Мініатюрна безпайкова плата для невеликих схем або модулів.
Ультразвуковий далекомір HC-SR04		Вимірювання відстані до об’єктів за допомогою ультразвуку.
Плата Elegoo Uno R3 (аналог Arduino Uno)		Центральна частина проєкту — мікроконтролер на базі ATmega328P [22].
Проводи-перемички (Dupont) типу "male–male"		З’єднання компонентів між собою або з макетною платою.