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: «Вивчення та відбір шрифтів для застосування у аналоговому методі криптографічного перетворення даних»

оцінка « _____ »

Голова ЕК

Мичуда Л.З.

Керівник: к.т.н. Громико І. О.

Рецензент: к.т.н. Шостак А.В.

Виконавець: студентка групи КБ-42

Боклаг Д. М.

Харків 2025

РЕФЕРАТ

Пояснювальна записка містить 60 сторінок, 12 рисунків, 2 таблиці, 1 додаток, 24 джерела.

Метою дипломної роботи є вивчення та відбір шрифтів для їх застосування в аналогових методах криптографічного перетворення даних. Це передбачає аналіз властивостей різних шрифтів, їх придатність для криптографічних цілей та розробку рекомендацій щодо їх ефективного використання.

Об’єктом дослідження дипломної роботи є графічні характеристики шрифтів як інструмент візуального (аналогового) криптографічного перетворення даних.

Предметом дослідження виступають шрифти та їх характеристики, які можуть впливати на ефективність і надійність аналогових криптографічних методів.

Методи дослідження включають аналіз існуючих аналогових методів криптографії з використанням шрифтів, вивчення впливу властивостей шрифтів на процес шифрування, відбір оптимальних шрифтів для практичного застосування та формування рекомендацій щодо їх впровадження в системи захисту інформації.

Результатами проведеної роботи є визначення перспектив розвитку впровадження шрифтів у криптографічний метод захисту інформації.

Проведене дослідження сприятиме підвищенню рівня захищеності інформації.

Ключові слова: ШРИФТ, АНАЛОГОВИЙ МЕТОД КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ, ЗАХИЩЕНІСТЬ ІНФОРМАЦІЇ, КРИПТОГРАФІЧНА СИСТЕМА, АДАПТАЦІЯ, АНАЛІЗ, ЦИФРОВЕ ШИФРУВАННЯ, АНАЛОГОВЕ ШИФРУВАННЯ, ТЕСТУВАННЯ, МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ, ГРАФІЧНА СТІЙКІСТЬ.

ABSTRACT

The explanatory note contains 60 pages, 12 figures, 2 tables, 1 annexes, 24 sources.

The purpose of the thesis is to study and select fonts for their application in analog methods of cryptographic data transformation. This involves analyzing the properties of different fonts, their suitability for cryptographic purposes and developing recommendations for their effective use.

The object of the study of the thesis is the graphic characteristics of fonts as a tool for visual (analog) cryptographic data transformation.

The subject of research are fonts and their characteristics, which can affect the efficiency and reliability of analog cryptographic methods.

Research methods include analyzing existing analog cryptography methods using fonts, studying the effect of font properties on the encryption process, selecting optimal fonts for practical application and forming recommendations for their implementation in information protection systems.

The results of the work carried out determine the prospects for the development of cryptographic systems.

The study will improve the level of information security.

Keywords: FONT, ANALOG CRYPTOGRAPHIC CONVERSION METHOD, INFORMATION SECURITY, CRYPTOGRAPHIC SYSTEM, ADAPTATION, ANALYSIS, DIGITAL ENCRYPTION, ANALOG ENCRYPTION, TESTING, SUITABILITY CRITERIA, INFORMATION PROTECTION METHODS, GRAPHICAL STABILITY.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СКОРОЧЕНЬ ТА СИМВОЛІВ

AES - Advanced Encryption Standard - симетричний блочний шифр, який використовується для шифрування даних у багатьох системах, включаючи операційні системи та програми шифрування даних.

RSA - Rivest–Shamir–Adleman - асиметричний криптографічний алгоритм, який використовується для шифрування та підпису даних. RSA використовується у багатьох системах, включаючи електронну пошту та онлайн-банкінг.

ECC - Elliptic Curve Cryptography – асиметричний криптографічний алгоритм, базується на математиці еліптичних кривих над скінченними полями. Використовується в електронних підписах, шифруванні каналів, аутентифікації.

PKI - Public Key Infrastructure – інфраструктура відкритих ключів. Сукупність апаратних, програмних та процедурних компонентів, які забезпечують створення, управління, розповсюдження, використання та відкликання цифрових сертифікатів і криптографічних ключів.

HSM - Hardware Security Model – апаратний модуль безпеки. Призначений для захищеного зберігання та використання криптографічних ключів.

KMS - Key Management System - служба управління ключами.

PCI DSS - Payment Card Industry Data Security Standart – стандарт безпеки даних індустрії платіжних карток.

GDPR - General Data Protection Regulation - загальний регламент захисту даних.

ISO - International Organization for Standardization – Міжнародна організація зі стандартизації.

NIST - National Institute of Standards and Technology (USA).

OCR - Optical Character Recognition – оптичне розпізнавання символів.

QKD - Quantum Key Distribuion – квантове розподілення ключів.

VPN - Virtual Private Network – віртуальна приватна мережа.

IoT - Internet of Things – Інтернет речей. Мережа фізичних пристроїв, які мають підключення до Інтернету і можуть обмінюватися даними.

ML - Machine Learning – машинне навчання.

ВСТУП

У сучасному світі безпека інформації набуває все більшої важливості, оскільки обсяги даних невпинно зростають, а методи їх несанкціонованого доступу стають дедалі складнішими. Хоча цифрові методи криптографії домінують у сфері інформаційної безпеки, аналогові методи залишаються актуальними, особливо в контексті фізичного збереження даних та офлайн-комунікацій. Використання шрифтів як засобу криптографічного перетворення даних відкриває нові можливості для приховування інформації та її захисту від несанкціонованого доступу.

Актуальність цього дослідження обумовлена необхідністю розробки нових методів захисту інформації, які можуть бути застосовані в умовах, де цифрові засоби є недоступними або ненадійними. Аналогові методи, зокрема використання шрифтів, дозволяють створювати додаткові шари безпеки та підвищувати стійкість систем до різних видів атак.

Метою даного дослідження є вивчення та відбір шрифтів для їх застосування в аналогових методах криптографічного перетворення даних. Це передбачає аналіз властивостей різних шрифтів, їх придатність для криптографічних цілей та розробку рекомендацій щодо їх ефективного використання.

Предметом дослідження виступають шрифти та їх характеристики, які можуть впливати на ефективність і надійність аналогових криптографічних методів. Завданнями є аналіз існуючих аналогових методів криптографії з використанням шрифтів, вивчення впливу властивостей шрифтів на процес шифрування, відбір оптимальних шрифтів для практичного застосування та формування рекомендацій щодо їх впровадження в системи захисту інформації.

Проведене дослідження сприятиме підвищенню рівня захищеності інформації в умовах обмеженого використання цифрових технологій та розширить можливості застосування аналогових методів криптографії в сучасних інформаційних системах.

1 ТЕОРЕТИЧНІ ОСНОВИ КРИПТОГРАФІЧНОГО ШИФРУВАННЯ

1.1 Аналіз технічних вимог до цифрового шифрування

Безпека та криптографічна стійкість є фундаментальними аспектами в аналізі технічних вимог до цифрового шифрування. Сучасні криптографічні алгоритми повинні забезпечувати надійний захист інформації від несанкціонованого доступу та протистояти різноманітним типам криптоаналітичних атак [1]. Це включає стійкість до атак грубої сили, статистичних методів, диференційного та лінійного криптоаналізу.

Одним із ключових параметрів криптографічної стійкості є довжина та якість ключів шифрування. Зі зростанням обчислювальних потужностей необхідно збільшувати розміри ключів для забезпечення належного рівня безпеки. Наприклад, для симетричних алгоритмів, таких як AES (Advanced Encryption Standard), рекомендується використовувати ключі довжиною 256 біт [2]. Для асиметричних алгоритмів, таких як RSA або ECC (Elliptic Curve Cryptography), довжина ключа повинна відповідати сучасним стандартам та враховувати потенційні квантові атаки [3].

Важливим аспектом є також стійкість до атак на основі побічних каналів, які використовують фізичні властивості системи, такі як споживана потужність або електромагнітне випромінювання, для отримання секретної інформації [4]. Захист від таких атак вимагає спеціальних методів реалізації та додаткових заходів безпеки.

Розвиток квантових обчислень ставить під загрозу безпеку традиційних криптографічних алгоритмів. Тому все більшої актуальності набувають постквантові криптографічні алгоритми, які повинні бути стійкими до атак з використанням квантових комп'ютерів [5]. Стандартизація та впровадження таких алгоритмів є важливим напрямком сучасних досліджень у сфері криптографії.

Крім вибору надійних алгоритмів, критичним є їх правильна реалізація. Помилки в реалізації можуть призвести до вразливостей, які компрометують

всю систему, незалежно від теоретичної стійкості алгоритму [6]. Тому необхідно дотримуватися найкращих практик програмування, використовувати перевірені бібліотеки та регулярно проводити аудит безпеки.

Загалом, забезпечення безпеки та криптографічної стійкості вимагає комплексного підходу, що включає використання сучасних та перевірених алгоритмів, належну довжину ключів, захист від фізичних атак, підготовку до квантових загроз та безпечну реалізацію криптографічних протоколів.

Управління криптографічними ключами є критичним аспектом забезпечення безпеки інформаційних систем, оскільки ефективність криптографічних алгоритмів значною мірою залежить від надійності зберігання та розповсюдження ключів. Відсутність належного управління ключами може призвести до компрометації системи, навіть якщо використовуються сильні алгоритми шифрування [7]. У сучасних умовах, коли обсяги передаваних та збережуваних даних постійно зростають, а кіберзагрози стають все більш складними, управління ключами набуває особливої актуальності.

Основні завдання управління криптографічними ключами включають генерацію ключів, їх безпечне зберігання, розповсюдження між автентифікованими сторонами, регулярну ротацію та своєчасне відкликання. Генерація ключів повинна здійснюватися з використанням надійних генераторів випадкових чисел, які забезпечують необхідний рівень ентропії та унеможливлюють передбачення ключів потенційними зловмисниками [8]. Безпечне зберігання ключів передбачає використання захищених апаратних чи програмних засобів, що перешкоджають несанкціонованому доступу та ексфільтрації ключової інформації.

Розповсюдження ключів між учасниками комунікації є одним з найбільш вразливих етапів, оскільки можливість перехоплення чи підміни ключа зловмисником може призвести до повного компрометації даних. Для вирішення цієї проблеми використовуються протоколи обміну ключами, такі як протокол Діффі — Геллмана, що забезпечує безпечне встановлення спільного секрету через відкритий канал [9]. Крім того, важливим є автентифікація сторін перед

обміном ключами, що може бути реалізовано за допомогою цифрових сертифікатів та інфраструктури відкритих ключів (PKI).

Регулярна ротація ключів є необхідною для зниження ризику компрометації, оскільки з часом можливість розкриття ключа збільшується. Політика ротації повинна визначати інтервали зміни ключів та процедури оновлення, що не порушують безперервність роботи системи [10]. Відкликання ключів здійснюється у випадку підозри чи підтвердження їх компрометації, а також при зміні прав доступу користувачів. Процес відкликання повинен бути оперативним та доводитися до всіх зацікавлених сторін.

Сучасні технології управління ключами включають використання апаратних модулів безпеки (HSM), які забезпечують фізичний захист ключів та виконання криптографічних операцій в ізольованому середовищі [11]. Хмарні сервіси управління ключами (KMS) надають можливість централізованого управління ключами в масштабованих системах з розподіленою архітектурою, забезпечуючи при цьому високий рівень безпеки та відповідність нормативним вимогам [12].

Крім технічних аспектів, управління криптографічними ключами вимагає розробки та впровадження організаційних політик та процедур, які регламентують всі етапи життєвого циклу ключів. Це включає призначення відповідальних осіб, визначення ролей та повноважень, документування процесів та регулярний аудит системи управління ключами [13]. Відповідність законодавчим та регуляторним вимогам, таким як стандарти безпеки даних у платіжній індустрії (PCI DSS) або Загальний регламент захисту даних (GDPR), є обов'язковою для організацій, що обробляють чутливу інформацію.

Таким чином, управління криптографічними ключами є комплексною задачею, що поєднує технічні, організаційні та нормативні аспекти. Ефективне вирішення цієї задачі є необхідною умовою забезпечення цілісності, конфіденційності та доступності інформації в сучасних інформаційних системах.

Продуктивність та ефективність криптографічних алгоритмів є критичними аспектами при розробці безпечних та високопродуктивних інформаційних систем. Під продуктивністю будемо розуміти показник швидкості роботи алгоритму, тобто кількість даних, які він може обробити за одиницю часу. Ефективність у свою чергу це співвідношення захисту, о надається, до ресурсів, що витрачаються (час, пам’ять, енергія, фінанси). У сучасних умовах стрімкого зростання обсягів даних та вимог до швидкодії, оптимізація криптографічних засобів стає необхідністю [14]. Висока продуктивність дозволяє забезпечити швидке шифрування та дешифрування інформації без значних затримок, що особливо важливо для систем реального часу та додатків з високою пропускною здатністю.

Симетричні алгоритми шифрування, такі як AES (Advanced Encryption Standard), відзначаються високою швидкістю та ефективністю обробки даних. Завдяки можливості апаратної реалізації та оптимізації під сучасні процесори, вони забезпечують мінімальні витрати ресурсів при високому рівні безпеки [14]. Це робить їх придатними для широкого спектру застосувань, від захисту даних у хмарних сервісах до мобільних додатків.

Асиметричні алгоритми, зокрема RSA та алгоритми на основі еліптичних кривих, зазвичай вимагають більше обчислювальних ресурсів і є повільнішими порівняно з симетричними [14]. Однак вони є незамінними для задач управління ключами та цифрового підпису. Оптимізація їх продуктивності часто досягається через використання спеціалізованих математичних методів та апаратних прискорювачів.

Енергетична ефективність є ще одним важливим фактором, особливо для мобільних та вбудованих систем з обмеженими ресурсами. Використання алгоритмів з низьким енергоспоживанням, тобто алгоритмів, які використовують мало енергії у процесі своєї роботи, дозволяє продовжити час автономної роботи пристроїв та знизити загальні витрати енергії [14].

Це досягається через оптимізацію алгоритмів та використання енергоефективних компонентів.

Алгоритми розглядаються як перспективні кандидати для заміни існуючих методів, проте їх продуктивність поки що є предметом активного вивчення [14].

Таким чином, при виборі криптографічних засобів необхідно враховувати не лише їх безпеку, але й продуктивність та ефективність. Баланс між цими характеристиками забезпечує оптимальне функціонування інформаційних систем та задовольняє вимоги сучасних користувачів щодо швидкості та надійності.

Сумісність та стандартизація відіграють ключову роль у забезпеченні ефективності та надійності систем цифрового шифрування. Важливим аспектом є забезпечення відповідності нормативним вимогам та правовим актам, які часто посилаються на міжнародні стандарти криптографії, такі як ті, що розробляються Міжнародною організацією зі стандартизації (ISO) або Національним інститутом стандартів і технологій (NIST).

Стандартизація полегшує навчання та сертифікацію фахівців у сфері інформаційної безпеки, оскільки наявність чітких стандартів дозволяє створювати уніфіковані навчальні програми та критерії оцінки знань.

Отже, сумісність та стандартизація є фундаментальними аспектами технічних вимог до цифрового шифрування.

Масштабованість та гнучкість є критичними аспектами при розробці та впровадженні систем цифрового шифрування, оскільки вони визначають здатність таких систем адаптуватися до зростаючих обсягів даних та змінних вимог безпеки. Це особливо важливо в умовах стрімкого розвитку цифрових технологій та інтернету речей, де обсяги передаваних та зберіганих даних постійно зростають.

Гнучкість системи шифрування визначається її здатністю адаптуватися до нових вимог безпеки, інтегруватися з різними платформами та підтримувати різноманітні алгоритми шифрування

Масштабованість та гнучкість сприяють довгостроковій стійкості системи шифрування, оскільки дозволяють їй ефективно реагувати на

технологічні зміни та нові вимоги ринку. Таким чином, забезпечення високої масштабованості та гнучкості є невід'ємною частиною розробки надійних та довговічних рішень у сфері цифрового шифрування.

На практиці досягнення високого рівня масштабованості та гнучкості може бути реалізовано через використання модульної архітектури, яка дозволяє легко додавати нові компоненти або замінювати існуючі без порушення функціональності системи.

Таким чином, масштабованість та гнучкість є ключовими факторами, що визначають ефективність та довговічність систем цифрового шифрування.

1.2 Дослідження технічних вимог до аналогового шифрування

На відміну від цифрової криптографії, де дані передаються у вигляді дискретних бітів, аналогова криптографія оперує безперервними параметрами: формами, кольором, розмірами, частотами або геометрією. Тут інформація може бути втілена у графічному зображенні, сигналі чи навіть фізичному об’єкті [15].

У контексті аналогового шифрування, забезпечення високого рівня безпеки передбачає не лише застосування надійних криптографічних принципів, але й адаптацію цих принципів до специфіки аналогових систем, які часто характеризуються іншими механізмами обробки та передачі інформації порівняно з цифровими аналогами. Одним із цікавих напрямків є використання шрифтів як засобу криптографічного перетворення, що відкриває нові можливості для приховування та захисту інформації.

Аналогові методи криптографії, на відміну від цифрових, можуть використовувати фізичні властивості носіїв інформації, такі як форми та структури шрифтів, для здійснення шифрування [16].

Вибір та відбір шрифтів для криптографічного перетворення повинні враховувати кілька ключових факторів, що впливають на безпеку системи.

По-перше, шрифти повинні мати достатню кількість варіантів та варіацій, що ускладнює прогнозування або відтворення шаблонів шифрування.

По-друге, необхідно забезпечити, щоб фізичні зміни у шрифтах були непомітними для сторонніх спостерігачів, тим самим приховуючи факт шифрування.

Криптографічна стійкість аналогових методів шифрування також залежить від їх здатності протистояти різним типам атак, включаючи статистичні аналізи, аналіз спектральних характеристик та інші форми криптоаналізу, специфічні для аналогових систем [16]. Вибір шрифтів зі складною та непередбачуваною структурою допомагає ускладнити такі атаки, підвищуючи рівень стійкості системи. Крім того, важливим аспектом є забезпечення того, щоб методи зміни шрифтів не призводили до створення слабких місць у системі, які могли б бути використані для зламу.

Аналогові системи шифрування, що використовують шрифти, також повинні враховувати можливість випадкових помилок або шумів, які можуть виникнути під час фізичної передачі або зберігання інформації. Таким чином, забезпечення криптографічної стійкості в аналогових методах шифрування вимагає інтеграції криптографічних принципів з фізичними характеристиками носіїв інформації, таких як шрифти.

В сучасних умовах, коли цифрові методи шифрування продовжують розвиватися та удосконалюватися, аналогові методи залишаються важливим додатковим засобом захисту інформації, особливо у специфічних сферах застосування, де цифрові технології можуть бути недоступними або ненадійними [16].

Управління криптографічними ключами є однією з ключових складових забезпечення безпеки інформаційних систем, незалежно від того, чи йдеться про цифрові чи аналогові методи шифрування. У контексті аналогового шифрування управління ключами набуває особливої важливості через специфіку самих методів перетворення даних, які часто базуються на фізичних характеристиках носіїв інформації або механічних процесах.

Одним із основних аспектів управління ключами в аналогових системах є їх генерація.

На відміну від цифрових методів, де ключі зазвичай представляють собою послідовність бітів, аналогові ключі можуть бути реалізовані через фізичні параметри, такі як частота, фаза, амплітуда або інші властивості сигналів. Це означає, що генерація ключів повинна забезпечувати високу ступінь випадковості та унікальності кожного ключа, щоб ускладнити їх відтворення або передбачення з боку потенційних зловмисників [16]. Використання спеціалізованих генераторів випадкових сигналів або шумових генераторів, може значно підвищити стійкість ключів до криптоаналітичних атак.

Розподіл ключів в аналогових системах також має свої особливості. Оскільки аналогові ключі часто передаються або використовуються у фізичній формі, необхідно забезпечити їх захищений канал передачі та унеможливити несанкціонований доступ під час обміну. Це може включати використання фізичних засобів захисту, таких як спеціальні кабелі, оптичні засоби передачі або навіть механічні пристрої для передачі ключів без електронної обробки. Важливо розробити протоколи для безпечного обміну ключами між сторонами, що мінімізують ризики їх перехоплення або модифікації.

Зберігання ключів в аналогових системах також потребує особливої уваги. Ключі повинні бути захищені від фізичного доступу та пошкоджень, що може вимагати використання спеціальних засобів захисту, таких як сейфи, шифрувальні коробки або інші фізичні бар'єри.

Ротація ключів є ще одним критичним аспектом управління криптографічними ключами в аналогових системах. Періодична зміна ключів допомагає знизити ризик їх компрометації та обмежити потенційні збитки від можливих атак. У аналогових системах ротація ключів може бути складнішою через необхідність фізичної заміни або переналаштування обладнання. Це може включати використання динамічних систем генерації ключів або автоматизованих процесів заміни ключів, які мінімізують людський фактор і скорочують час на зміну ключів.

Також важливо впровадити процедури перевірки ключів перед їх використанням у процесі шифрування, щоб виявити будь-які спроби несанкціонованих змін або підробок.

Таким чином, управління криптографічними ключами в аналогових методах шифрування є складним та багатогранним процесом, який вимагає врахування як фізичних, так і логічних аспектів безпеки.

Продуктивність та ефективність є важливими аспектами при розробці та впровадженні аналогових методів шифрування, оскільки вони визначають здатність системи забезпечувати необхідний рівень захисту інформації при оптимальному використанні ресурсів [17].

На відміну від цифрових систем, де продуктивність часто оцінюється через обчислювальну потужність та швидкість обробки даних, аналогові методи шифрування потребують окремого підходу до аналізу цих характеристик, враховуючи фізичні властивості та обмеження аналогових пристроїв.

Одним із основних факторів, що впливають на продуктивність аналогових систем шифрування, є швидкість обробки сигналів [17]. Аналогові методи зазвичай працюють у режимі безперервного сигналу, що дозволяє досягати високих швидкостей передачі та обробки даних у реальному часі.

Ефективність аналогових методів шифрування також залежить від енергоспоживання та використання ресурсів. У порівнянні з цифровими системами, аналогові пристрої можуть бути більш енергоефективними. По-перше, вони не потребують інтенсивних обчислень, по-друге, можуть реалізовуватися через пасивні або малопотужні пристрої (напр. оптичні фільтри, механічні об’єктиви).

Важливим аспектом є також розмір та вартість обладнання, що використовується для аналогового шифрування. Компактність та доступність компонентів впливають на загальну ефективність системи, особливо в умовах обмежених ресурсів або мобільних застосувань.

Крім того, ефективність аналогових методів шифрування може бути оцінена через їх здатність до інтеграції з існуючими системами та технологіями. Аналогові методи часто легше інтегрувати в традиційні комунікаційні мережі, які вже працюють з аналоговими сигналами, що знижує необхідність у складних конвертаціях та перетвореннях. Це сприяє збереженню продуктивності системи та зменшенню затримок у передачі даних. Однак, інтеграція з цифровими системами може вимагати додаткових ресурсів для перетворення сигналів, що може вплинути на загальну ефективність.

Важливим аспектом продуктивності є також адаптивність аналогових методів до різних умов експлуатації та змінних вимог до безпеки [17].

Аналогові системи можуть бути менш гнучкими у порівнянні з цифровими, оскільки зміна параметрів шифрування часто вимагає фізичних модифікацій або переналаштувань обладнання.

Загалом, продуктивність та ефективність аналогових методів шифрування є багатогранними характеристиками, які залежать від взаємодії численних факторів, включаючи швидкість обробки, енергоспоживання, інтеграцію з існуючими системами та адаптивність до змінних умов.

Важливим аспектом є забезпечення сумісності між новими аналоговими методами шифрування та існуючими цифровими системами, що може вимагати розробки спеціалізованих інтерфейсів або адаптерів.

Крім того, стандартизація сприяє підвищенню довіри користувачів до аналогових методів шифрування, оскільки наявність чітких та перевірених стандартів гарантує відповідність систем встановленим вимогам безпеки та надійності.

Узгодження аналогових методів шифрування з існуючими стандартами безпеки дозволяє також інтегрувати їх у багатошарові системи захисту, де аналогові та цифрові методи взаємодоповнюють один одного, забезпечуючи більш високий рівень захисту даних.

Масштабованість та гнучкість є ключовими аспектами при розробці та впровадженні аналогових методів шифрування [15], оскільки вони визначають

здатність системи адаптуватися до зростаючих вимог та змінних умов експлуатації.

Гнучкість аналогових методів шифрування стосується здатності системи адаптуватися до різноманітних вимог та умов експлуатації, включаючи зміни в архітектурі системи, алгоритмах шифрування та середовищі їх застосування. Крім того, гнучкість передбачає здатність системи інтегрувати нові технології та методи шифрування, що дозволяє підвищувати рівень безпеки та ефективності захисту даних без значних витрат часу та ресурсів.

Інтеграція масштабованості та гнучкості в аналогові методи шифрування вимагає комплексного підходу до проектування системи, що включає використання модульної архітектури, підтримку стандартів відкритого інтерфейсу та забезпечення високої ступені автоматизації процесів управління системою. Використання програмно-апаратних засобів, які дозволяють динамічно змінювати конфігурацію системи, сприяє підвищенню її гнучкості та масштабованості, забезпечуючи можливість швидкого реагування на змінні умови експлуатації та вимоги безпеки.

Таким чином, забезпечення високої масштабованості та гнучкості аналогових методів шифрування є критично важливим для їх успішного застосування в сучасних інформаційних системах. Це дозволяє не лише ефективно захищати зростаючі обсяги даних, але й швидко адаптуватися до нових викликів та змінних умов, забезпечуючи стабільну та надійну роботу системи шифрування у довгостроковій перспективі.

1.3 Порівняння цифрових та аналогових методів шифрування

Цифрові методи шифрування традиційно домінують у сучасних інформаційних системах завдяки їхній здатності обробляти великі обсяги даних з високою швидкістю та інтегруватися з цифровою інфраструктурою. Вони використовують дискретні дані та алгоритми, які забезпечують високий рівень безпеки через складність математичних операцій та криптографічних ключів. Цифрові алгоритми, такі як AES або RSA [17], широко використовуються в різних сферах, від захисту особистих даних до забезпечення безпеки

комунікацій у державних та комерційних структурах. Їхня ефективність забезпечується високою ступенем автоматизації та можливістю швидкого оновлення та вдосконалення алгоритмів у відповідь на нові загрози та вразливості.

Аналогові методи шифрування, хоча й менш поширені в сучасних цифрових системах, мають свої специфічні переваги, особливо в контексті фізичного захисту даних та умов, де цифрові засоби можуть бути недоступними або ненадійними. Аналогові методи використовують неперервні сигнали для перетворення інформації, що дозволяє створювати додаткові шари безпеки через фізичні властивості сигналів, такі як амплітуда, частота та фаза. Це може забезпечити високий рівень стійкості до деяких типів атак, особливо тих, що спрямовані на цифрові системи, таких як атаки грубої сили або криптоаналітичні методи. Крім того, аналогові системи можуть бути менш вразливими до електронних загроз, таких як перехоплення або підслуховування, оскільки вони можуть використовувати фізичні засоби захисту, які важко реалізувати в цифрових системах.

Однак, аналізуючи ці два підходи, слід враховувати ряд суттєвих відмінностей, які впливають на їхню ефективність та застосовність. Цифрові методи шифрування забезпечують високу ступінь автоматизації та інтеграції з існуючими цифровими системами, що робить їх незамінними в сучасних інформаційних технологіях. Вони дозволяють легко масштабувати системи безпеки та адаптувати їх до різних вимог, забезпечуючи при цьому високу швидкість обробки даних та ефективність використання ресурсів. Аналогові методи, хоча й мають свої переваги у специфічних умовах, часто стикаються з викликами, пов'язаними з точністю та стабільністю сигналів, а також складністю інтеграції з цифровими системами. Крім того, аналогові системи можуть вимагати більш складного апаратного забезпечення та фізичних засобів захисту, що може збільшувати їхню вартість та ускладнювати процес впровадження.

З точки зору безпеки, цифрові методи шифрування забезпечують високий рівень захисту через складність математичних алгоритмів та можливість регулярного оновлення криптографічних ключів [16]. Вони дозволяють ефективно захищати дані від різних видів атак, включаючи ті, що використовують сучасні обчислювальні потужності. Аналогові методи, хоча й можуть забезпечувати додаткові шари безпеки через фізичні характеристики сигналів, часто залежать від точності та стабільності апаратного забезпечення, що може бути вразливим до фізичних атак або експлуатації апаратних помилок. Таким чином, цифрові методи шифрування, завдяки своїй гнучкості та високій ступені автоматизації, залишаються більш універсальними та надійними для широкого спектру застосувань, тоді як аналогові методи можуть бути корисними у спеціалізованих ситуаціях, де необхідно забезпечити фізичний захист даних або працювати в умовах, де цифрові системи є ненадійними.

У підсумку, порівняння цифрових та аналогових методів шифрування демонструє, що обидва підходи мають свої переваги та обмеження, які визначають їхню придатність для конкретних завдань та умов експлуатації. Цифрові методи шифрування, завдяки своїй високій продуктивності, гнучкості та можливості інтеграції з сучасними інформаційними системами, залишаються основним вибором для забезпечення безпеки даних у більшості сучасних застосувань. Проте, аналогові методи шифрування можуть забезпечити додаткові рівні захисту та бути корисними у спеціалізованих ситуаціях, де цифрові методи можуть бути недостатніми або ненадійними. Таким чином, оптимальне використання обох підходів може забезпечити більш комплексний та стійкий захист інформації, враховуючи різноманітні вимоги та загрози сучасного інформаційного середовища.

2 ПІДБІР ТА ТЕСТУВАННЯ ШРИФТІВ ДЛЯ АНАЛОГОВОГО ШИФРУВАННЯ

2.1 Визначення критеріїв придатності шрифтів для аналогового криптографічного перетворення

У межах завдання дослідження та відбору шрифтів для використання в аналоговому методі криптографічного перетворення даних слід сформувати чіткі критерії їхньої придатності, орієнтуючись на специфіку цього підходу до шифрування. Основна ідея аналогового методу полягає у представленні символів як елементів, що можуть бути графічно трансформовані без втрати їхньої розпізнаваності, при цьому забезпечуючи достатній рівень складності для криптографічного захисту. Цей підхід вимагає ретельного аналізу характеристик шрифтів для забезпечення їхньої функціональності в умовах трансформації та дешифрування.

Першочерговим критерієм є графічна стійкість шрифтів до трансформацій. [18] У процесі криптографічного перетворення символи можуть зазнавати різноманітних змін, таких як масштабування, повороти, спотворення або сегментація. У зв'язку з цим шрифти повинні зберігати базову форму символів незалежно від типу застосованої трансформації. Наприклад, при зміні масштабу або розтягуванні окремих елементів символ має залишатися зрозумілим для розшифрування. На рисунку 2.1 демонструється процес трансформації символу, де наведено початковий вигляд, масштабований зі зміною кольору і результат з повною деформацією (зміна розміру, кольору, прозорості, поворот символу та розтягнення).

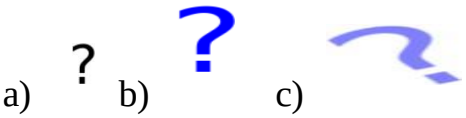

Рисунок 2.1 – Зміна масштабу символу (a – початковий; b – зміна кольору і розміру; c – повна деформація)

Другим важливим критерієм є розбірливість символів у складних графічних композиціях. Аналоговий метод шифрування передбачає можливість використання накладання або комбінування символів для створення складних графічних патернів. [18] Це означає, що символи мають бути достатньо унікальними, щоб їх можна було виділити серед інших елементів навіть у випадках часткового перекриття. Наприклад, у випадку взаємного накладання символів на рисунку 2.2 показано, як шрифти з проміжками різної відстані між елементами демонструють наявність можливості коректного розпізнавання кожного символу.

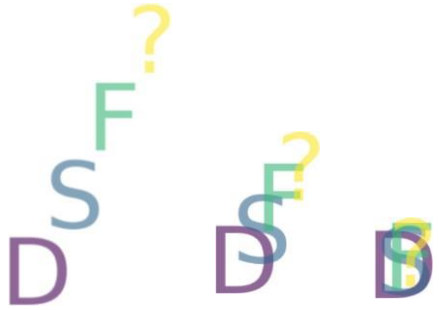

Рисунок 2.2 – Комбінування символів для створення патернів

Третій критерій пов'язаний із варіативністю застосування шрифтів. Вони повинні підтримувати модифікації, зокрема зміни кута нахилу, варіації товщини ліній, або навіть часткову заміну окремих елементів. Це дає можливість збільшити складність криптографічного перетворення, залишаючи базову структуру символу незмінною. Наприклад, на рисунку 2.3 наведено приклади варіацій одного і того ж символу, що дозволяють адаптувати його для різних умов шифрування.

Рисунок 2.3 – Приклади варіацій символу

Враховуючи найпоширеніші види модифікацій символів, демонструю наглядний радарний графік для показу варіативності одночасно за кількома параметрами (рис. 2.4). Чим більша площа – тим більша варіативність шрифту.

Рисунок 2.4 – Схема для демонстрації впливу критерію варіативності на придатність шрифту

Окрім цього, важливим є критерій інтеграції шрифтів із графічними методами перетворення. Для перевірки цього критерію слід провести тестування шрифтів на предмет їхньої придатності до використання з алгоритмами генерації псевдовипадкових графічних шумів, які можуть бути

накладені на шрифти для ускладнення їхнього дешифрування. Наприклад, рисунок 2.5 демонструє, як символ зберігає свою базову форму навіть за наявності випадкових графічних перешкод.

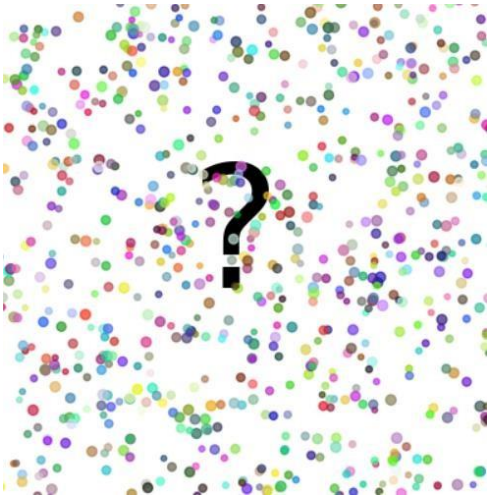

Рисунок 2.5 – Накладення графічного шуму на символ

Отже, визначення критеріїв придатності шрифтів для аналогового криптографічного перетворення охоплює аспекти стійкості до трансформацій, розбірливості у складних композиціях, підтримки варіативності та інтеграції із графічними методами. На основі цих критеріїв проводиться відбір шрифтів, що забезпечують максимальну функціональність та надійність у межах заданої криптографічної системи. Додаткові експерименти, спрямовані на візуалізацію результатів тестування, дозволяють оцінити ефективність вибраних шрифтів та зробити висновки щодо їхньої придатності.

2.2 Відбір шрифтів на основі заданих критеріїв

Відбір шрифтів для застосування в аналоговому методі криптографічного перетворення є ключовим етапом у забезпеченні ефективності системи захисту інформації. Цей процес передбачає аналіз і тестування графічних властивостей шрифтів відповідно до визначених критеріїв, які враховують специфіку аналогової криптографії. Зокрема, важливими аспектами є здатність шрифтів адаптуватися до графічних трансформацій, їхня читабельність у складних

композиціях та варіативність, що дозволяє використовувати їх у багатофункціональних криптографічних структурах.

Перший крок у відборі шрифтів полягає у визначенні їхньої графічної стійкості до трансформацій. Аналогове перетворення часто включає масштабування, повороти, накладення шуму та інші графічні зміни. [19] Шрифти повинні зберігати розпізнаваність символів навіть після таких змін. Наприклад, тонкі лінії символів можуть виявитися непридатними через ризик втрати видимості в умовах графічного шуму або масштабування. Відповідно, шрифти з чіткими контурами та достатньою товщиною ліній є кращими для цього завдання. Це пояснюється тим, що товщина ліній прямо впливає на їхню стійкість до спотворення в умовах накладення додаткових графічних елементів, таких як шум, що демонструється в попередніх рисунках.

Другим важливим аспектом є тестування шрифтів на предмет їхньої здатності формувати складні композиції, характерні для криптографічного кодування. Символи повинні легко інтегруватися в патерни, залишаючи можливість їхнього виділення серед інших елементів.[18] Відбір на основі цього критерію включає аналіз ширини символів, їхньої внутрішньої структури, а також візуальних проміжків між елементами. Наприклад, шрифти з надмірно широкими символами можуть утруднити формування компактних графічних патернів, тоді як надто вузькі символи ризикують зливатися в єдину структуру, що ускладнює дешифрування.

Третій етап передбачає перевірку шрифтів на варіативність їхнього використання. Аналогова криптографія передбачає можливість модифікації символів без втрати їхньої основної структури. Це може включати зміну кута нахилу, товщини ліній або навіть додавання додаткових елементів. Наприклад, шрифти, які дозволяють створювати різні варіанти одного і того ж символу, є більш гнучкими для криптографічних потреб. Це дає змогу ускладнити злам шифру через необхідність врахування безлічі можливих варіацій.

Таким чином, підставі проведеної мною роботи та викладених вище матеріалів, можна створити таку схему-алгоритм для відбору шрифтів, який включає кілька послідовних етапів, які показано на рисунку 2.6.

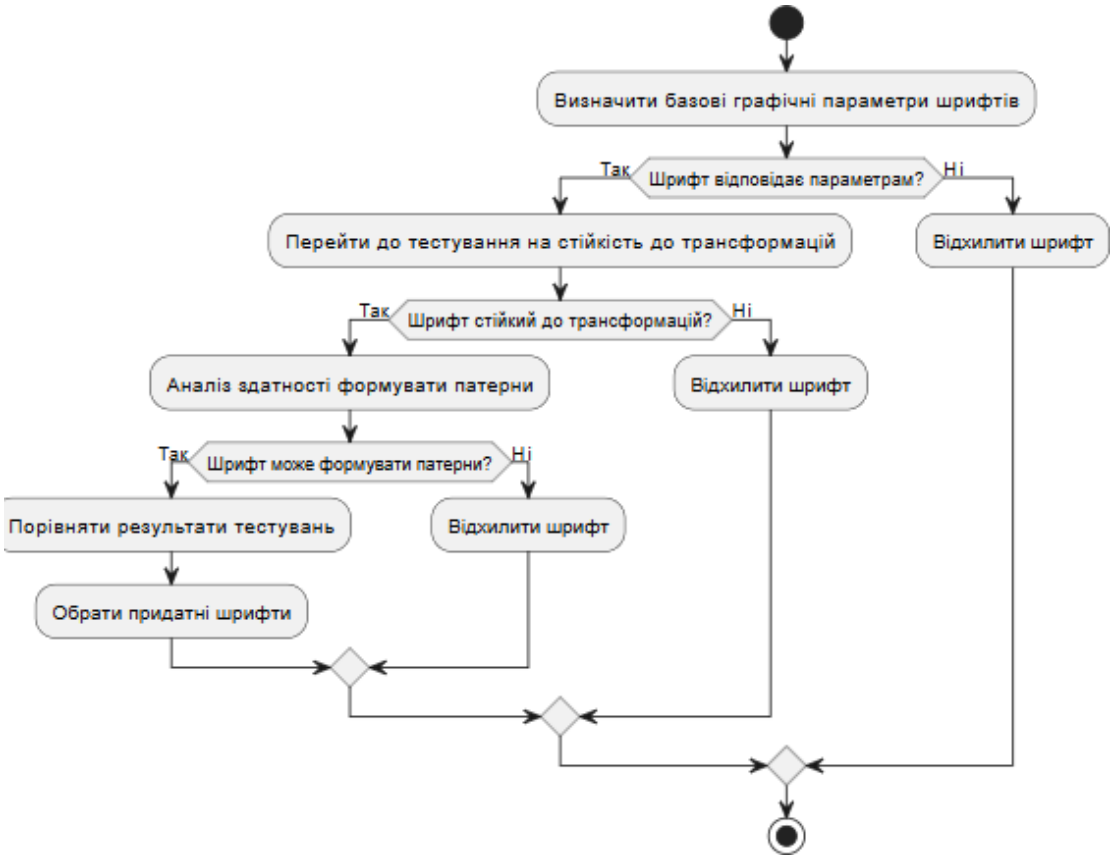

Рисунок 2.6 – Алгоритм відбору шрифтів для аналогового криптографічного перетворення

Алгоритм починається з визначення базових графічних параметрів шрифтів, які відповідають встановленим критеріям. Далі шрифти піддаються тестуванню на стійкість до трансформацій, де кожен символ перевіряється на розпізнаваність після масштабування, поворотів і накладення шуму. Наступним кроком є аналіз здатності шрифтів формувати патерни, що включає оцінку їхньої композиційної гнучкості та адаптивності. Завершальний етап алгоритму передбачає порівняння результатів тестувань і вибір найбільш придатних шрифтів для використання в криптографічній системі.

Отже, відбір шрифтів є складним багатокроковим процесом, що базується на ретельному аналізі їхніх графічних характеристик. Правильний вибір

шрифтів є вирішальним для забезпечення надійності системи аналогового криптографічного перетворення, оскільки графічні особливості шрифтів безпосередньо впливають на їхню здатність протистояти криптографічним атакам. Відповідно, використання алгоритму відбору дозволяє систематизувати процес і досягти максимальної ефективності при виборі шрифтів.

2.3 Комп'ютерне тестування шрифтів для аналогового криптографічного перетворення

Комп'ютерне тестування шрифтів для аналогового криптографічного перетворення є критично важливим етапом у процесі відбору графічних елементів, придатних для використання в умовах криптографічного захисту інформації. Такий підхід дозволяє не лише теоретично оцінити властивості шрифтів, але й перевірити їхню стійкість до різноманітних трансформацій та візуальних змін у реальних умовах, моделюючи можливі атаки та складні графічні композиції.

Проведений вище аналіз дозволяє розробити послідовність етапів для тестування шрифтів. Для цього було прийнято рішення створити програму з зручним інтерфейсом для кращої наглядності та спрощення процесу відбору. Мною реалізовано спеціальний Python-застосунок з графічним інтерфейсом на основі бібліотеки Tkinter та пакетів Pillow, numpy (повноцінний код програми можна перелянути в Додатку А). Він дозволяє у реальному часі моделювати різні варіанти зображення шрифтів із застосуванням криптографічних спотворень.

Тестування включає кілька послідовних етапів:

Перший етап — перевірка стійкості до масштабування. Програма дозволяє регулювати розмір шрифту за допомогою повзунка Scale:

```
size_var = tk.IntVar(value=50)
size_slider = tk.Scale(root, from_=10, to=150, orient="horizontal", label="Розмір", variable=size_var, command=update_image)
size_slider.pack()
```

Відображення тексту:

draw.text(position, text, fill="black", font=font)

Це дозволяє контролювати розмір символів та зберігати їхню впізнаваність при масштабуванні.

Другий етап — аналіз впливу графічного шуму. Накладання різних типів шуму реалізовано за допомогою генерації випадкових точок, ліній та сіток.

Наприклад, для точкового шуму:

```
for _ in range(noise_level * 20):
    x, y = random.randint(0, width-1), random.randint(0, height-1)
    color = tuple(np.random.randint(0, 255, 3))
    draw.ellipse((x, y, x+4, y+4), fill=color)
```

Користувач може обрати тип шуму з випадаючого списку.

Третій етап — перевірка варіативності елементів. Для цього користувач може обрати не лише шрифт, але й його стиль: normal, bold, italic, bold italic:

```
style_menu = ttk.Combobox(root, textvariable=style_var, values=["normal", "bold", "italic", "bold italic"])
```

Функція вибору шрифту зі стилем:

```
def get_font_path(base_font, style):
    style_suffix = {"normal": "", "bold": "bd", "italic": "i", "bold italic": "bi"}
    styled_font = f"{name}{style_suffix[style]}{ext}"
    if os.path.exists(styled_font):
        return styled_font
    else:
        return base_font
```

Це дозволяє перевіряти збереження основних ознак символів під час модифікацій.

Четвертий етап — симуляція умов дешифрування. На цьому етапі додається розмиття та додатковий випадковий фон:

```
if blur_amount > 0:
    image = image.filter(ImageFilter.GaussianBlur(blur_amount))
```

А також накладається псевдовипадковий колірний шум:

```
overlay = Image.new("RGB", (width, height), (255, 255, 255))
for _ in range(noise_level * 5):
    x, y = random.randint(0, width-1), random.randint(0, height-1)
    overlay.putpixel((x, y), (random.randint(0, 255), random.randint(0, 255), random.randint(0, 255)))
image = Image.blend(image, overlay, 0.3)
```

Таким чином моделюються реальні умови дешифрування на зашумлених або спотворених зображеннях.

Комп'ютерне тестування за допомогою цієї програми дозволяє систематизувати процес аналізу шрифтів, забезпечити наочність, керованість параметрами та обґрунтувати вибір найбільш придатних для аналогового криптографічного перетворення графічних елементів.

2.4 Процес тестування шрифтів для аналогового криптографічного перетворення

Тестування шрифтів для застосування в аналоговому криптографічному перетворенні включає кілька послідовних етапів, спрямованих на перевірку їхніх графічних характеристик та стійкості до змінних умов. Дослідження проводиться на основі програмного забезпечення, яке дозволяє моделювати текст у різних умовах. Етапи тестування охоплюють перевірку відображення тексту, регулювання параметрів товщини ліній, розміру шрифту, додавання графічного шуму та аналіз результатів для різних типів шрифтів.

На початковому етапі тестування вводиться текст, який буде використовуватись для аналізу. Наприклад, текст «Information technology 2025» вибрано для перевірки комбінацій літер і цифр. Це дає змогу оцінити відображення символів різного характеру в межах заданих параметрів. Введення тексту здійснюється через інтерактивне текстове поле, а його вигляд відображається на графічному полотні програми (рис. 2.7).

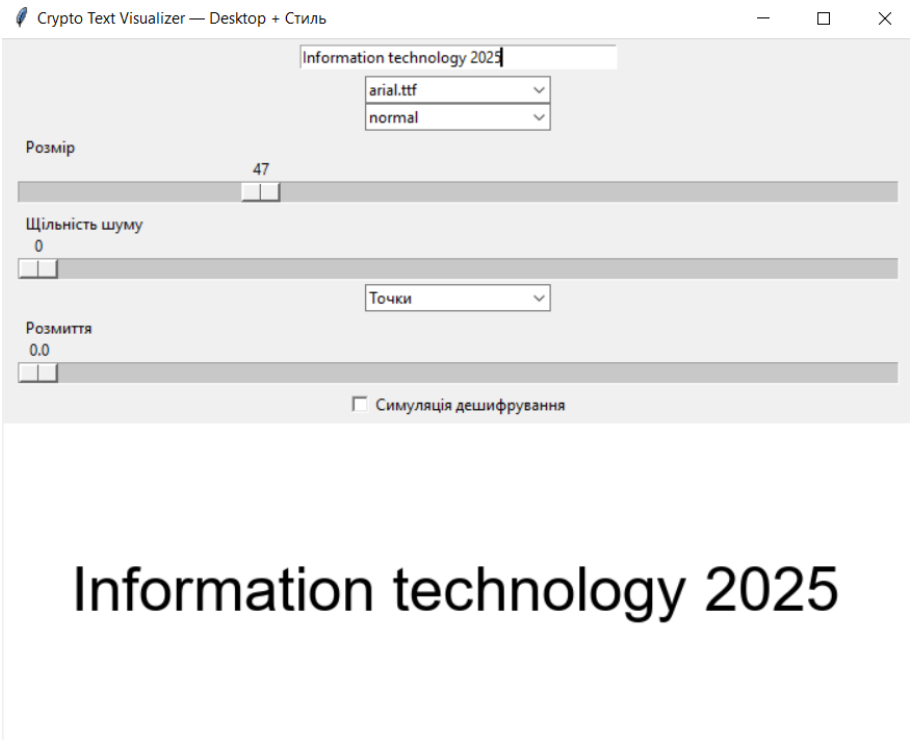

Рисунок 2.7 – Введення тестового тексту

Наступним кроком є вибір шрифту. Програма забезпечує можливість вибору будь-яких шрифтів, які будуть завантажені. На етапі тестування були завантажені такі шрифти як Arial, Georgia, Gothic та ін. Кожен із них демонструє різні особливості відображення, що впливають на стійкість до модифікацій, таких як масштабування, накладення шуму та зміна товщини ліній. Шрифт обирається через випадаюче меню (рис. 2.8), що дає змогу швидко перемикатись між шрифтами для аналізу їхньої придатності.

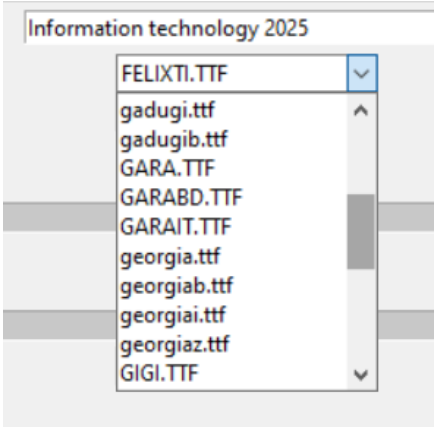

Рисунок 2.8 – Вибір шрифту в інтерфейсі програми

Критично важливим етапом є тестування масштабування тексту (рис. 2.9). Розмір шрифту регулюється в межах від 10 до 150 одиниць. Це дозволяє оцінити, як шрифт виглядає при зміні масштабу та чи зберігається його читабельність. Наприклад, символи з тонкими лініями можуть втрачати свою форму при значному зменшенні розміру, що робить їх непридатними для використання в умовах криптографічних перетворень. Під час тестування масштабу користувач може візуально оцінити, чи залишаються символи зрозумілими для дешифрування навіть за екстремальних змін розміру.

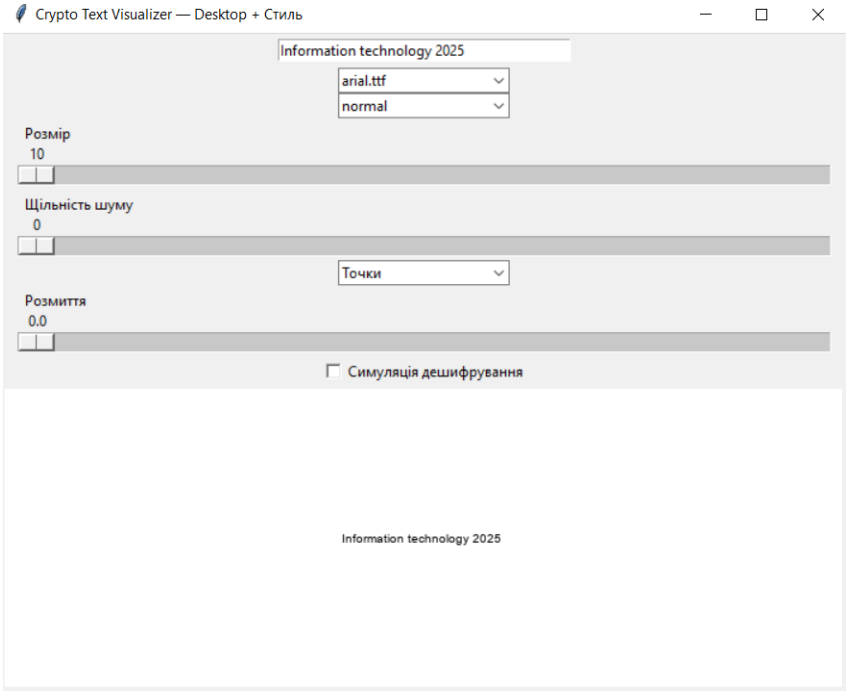

Рисунок 2.9 – Тестування масштабування тексту

Наступний етап передбачає зміну варіативності шрифту. У програмі передбачено можливість коригування стилю тексту, що імітує графічні модифікації, які можуть бути застосовані до тексту. Наприклад, стиль bold (жирний шрифт) підвищує стійкість символів до спотворень, але в той же час може ускладнювати формування складних композицій через накладання елементів. Стиль italic (курсив), навпаки, більш вразливий до візуальних змін і графічного шуму. Стиль налаштовується через випадаюче меню, і результати одразу відображаються на полотні програми (рис. 2.10).

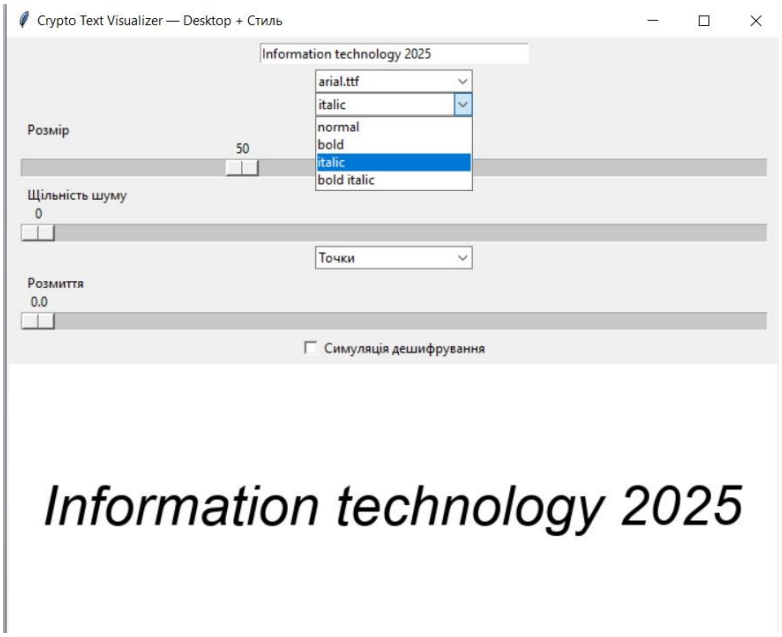

Рисунок 2.10 – Візуалізація тексту різного стилю

Додатковим аспектом тестування є накладення графічного шуму. Умови реального використання шрифтів у криптографії можуть включати наявність шумів, що ускладнюють розпізнавання символів. У програмі передбачено можливість додавання різних видів шуму (точки, лінії, сітка, комбінований) на графічне полотно. Користувач може налаштувати рівень шуму від 0 до 100 одиниць і спостерігати, як це впливає на читабельність тексту (рис. 2.11). Шрифт вважається придатним, якщо навіть за високого рівня шуму символи залишаються розпізнаваними.

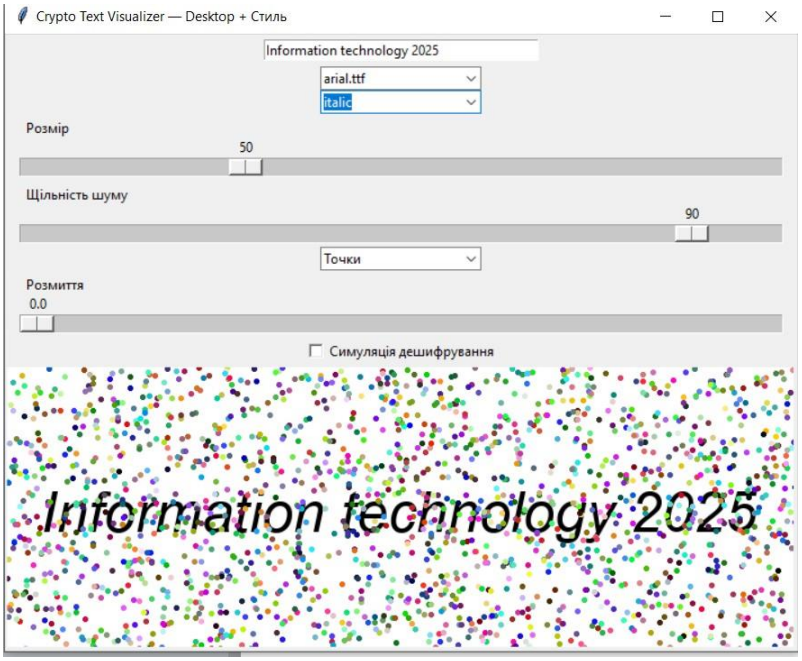

Рисунок 2.11 – Накладення графічного шуму на текст

Ще одним етапом є симуляція умов дешифрування. На цьому етапі користувач може коригувати рівень розмиття від 0.0 до 10.0 (рис. 2.12) та додати випадковий фон за допомогою опції «Симуляція дешифрування». Таким чином програма створює реальні умови дешифрування на зашумлених або спотворених зображеннях.

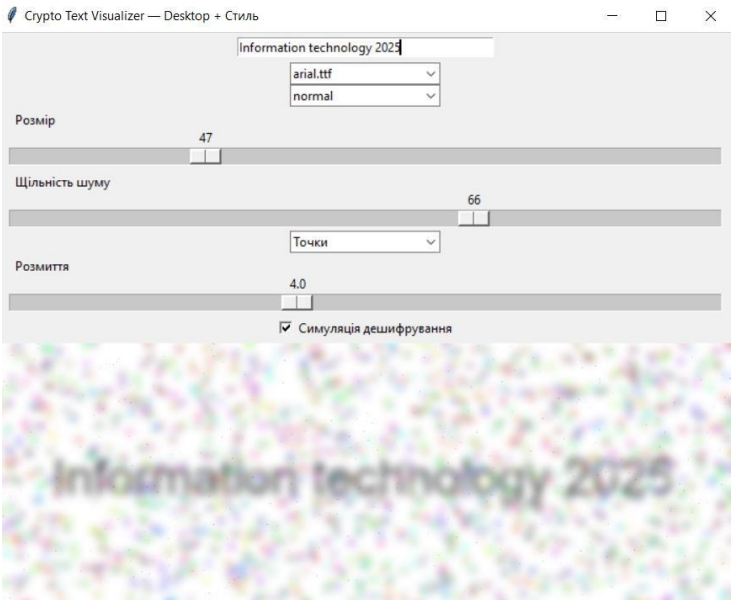

Рисунок 2.12 – Симуляція умов дешифрування

На завершальному етапі тестування проводиться аналіз придатності кожного шрифту для використання в умовах криптографічного перетворення. Враховуються результати всіх етапів: збереження форми символів при зміні масштабу, адаптивність до зміни товщини ліній та стійкість до шумів. Програма забезпечує інтерактивну візуалізацію, що дає змогу користувачеві прийняти обґрунтоване рішення про вибір оптимального шрифту.

Для комп’ютерного тестування придатності шрифтів до аналогового криптографічного перетворення було обрано набір шрифтів, що репрезентують різні типи графічних рішень, стилістичних особливостей і сфер використання. Такий вибір дозволяє комплексно оцінити поведінку шрифтів у ситуаціях, що моделюють реальні умови перешкод, спотворень і дешифрування.

До тестової вибірки увійшли такі шрифти:

- Arial — класичний sans-serif шрифт, який широко використовується в цифрових документах. Має збалансовану геометрію та чіткі контури, що дозволяє оцінити його стійкість до спотворень при збереженні впізнаваності символів.
- Times New Roman — шрифт із зарубками (serif), типовий для друкованих видань. Його використання у тестуванні дозволяє виявити вразливість дрібних елементів (зарубок) до графічного шуму та розмиття.
- Calibri — сучасний шрифт без зарубок, оптимізований для екранів. Завдяки округлим формам та збалансованій товщині ліній, цей шрифт дозволяє проаналізувати, як різні цифрові спотворення впливають на читабельність.
- Courier New — моноширинний шрифт, у якому кожен символ займає однакову ширину. Використовується переважно у програмуванні. Його специфіка дозволяє виявити особливості взаємного накладання символів та вплив стилізації на графічну регулярність.

- Comic Sans — неформальний шрифт з нерівномірною геометрією. Вибраний для тестування стійкості до шуму шрифтів з нетиповою структурою та декорованими елементами.
- Open Sans — відкритий, висококонтрастний шрифт із гарною читабельністю. Підтримує широке стилістичне варіювання, що дозволяє дослідити його придатність у різних графічних сценаріях.
- Roboto — шрифт, оптимізований для цифрових платформ (зокрема Android). Застосовується для оцінки адаптації до цифрового середовища та впливу візуальних ефектів на впізнаваність символів.

Обрані шрифти охоплюють як традиційні, так і сучасні графічні стилі, а також відрізняються наявністю зарубок, товщиною ліній, регулярністю структури та призначенням. Це дозволяє здійснити комплексне тестування, виявити сильні та слабкі сторони кожного шрифту при моделюванні аналогового криптографічного перетворення.

Під час оцінки масштабованості (рис. 2.9) було виявлено, що Arial, Calibri, Open Sans та Roboto найкраще зберігають читабельність символів при значному зменшенні та збільшенні розміру. Їхні тонкі та чіткі контури забезпечують стабільну форму літер навіть у найменших розмірах. У той час як Courier продемонстрував задовільні результати лише у середньому та великому діапазоні розмірів, символи Times почали втрачати розбірливість при зменшенні шрифту через складні деталі конструкції.

Одним із важливих критеріїв оцінки придатності шрифтів для використання в аналоговому криптографічному перетворенні є їхня стійкість до стилістичних модифікацій (варіативність), таких як жирність (bold), нахил (italic) або їх поєднання (рис. 2.10). Цей критерій визначає, наскільки символи зберігають свою впізнаваність при зміні графічного стилю.

Arial продемонстрував добру варіативність стилів. Шрифт підтримує всі стандартні стилі: звичайний, жирний, курсив та жирний курсив. У всіх варіаціях він зберігає геометрію символів. Жирність чітко посилює візуальну вагу, а курсив створює помірний нахил без помітного спотворення символів.

Calibri має високу стійкість до стилістичних змін. Плавні переходи між стилями, добре збалансовані контури та відсутність зайвих деталей забезпечують читабельність у будь-якій комбінації стилів. Roboto також показав гарні результати. Усі стилі працюють злагоджено, не викликаючи спотворень.

Courier New як моноширинний шрифт зберігає чіткість символів при зміні стилю, проте самі варіації стилів є менш вираженими. Bold і italic виглядають майже однаково, оскільки загальна геометрія символів практично не змінюється. Проте форма залишалася стабільною й чіткою в усіх випадках.

Times New Roman показав менш стабільну варіативність. Через наявність зарубок деякі стилістичні трансформації, особливо курсив, можуть деформувати дрібні елементи символів. Жирність іноді призводить до злиття деталей, особливо при зменшеному розмірі або на тлі шуму.

Comic Sans показав найнижчу варіативність стилю. Між варіаціями жирності та нахилу практично немає суттєвих змін. Це зменшує здатність шрифту до адаптації, а його декоративна природа робить його менш придатним для умов, де важлива графічна точність.

Найкращим серед усіх шрифтів у цій категорії виявився Open Sans. Він відмінно підтримує всі стилі, демонструє чітке розмежування між ними, а зміна стилю не призводить до втрати геометрії символів. Жирність не перекриває елементи, а курсив виконується акуратно та пропорційно.

У реальних умовах передача або зберігання інформації може супроводжуватися додаванням різного роду перешкод, таких як цифрові артефакти, фонові накладення або спотворення, які ускладнюють процес розпізнавання символів. Саме тому важливим критерієм при оцінці придатності шрифтів до використання в аналоговому криптографічному перетворенні є їх стійкість до графічного шуму (рис. 2.11).

Шрифти з чіткими та простими геометричними формами, зокрема Arial, Calibri, Open Sans та Roboto, продемонстрували високий рівень стійкості. Незважаючи на різний рівень накладеного шуму, ці шрифти зберігали

структуру символів, що дозволяло впізнати текст навіть за умов високої щільності артефактів.

Особливо добре себе показали Open Sans і Roboto — навіть за умови комбінованого шуму з високою щільністю символи залишались впізнаваними завдяки достатньому міжсимвольному інтервалу, збалансованій товщині ліній та великій висоті малих літер (x-height).

Courier New також виявився доволі стійким через чітку сіткову структуру та однакову ширину символів, проте візуально шум сприймався сильніше через щільне розміщення символів, що трохи ускладнювало зчитування при великій щільності перешкод.

Натомість Times New Roman виявився вразливішим до шуму. Його тонкі зарубки та декоративні елементи швидко «губилися» у точковому або лінійному шумі. Це призводило до зменшення чіткості символів, особливо при малому розмірі тексту.

Comic Sans, через свою нерегулярну структуру і слабко виражені контури, виявився одним з найменш стійких шрифтів. Навіть при середньому рівні шуму деякі символи втрачали форму і були складно впізнавані.

Нижче наведена таблиця 2.1 з усіма критеріями тестування

Таблиця 2.1 - Оцінка стійкості шрифтів

Назва шрифту	Масштабування (стійкість)	Шум (точки)	Шум (лінії)	Шум (сітка)	Розмиття	Стиль (адаптація)	Оцінка
Arial	Висока	Висока	Середня	Висока	Висока	Стабільна	9/10
Times New Roman	Середня	Низька	Середня	Середня	Середня	Погана	6/10
Calibri	Висока	Висока	Висока	Висока	Висока	Стабільна	9/10
Courier New	Висока	Середня	Висока	Низька	Середня	Стабільна	8/10
Comic Sans	Середня	Середня	Низька	Середня	Низька	Погана	5/10

Продовження таблиці 2.1

Open Sans	Висока	Висока	Висока	Висока	Висока	Стабільна	10/10
Roboto	Висока	Висока	Висока	Середня	Висока	Стабільна	9/10

Таким чином, за результатами всіх етапів тестування найкращі результати продемонстрував шрифт Open Sans, який зберігав високу читабельність та стабільність форми в усіх тестових ситуаціях. Його поведінка при накладенні шуму, зміні стилів та під час симуляції умов дешифрування залишалася передбачуваною, що свідчить про високу придатність до застосування в криптографічному контексті.

Шрифти Calibri, Arial та Roboto, які також отримали високу підсумкову оцінку (9/10), можуть ефективно використовуватись у більшості графічних сценаріїв. Водночас, під час роботи з ними слід враховувати певні нюанси. Наприклад, Arial втрачає частину деталей при сильному розмитті, а Calibri менш чітко передає стилі при мінімальному масштабі. Roboto ж може видаватися надто «механістичним» у поєднанні з сітковим шумом. Проте всі ці шрифти залишаються стабільними, зберігаючи впізнаваність навіть у складних умовах.

Найменш придатним виявився Comic Sans, структура якого нестабільна, а стилістична варіативність обмежена. У присутності шуму символи швидко втрачають чіткість, що робить його непридатним для графічно-навантажених середовищ.

Проведене дослідження засвідчило важливість детального аналізу шрифтів при їхньому застосуванні в задачах інформаційної безпеки. Використання комп’ютерного тестування дозволяє здійснювати усвідомлений вибір графічних елементів, підвищуючи стійкість систем до візуальних атак, спотворень і несанкціонованого дешифрування.

3 РОЗРОБКА РЕКОМЕНДАЦІЙ ДЛЯ ВИКОРИСТАННЯ ШРИФТІВ У АНАЛОГОВОМУ КРИПТОГРАФІЧНОМУ ПЕРЕТВОРЕННІ

3.1. Формування рекомендацій для вибору шрифтів

При виборі шрифтів для використання в аналоговому криптографічному перетворенні даних необхідно враховувати різноманітні аспекти, які безпосередньо впливають на ефективність шифрування, його стійкість до атак і швидкість виконання криптографічних операцій. Кожен тип шрифту має свої особливості, які можуть як покращити, так і ускладнити криптоаналітичні методи. Тому підбір шрифтів є критично важливим для створення надійних систем захисту.

Одним з перших критеріїв для вибору шрифтів є їх типологія. Шрифти можна розділити на кілька основних категорій: шрифти з засічками (serif), шрифти без засічок (sans-serif) та декоративні шрифти. Кожен з цих типів має свої переваги та недоліки в контексті криптографії.

Шрифти з засічками є традиційно популярними в книгодрукуванні та використовуються для текстів, що потребують легкості сприйняття при довготривалому читанні. Наприклад, Times New Roman є одним з найбільш відомих шрифтів цієї категорії. Засічки допомагають полегшити читання на великих відстанях, проте в контексті криптографії вони можуть стати проблемою. Засічки ускладнюють розпізнавання символів, і в поєднанні з іншими параметрами (наприклад, великі літери, зміна накреслення) можуть створювати складні патерни. Однак для криптографічних систем, що використовують аналогове перетворення, шрифти з засічками можуть бути менш оптимальними через складність в створенні чітких, регулярних структур символів, що спрощує криптоаналіз.

Важливим фактором є те, що шрифти з засічками можуть значно збільшувати час обробки символів при шифруванні, оскільки кожна засічка створює додаткові варіації символів, що вимагають більш складних математичних операцій для дешифрування. Таким чином, їх застосування може

бути обмеженим у високопродуктивних системах або тих, де важлива швидкість шифрування.

Шрифти без засічок, такі як Arial, Helvetica або Calibri, є найбільш поширеними в сучасних комп'ютерних системах. Вони мають просту та чітку структуру, що дозволяє легко та швидко розпізнавати символи, а також прискорює процес шифрування та дешифрування. Шрифти без засічок мають деякі переваги в контексті криптографії, оскільки їх регулярні форми та відсутність додаткових елементів роблять аналіз значно простішим для машинних алгоритмів. Завдяки своїй простоті, шрифти без засічок також сприяють більш швидким криптографічним операціям, що може бути корисним в умовах обмежених обчислювальних ресурсів або для систем, де ефективність та швидкість є критичними. Проте для підвищення надійності шифрування в таких шрифтах можна використовувати додаткові варіації накреслення чи жирності, щоб ускладнити дешифрування.

Шрифти з нерівними пропорціями букв (наприклад, шрифти, в яких символи мають різну ширину, як у шрифтах Monospaced або інші варіанти із змінною шириною символів) є досить цікавими з точки зору криптографії. Вони створюють більшу складність для криптоаналітиків, оскільки різні символи мають різну фізичну ширину, що ускладнює дешифрування, особливо коли шифр використовує стеганографічні методи (приховування даних у вигляді символів).

Шрифти з нерівними пропорціями букв можуть створювати додаткові бар'єри для дешифрувальників, оскільки наявність різної ширини дозволяє ефективніше маскувати зміст повідомлень. Для прикладу, такі шрифти можуть бути корисними в методах аналогового шифрування, де кожен символ має не лише певну візуальну форму, але й певну кількість одиниць вимірювання, що ускладнює розпізнавання окремих символів під час дешифрування.

Проте використання шрифтів з нерівними пропорціями може бути обмеженим у ситуаціях, де є високі вимоги до швидкості обробки даних. Оскільки кожен символ має різну ширину, процес шифрування може бути

більш обтяжливим для системи. Також важливо, щоб шрифт не ставав занадто складним для автоматичних систем розпізнавання, оскільки це може призвести до втрати продуктивності.

Іншим важливим фактором, що впливає на вибір шрифтів для криптографічного шифрування, є варіації жирності та накреслення символів. Змінюючи ці параметри, можна створювати додаткові варіації символів [20], що ускладнює дешифрування. Наприклад, для одного й того ж символу можна використовувати кілька варіантів жирності (звичайний, напівжирний, жирний), а також варіанти накреслення (курсив, звичайний, підкреслений). Це дозволяє заплутати аналіз шифрування та зробити його більш стійким до простих атак, заснованих на частотному аналізі.

Проте використання шрифтів з варіаціями жирності чи накреслення потребує обережності, оскільки це може значно збільшити обчислювальні витрати при шифруванні та дешифруванні. Тому важливо знайти оптимальний баланс між додаванням складності до шифру та забезпеченням достатньої швидкості роботи системи.

При виборі шрифтів для аналогового криптографічного перетворення важливо враховувати як рівень безпеки, так і технічні обмеження на швидкість обробки даних, щоб досягти найкращих результатів у захисті інформації.

На основі наведеної вище інформації можна створити таблицю з рекомендаціями для вибору шрифтів, яка може стати корисним інструментом у процесі аналізу та відбору шрифтів.

Таблиця 3.1 - Рекомендації для відбору шрифтів

№	Критерій	Рекомендація
1	Типологія	Шрифти без засічок я кращим варіантом для використанні в контексті аналогового шифрування, бо вони є стійкими до спотворень, трансформацій, не втрачають читабельність.

Продовження таблиці 3.1

2	Пропорційність	Шрифти з нерівними пропорціями букв можуть створювати додаткові бар'єри для зловмисників, оскільки наявність різної ширини дозволяє ефективніше маскувати зміст повідомлень
3	Варіативність	Шрифти з різними варіаціями жирності та накреслення можуть бути корисними в контексті створення складніших схем шифрування, оскільки вони дозволяють створювати різні вигляди одного й того ж символу, що ускладнює криптоаналітичні методи на основі порівняння символів у зашифрованому тексті.

Враховуючи рекомендації та викладену вище інформацію, було визначено послідовність дій для ефективного відбору шрифтів і застосування їх в аналоговому методі криптографічного перетворення даних:

1) Проаналізувати особливості системи, в якій планується використовувати шрифт (рівень продуктивності, кількість та рівень ресурсів, швидкість обробки інформації в системі тощо);
2) Визначити типологію шрифту;
3) Переглянути рівень варіативності шрифту;
4) Проаналізувати кожну структурну характеристику шрифту на прикладі декількох його символів (цифри, велика/маленька літери, спеціальні символи);
5) Перевірити читабельність шрифту після друку, створення скан-копії, на різних цифрових пристроях (телефон, планшет, ноутбук тощо);
6) Провести комп’ютерне тестування шрифту, використовуючи Python-застосунок;

7) Шрифт допускається до застосування лише за умови успішного проходження всіх етапів відбору, причому кожен етап має підтвердити його відповідність встановленим критеріям.

3.2. Обґрунтування вибору шрифтів для аналогового шифрування

Обґрунтування вибору шрифтів для аналогового шифрування є важливим етапом у розробці системи захисту даних, оскільки типи шрифтів мають суттєвий вплив на складність криптографічного перетворення та на стійкість до криптоаналітичних атак. Правильний вибір шрифтів забезпечує не лише ефективність шифрування, але й максимальний рівень безпеки для передаваних або збережених даних.

Аналогове шифрування відрізняється від цифрових методів тим, що дані шифруються без застосування математичних функцій на бінарному рівні, а зміни вносяться до фізичних або візуальних властивостей символів. Таким чином, для забезпечення безпеки за допомогою аналогового шифрування, кожен символ шрифту може бути трактований як окрема одиниця інформації. Вибір шрифтів стає критичним для забезпечення стійкості до атак, таких як частотний аналіз, аналіз пропорцій та стеганографія, де навіть мінімальні візуальні варіації можуть мати велике значення.

Оскільки для аналогового шифрування використовуються фізичні або графічні зміни символів, що їх відображають, ці зміни повинні бути достатньо складними для того, щоб заплутати можливі криптоаналітичні атаки.[16] Різні шрифти, що мають варіації в структурі символів, а також змінні характеристики (якщо йдеться про жирність, накреслення або пропорції), можуть допомогти створити «шум» у процесі дешифрування.

Важливим аспектом є товщина ліній, які утворюють символи шрифту. Шрифти можуть мати лінії різної товщини, від дуже тонких до дуже товстих. Це може додатково ускладнити дешифрування, якщо символи мають різні варіації по товщині ліній. У випадку застосування шрифтів для аналогового шифрування вибір шрифту з варіативною товщиною ліній дозволяє створити

додаткові ускладнення для криптоаналітичних методів, оскільки кожен символ може мати декілька варіацій, що ускладнює пошук шаблонів.

Пропорції між символами також є важливим елементом, який впливає на шифрування. Вибір шрифтів з нерівними пропорціями символів, де деякі літери ширші або вищі за інші, може створити додаткові труднощі в процесі дешифрування. Наприклад, якщо в одному шрифті деякі літери мають значно більшу ширину, ніж інші, це може допомогти заплутати аналітика, оскільки такі шрифти ускладнюють стандартні методи дешифрування, орієнтуючись на частотний аналіз чи інші математичні методи.

У випадку аналогового шифрування розмір символів також має важливе значення, оскільки зміна розміру може не тільки змінити візуальний вигляд тексту, але й вплинути на його читабельність і сприйняття. Тому при виборі шрифтів для шифрування важливо враховувати не тільки стандартні розміри, але й можливість маніпулювати цими розмірами для створення додаткових варіацій символів.

Шрифти можуть бути моноширинними або пропорційними. Моноширинні шрифти використовують однакову ширину для кожного символу, що може бути корисно для деяких специфічних типів шифрування, де кожен символ має бути чітко вирівняним, щоб забезпечити надійне шифрування і захист від криптоаналізу. Пропорційні шрифти, в свою чергу, дозволяють символам мати різну ширину, що може бути використано для створення більш складних і багатих варіацій тексту, що значно ускладнює криптоаналіз.

Додаткові варіації накреслення та жирності шрифтів є важливими аспектами, що можуть значно вплинути на ефективність та надійність аналогових криптографічних систем. Вони створюють додаткові варіації у візуальному вигляді символів, що ускладнює процес їх дешифрування, роблячи криптографічні атаки більш складними та менш ефективними. Накреслення та жирність шрифтів можуть використовуватися як інструмент для модифікації

звичних символів, надаючи їм нові ознаки, які важко розпізнати за допомогою стандартних методів криптоаналізу.

Одним із основних типів варіацій є накреслення шрифтів, яке включає стандартні варіанти, такі як звичайний, курсив, напівжирний, жирний та інші. Звичайний накреслений шрифт, тобто стандартний прямий текст, зазвичай є найпростішим для сприйняття, але на додачу до нього можна застосовувати інші стилі, що значно ускладнюють криптографічний аналіз. Наприклад, курсивне накреслення створює ефект нахилу символів, що змінює їх форму та положення у рядку. Такий стиль може додавати складності для аналізу шифрованого тексту, оскільки символи стають дещо спотвореними, що робить їх менш чіткими та знижує ефективність стандартних методів дешифрування.

Застосування жирності також має важливе значення. Жирний шрифт створює більш виразні лінії для кожного символу, що може стати перевагою при шифруванні, оскільки дозволяє створити додаткові варіації у вигляді букви. Жирні символи можуть значно змінювати візуальні характеристики тексту, порівняно зі стандартними, надаючи додаткові можливості для ускладнення шифрування.

Важливим аспектом є комбінація різних варіацій накреслення і жирності в одному шрифті. Наприклад, можна використовувати курсив і жирний шрифт одночасно, що дозволяє створити більш виразну візуальну варіацію символів. Така комбінація не тільки спотворює вигляд символів, але й створює додаткову варіативність у тексті, що значно ускладнює його дешифрування. Оскільки ці варіації комбінуються на рівні кожного окремого символу, їх складність для розпізнавання збільшується, що робить текст менш уразливим для різних криптоаналітичних атак.

Використання варіацій накреслення та жирності також дозволяє зберегти певну читабельність тексту, але одночасно додати достатню складність для криптоаналізу. Це може бути особливо корисно, коли важливо зберегти загальний вигляд тексту, але додати декілька рівнів варіативності для ускладнення дешифрування. В результаті, текст з такими варіаціями

виглядатиме більш складним для сприйняття та аналізу, оскільки навіть з використанням стандартних методів дешифрування він виглядатиме як множина варіацій того самого повідомлення.

Наслідком цього є значне підвищення безпеки шифрування, оскільки будь-які зміни в накресленні та жирності можуть внести додаткові перешкоди для алгоритмів криптоаналізу, що зазвичай покладаються на розпізнавання шаблонів і частотний аналіз. Використання таких варіацій може також обмежити застосування деяких криптографічних атак, таких як атаки методом підбору або криптоаналіз на основі шаблонів.

Візуальні ускладнення для криптоаналізу є важливим аспектом у розробці надійних шифрів, які повинні бути стійкими до різноманітних атак [17]. Криптографічні системи зазвичай покладаються на певні властивості шрифтів, що дозволяють здійснювати розпізнавання символів або проводити аналіз частотності для дешифрування. Візуальні ускладнення, що додаються до шрифтів або шифрованих повідомлень, значно ускладнюють ці процеси, створюючи додаткові перешкоди для криптоаналізу.

Одним із основних методів ускладнення є використання шрифтів з нерівними пропорціями букв. У стандартних шрифтах, таких як моноширинні шрифти, всі символи мають однакову ширину. Це полегшує процес дешифрування, оскільки криптоаналітики можуть легко побудувати графіки або таблиці для визначення частоти появи певних літер чи груп символів. Шрифти з нерівними пропорціями, у яких різні букви займають різну кількість горизонтального простору, змінюють цю ситуацію. Вони створюють значно більш складні варіації символів, що ускладнюють проведення частотного аналізу, оскільки простежити закономірності в таких шрифтах значно важче.

Іншим важливим аспектом є варіації висоти та нахилу букв. Шрифти, де символи можуть бути подовжені чи скорочені, а також ті, що мають різні варіанти нахилу або зміщення, додають ще один рівень складності для криптоаналізу. Це дозволяє приховати значення символів, що робить стандартні методи розпізнавання менш ефективними. Нахилений текст або

текст із зміненою висотою букв порушує звичний порядок символів, що також впливає на точність частотного аналізу, який є основним методом для дешифрування деяких видів шифрів.

Ще одним важливим аспектом є використання деформацій і нестандартних інтерліньяжів (відстаней між рядками). Це робить текст ще більш важким для розпізнавання, оскільки змінюється не тільки структура символів, але й їх взаємне розташування в межах тексту. У шифрованому тексті, де застосовуються такі зміни, криптоаналітик може мати труднощі при спробах реконструювати оригінальний вигляд повідомлення. Навіть якщо окремі символи будуть легко розпізнані, правильний порядок і структура тексту можуть стати для аналітика проблемою, що істотно сповільнює процес дешифрування.

До того ж, використання різних кольорів шрифтів або зміни їх насиченості та контрасту може додати ще один рівень ускладнення. Кольорове шифрування не є новою концепцією в криптографії і може використовуватися як додатковий механізм для ускладнення процесу розшифровки. Якщо змішувати різні кольори або варіанти насиченості, це може вплинути на загальний вигляд тексту, що робить його ще важчим для автоматизованих систем аналізу. Такий підхід дозволяє розподіляти інформацію за допомогою кольору, що додає додаткові варіації та ускладнює процес дешифрування.

Незважаючи на те, що візуальні ускладнення можуть допомогти захистити дані від простих атак, вони також можуть додавати виклики для звичних методів обробки інформації. Наприклад, шрифт з сильно деформованими символами або з багатьма візуальними змінами може бути неприязним для програм, які виконують автоматичну обробку тексту, таких як оптичне розпізнавання символів (OCR). [18] Це може стати корисним елементом для захисту даних, особливо якщо шифровані повідомлення повинні передаватися через канали, де автоматизовані системи обробки даних є основним методом для дешифрування.

Окрім того, для ускладнення криптоаналізу можуть використовуватися нестандартні стилі, як, наприклад, рукописні шрифти або шрифти, що мають хаотичні чи складні форми. Це створює додаткові труднощі для розпізнавання і дешифрування тексту, оскільки в таких шрифтах немає чітких правил для побудови букв чи цифр, що дозволяє значно збільшити складність дешифрування за допомогою традиційних методів, таких як частотний аналіз.

Усі ці візуальні ускладнення можуть створити багатоступеневий захист для шифрованого тексту, роблячи його більш стійким до різних видів криптоаналізу. Однак важливо враховувати, що надмірне ускладнення шрифтів може вплинути на швидкість передачі та читабельність тексту. Тому для забезпечення ефективного криптографічного захисту важливо знайти оптимальний баланс між складністю шрифтів і їхньою здатністю забезпечувати надійне шифрування.

Одним з основних аспектів, чому шрифти з нерівними ширинами символів можуть бути корисними для криптографії, є те, що вони ускладнюють проведення частотного аналізу, який є одним з найпоширеніших методів криптоаналізу. У моноширинних шрифтах, де всі символи мають однакову ширину, часто можна легко відслідковувати співвідношення між символами, оскільки це дозволяє спостерігати постійну структуру в тексті. У пропорційних шрифтах, проте, кожен символ займає різний простір, що змінює загальний вигляд тексту і робить відстеження таких закономірностей значно складнішим.

Наприклад, у моноширинному шрифті символи «I» та «W» займають рівну кількість горизонтального простору, тому аналізуючи частоту використання цих літер, криптоаналітик може побудувати таблиці або діаграми, щоб виявити шаблони, що допомагають у розшифруванні. У пропорційних шрифтах, де «I» займає менше місця, ніж «W», та ж сама частота символів буде виглядати по-різному в залежності від конкретної форми кожної літери. Це додає складності для аналізу частоти символів, оскільки тепер необхідно враховувати варіації в ширині символів, що робить традиційний метод частотного аналізу набагато менш ефективним.

Крім того, шрифти з нерівними ширинами символів можуть надавати додаткові можливості для прихованого кодування інформації. Завдяки різним пропорціям букв, можливо ввести елементи шифрування через варіації в горизонтальних інтервалах між символами. Це може бути корисним у ситуаціях, коли потрібно забезпечити додаткову захищеність даних без використання складних криптографічних алгоритмів. Якщо для кожного символу чи літери використовувати певну ширину, яка змінюється відповідно до деякого правила чи ключа, то це може додатково ускладнити спроби відновлення оригінального тексту.

Також важливим є той факт, що шрифти з нерівними ширинами дозволяють створювати графічні та візуальні варіації тексту, які ускладнюють його читання автоматизованими системами, такими як оптичне розпізнавання символів (OCR). [18] У разі, якщо текст зашифрований або прихований в певному шрифті з нерівними пропорціями символів, система OCR може зіштовхнутися з труднощами при спробі правильно розпізнати або класифікувати символи, оскільки для кожної літери або цифри потрібна буде індивідуальна перевірка та адаптація алгоритмів.

Пропорційні шрифти також можуть застосовуватися у контексті використання криптографічних ключів або кодів, де виведення або надання певних даних залежить від ширини символів. Наприклад, у деяких випадках криптографічні ключі можуть бути закодовані у вигляді змінних пропорцій шрифтів, що дозволяє створити додатковий рівень захисту даних. У такому випадку ширина символів стає важливою складовою для правильного дешифрування повідомлень або для подолання шифру.

Важливо відзначити, що застосування шрифтів з нерівними ширинами може мати певні технічні обмеження та вимоги, зокрема щодо швидкості обробки тексту або його виведення. Оскільки кожен символ має свою ширину, розміщення тексту на сторінці чи екрані може бути менш передбачуваним, і для комп’ютерних програм чи автоматизованих систем це може створювати додаткові труднощі при обробці. З точки зору технічної реалізації, робота з

такими шрифтами може вимагати більше ресурсів для збереження або виведення тексту у вигляді, що задовольняє криптографічні вимоги.

При виборі шрифтів для застосування в криптографії необхідно враховувати низку критеріїв, що сприяють забезпеченню безпеки, швидкості шифрування та ефективності застосування шрифтів в різних контекстах. Кожен з цих критеріїв є важливим для визначення, наскільки підходить певний шрифт для використання в аналогових криптографічних методах.

Першим і найбільш важливим критерієм є безпека шрифта, його стійкість до крипто аналізу [21]. У криптографії основна мета полягає в забезпеченні того, щоб зашифрований текст не піддавався розшифруванню без наявності відповідного ключа або методу дешифрування. Для цього необхідно використовувати шрифти, які ускладнюють застосування традиційних методів криптоаналізу. Це включає в себе частотний аналіз, який є одним з основних способів розкриття шифрів. Для зменшення ефективності цього методу слід використовувати шрифти, які мають нерівні ширини символів або значно варіативні форми букв. Такі шрифти значно складніше аналізувати з точки зору частоти, адже навіть одна й та сама буква може мати різну ширину залежно від її положення в тексті. Також шрифти з нерівними пропорціями букв або схованими елементами можуть допомогти приховати відомості, що використовуються в криптографічному процесі.

Наступним важливим критерієм є швидкість та ефективність шифрування. Незважаючи на важливість безпеки, криптографічні процеси мають бути досить швидкими та ефективними для практичного використання. Затримки в процесі шифрування або розшифрування можуть бути неприязні для користувачів або для систем, які потребують миттєвих операцій, наприклад, в системах електронної комерції чи для реального часу передачі даних. Шрифти, які володіють простими або менш складними візуальними характеристиками, можуть бути більш ефективними з точки зору швидкості криптографічних операцій. Однак важливо знайти баланс між швидкістю обробки та безпекою. Вибір шрифтів для шифрування повинен забезпечувати

достатній рівень складності для криптоаналізу, не знижуючи при цьому ефективність процесу шифрування.

Ще одним критерієм є універсальність застосування шрифтів. Шрифт, який обирається для криптографії, має бути універсальним для різних видів застосувань. Це означає, що він повинен бути сумісний з різними мовами та системами, в яких використовуються різні символи. Для систем, що працюють з декількома мовами, вибір шрифтів може бути важливим аспектом, оскільки деякі символи або літери можуть виглядати схоже на інші, що може призвести до помилок у шифруванні або розшифруванні. Пропорційні шрифти, які мають індивідуальну ширину для кожного символу, можуть бути більш підходящими для таких систем, оскільки вони можуть допомогти зменшити ймовірність помилок через схожість символів.

Універсальність також включає адаптивність шрифтів до різних типів криптографічних операцій [21]. Деякі шрифти можуть бути ефективнішими для використання в системах, що потребують швидкої обробки тексту, тоді як інші можуть бути корисними для більш складних методів шифрування, таких як алгоритми, що використовують багаторівневу обробку даних або спеціальні криптографічні ключі.

Крім того, важливим аспектом є адаптивність шрифтів до різних технологій. У сучасних криптографічних системах шрифти повинні бути сумісні з різними платформами та середовищами, як для апаратних, так і для програмних рішень. Це включає сумісність із різними операційними системами, бібліотеками шифрування та іншими криптографічними інструментами, які використовуються в практиці. Вибір шрифтів, які можуть легко інтегруватися в різні програмні платформи, важливий для забезпечення гнучкості та масштабованості криптографічних рішень.

Критерії вибору шрифтів для криптографії включають безпеку, швидкість, ефективність шифрування та універсальність застосування. Шрифт повинен бути стійким до криптоаналізу, забезпечувати оптимальну швидкість шифрування та бути здатним до універсального застосування в різних

криптографічних системах та платформах. Вибір шрифтів, що відповідають цим вимогам, є важливим кроком у створенні надійних криптографічних рішень.

3.3. Аналіз перспектив застосування обраних шрифтів

Вплив новітніх криптоаналітичних методів на вибір шрифтів є важливим аспектом при розробці криптографічних систем. З розвитком технологій криптоаналізу і застосуванням новітніх методів, таких як машинне навчання, глибинне навчання та інші техніки штучного інтелекту, зростає здатність автоматичних систем знаходити та аналізувати закономірності в зашифрованих даних. Це значно змінює вимоги до шрифтів, які використовуються в криптографії, оскільки потрібно забезпечити максимальну стійкість до таких інструментів.

Традиційні методи криптоаналізу, як правило, ґрунтуються на виявленні шаблонів, статистичних аномалій або частотного аналізу, що допомагає дешифрувати зашифровану інформацію. Однак з розвитком алгоритмів машинного навчання ці методи стають значно ефективнішими. Машинне навчання дозволяє системам "вчитися" на великих масивах даних, виявляючи навіть неявні закономірності, які можуть бути використані для розшифрування тексту. Шрифти, які використовуються в криптографії, мають враховувати цю зміну. Для того щоб підвищити стійкість шрифтів до таких атак, необхідно ускладнити візуальні характеристики символів. Наприклад, шрифти з нерівними пропорціями, варіаціями товщини літер або несиметричними елементами можуть ускладнити роботу алгоритмів, оскільки вони не дозволяють виявити чіткі патерни для дешифрування.

Крім того, новітні методи криптоаналізу використовують підхід, який полягає в обробці великих обсягів даних з різними характеристиками. Це означає, що шрифт повинен бути не тільки складним у плані візуальних характеристик, але й мати здатність змінювати свої параметри в залежності від контексту використання. Наприклад, шрифт, який варіює товщину ліній або пропорції літер залежно від зовнішніх умов (таких як освітлення чи кут

нахилу), може створити додаткові труднощі для автоматичних систем, які не зможуть ідентифікувати стандартні патерни.

Машинне навчання також дозволяє створювати моделі, які здатні розпізнавати й аналізувати навіть мінімальні відмінності в шрифтах, що ставить вимоги до складності та варіативності вибору шрифтів для криптографічних задач. Важливо, щоб шрифти, що використовуються для шифрування, забезпечували рівень ускладнення, який буде достатнім для запобігання криптоаналізу, навіть якщо будуть застосовуватися найсучасніші методи обробки інформації.

Квантова криптографія є новим етапом у розвитку технологій захисту інформації, що базується на принципах квантової механіки, і вона може значно вплинути на вибір шрифтів, використовуваних у криптографічних системах. Ключовою особливістю квантових обчислень є їх здатність швидко вирішувати задачі, які є складними або навіть неможливими для класичних комп'ютерів, що має важливі наслідки для безпеки криптографії та вибору шрифтів.

З розвитком квантових комп'ютерів з'являються нові загрози для класичних методів шифрування, таких як RSA або алгоритми на основі факторизації великих чисел. Квантові алгоритми, зокрема алгоритм Шора, здатні ефективно розкладати великі числа на прості множники, що робить традиційні криптографічні системи вразливими до атак. Це має суттєвий вплив на вибір шрифтів для криптографічних алгоритмів, оскільки необхідно забезпечити стійкість не лише до класичних атак, а й до нових квантових загроз.[23]

У цьому контексті важливим аспектом є впровадження квантово-стійких шрифтів, які здатні ускладнювати криптоаналіз, навіть за умови використання квантових комп'ютерів. Вибір шрифтів для криптографії в умовах квантової ери повинен бути орієнтований на створення таких шрифтів, які можуть витримувати новітні атаки з боку квантових обчислювальних систем, здатних до високопродуктивної обробки інформації. Це може включати використання шрифтів із більш складними геометричними властивостями, змінними

параметрами символів або складними шрифтами, що ускладнюють задачу їх дешифрування.

Квантова криптографія також відкриває нові можливості для шифрування, які можуть змінити підходи до вибору шрифтів. Наприклад, одна з основних квантових технологій — квантове розподілення ключів (Quantum Key Distribution, QKD) — дозволяє здійснювати обмін криптографічними ключами з використанням квантових властивостей фотонів, що гарантує високий рівень безпеки і неможливість перехоплення ключів без виявлення цього факту. У поєднанні з квантовими шифрувальними методами це може спричинити зміну підходів до формування шрифтів, які використовуються для шифрування та дешифрування повідомлень [22].

У зв'язку з цим важливим напрямом у виборі шрифтів стане інтеграція квантових технологій і класичних криптографічних методів, що може привести до створення нових гібридних систем шифрування. Для таких систем шрифти повинні бути не лише стійкими до атак, що базуються на класичних криптографічних методах, але й здатними витримувати потенційні атаки з боку квантових комп'ютерів.

Одним з можливих рішень може бути використання шрифтів, які здатні змінювати свої характеристики в залежності від типу криптографічної операції або конкретних умов обміну даними, щоб ускладнити їх аналіз і зменшити ймовірність розшифрування [23], навіть при наявності квантових комп'ютерів. Крім того, шрифти, які використовують особливості квантових явищ, такі як суперпозиція чи квантова заплутаність, можуть бути важливим елементом для створення нових видів шифрування, що значно підвищують рівень безпеки.

Адаптація шрифтів до новітніх криптографічних стандартів є важливим напрямом у розвитку криптографії, оскільки вона дозволяє забезпечити високу безпеку шифрування та стійкість до сучасних атак. З новими криптографічними стандартами, які виникають у відповідь на зміни в технологіях шифрування, обробки даних і вимогах до захисту інформації, шрифти повинні відповідати

певним вимогам, щоб залишатися ефективними інструментами для криптографічних методів.

Перш за все, необхідно враховувати постійно змінювані вимоги до криптографічних стандартів, пов’язані з рівнем безпеки. Наприклад, у зв'язку з розвитком квантових комп'ютерів і новітніх методів криптоаналізу, багато традиційних криптографічних стандартів, таких як RSA та ECC (еліптичні криві) [23], стають вразливими до атак. У зв’язку з цим новітні стандарти шифрування орієнтуються на квантово-стійкі методи, які повинні бути здатні витримувати атаки з боку квантових комп’ютерів. У такому контексті шрифти для криптографічних алгоритмів повинні враховувати специфікації цих нових стандартів, що вимагає вдосконалення їх конструктивних і візуальних характеристик.

Шрифти для новітніх криптографічних стандартів повинні забезпечувати не лише візуальну стійкість до криптоаналізу, а й бути сумісними з новими методами шифрування, які базуються на постквантових алгоритмах. Наприклад, у зв'язку з розвитком криптографії на основі лінійних кодів або решіток, шрифт повинен бути здатним підтримувати нові типи криптографічних операцій і взаємодіяти з постквантовими криптографічними алгоритмами, що забезпечує його адаптацію до нових стандартів.

Ще одним важливим аспектом адаптації шрифтів до новітніх криптографічних стандартів є забезпечення їхньої здатності до високої швидкості обробки даних при одночасному збереженні високого рівня безпеки. Сучасні криптографічні методи все більше орієнтуються на ефективність обробки великих обсягів даних. Саме тому шрифт, який оптимізований для швидкої обробки на новітніх криптографічних платформах, може стати важливим компонентом в досягненні кращої ефективності шифрування в межах нових стандартів.

Крім того, в умовах швидкого розвитку новітніх криптографічних стандартів необхідно забезпечити гнучкість шрифтів, щоб вони могли підтримувати різні формати і протоколи шифрування, які можуть бути введені

у майбутньому. Це включає підтримку нових форматів повідомлень і алгоритмів, а також адаптацію до змінюваних умов безпеки. Шрифт, який можна адаптувати до нових умов, буде важливим інструментом у боротьбі з новими типами атак і забезпеченні стійкості криптографічних систем до різноманітних загроз.

Необхідність ускладнення візуальних характеристик шрифтів для криптографічних застосувань стає все більш очевидною у контексті розвитку криптоаналізу і зростання здатності автоматизованих систем до виявлення шаблонів у зашифрованих текстах. Завдяки розвитку таких технологій, як машинне навчання і штучний інтелект, сучасні криптоаналітики мають змогу швидко аналізувати великі обсяги даних, виявляючи навіть найменші закономірності, які можуть бути використані для дешифрування. Тому забезпечення високої стійкості шрифтів до криптоаналізу є критично важливим, і однією з основних стратегій для цього є ускладнення візуальних характеристик шрифтів.

По-перше, шрифти з рівними або простими формами символів (наприклад, стандартні шрифти без засічок) мають чітку структуру, що дозволяє ефективно використовувати методи статистичного аналізу для розпізнавання частотних шаблонів або специфічних елементів, які можна виявити в зашифрованому тексті. Щоб ускладнити цю задачу, шрифт повинен мати більше варіацій у своїх символах. Це можуть бути шрифти з нерівними пропорціями літер, де одна буква може бути ширшою або вищою за іншу, що робить складнішим розпізнавання частотних шаблонів у тексті. Такі варіації додають складність, оскільки навіть якщо криптоаналітик намагається застосувати частотний аналіз, йому буде важче виявити закономірності, порівнюючи різні символи.

Додатково, варіації в товщині ліній, незвичні пропорції шрифтів або навіть змішування різних стилів у межах одного тексту можуть зробити навіть найпростіші криптоаналізи менш ефективними. Наприклад, шрифт, у якому одна частина літери має більшу товщину ліній, а інша — тоншу, може створити

значні труднощі для традиційних криптоаналітичних технік, таких як порівняння частот та характерних елементів. Це дозволяє зменшити ймовірність успішної атаки, оскільки аналізатор буде змушений враховувати більше варіантів для кожного символу.

Ще одним методом ускладнення є використання шрифтів, що мають складні, асиметричні форми літер. Символи, що виглядають схожими на базові латинські або кириличні букви, але мають незвичні лінії, додаткові елементи чи асиметричні деталі, можуть значно збільшити труднощі для автоматизованих систем, що намагаються зламати шифр.

Важливою стратегією є також застосування шрифтів з варіативними елементами, які змінюються залежно від контексту використання або від параметрів шифрування. Наприклад, шрифт, який змінює свою форму в залежності від певних криптографічних параметрів або навіть випадкових факторів, може значно ускладнити криптоаналіз. У такому випадку кожне повідомлення буде виглядати по-різному навіть при використанні однакових символів, що робить його набагато складнішим для розшифрування.

Не менш важливим є застосування шрифтів, що мають нетипові елементи в своїй структурі. Наприклад, букви, що мають нестандартні з'єднання або позначки, можуть створити враження на перший погляд важливих деталей, які насправді є випадковими елементами шрифту. Це може заплутати навіть досвідчених криптоаналітиків, змушуючи їх витрачати час на вивчення непотрібних частин шрифту.

Ускладнення візуальних характеристик шрифтів є необхідним етапом для забезпечення високого рівня безпеки криптографічних систем. Завдяки застосуванню складних, нерівних, асиметричних, варіативних та нестандартних шрифтів можна значно ускладнити криптоаналіз, знизивши ймовірність успішних атак і підвищивши загальний рівень захисту зашифрованої інформації.

Перспективи використання адаптивних шрифтів у майбутніх криптографічних системах відкривають нові горизонти для підвищення безпеки

та ефективності шифрування. Адаптивні шрифти мають потенціал не лише для вдосконалення існуючих методів шифрування, але й для створення нових підходів до захисту інформації в умовах постійно змінюваного криптографічного середовища.

Однією з основних переваг адаптивних шрифтів є їх здатність до динамічної зміни характеристик в залежності від параметрів криптографічної операції. Це означає, що шрифт може адаптуватися під конкретні умови шифрування, що ускладнює використання стандартних криптоаналітичних методів. Наприклад, в залежності від ключа шифрування або алгоритму, шрифт може змінювати товщину ліній, висоту літер або навіть форму символів, що робить процес дешифрування складнішим для криптоаналітика, оскільки він повинен враховувати змінні властивості кожного символу.

Адаптивні шрифти можуть використовуватися для реалізації так званих «самооновлюваних» шифрів. У таких системах шрифт може змінювати свої властивості в реальному часі, роблячи текст непередбачуваним для сторонніх осіб. Цей підхід може бути особливо корисним для захисту інформації в умовах, де ключі шифрування можуть бути втрачені або перехоплені. Оскільки адаптивні шрифти постійно змінюються, навіть якщо ключ шифрування потрапляє до злому, шрифт, використовуваний для створення тексту, все одно залишатиметься змінним і стійким до розшифровки.

Ще однією перспективою є використання адаптивних шрифтів в контексті зберігання і передачі великих обсягів даних, особливо в мережах з високим рівнем загроз, таких як віртуальні приватні мережі (VPN) або Інтернет речей (IoT) [24]. У таких системах адаптивні шрифти можуть застосовуватися для динамічного налаштування параметрів шифрування, що дозволяє знизити ймовірність успішної атаки на конкретну точку шифрування. Вони можуть також змінювати свої характеристики в залежності від зовнішніх факторів, таких як географічне розташування, рівень загрози або наявність шкідливих програм, що дає можливість адаптувати захист до актуальних умов.

У майбутніх криптографічних системах адаптивні шрифти також можуть стати частиною систем захисту інформації з інтегрованими штучним інтелектом (ШІ) та машинним навчанням (ML). ШІ та ML можуть допомогти шрифтам адаптуватися до нових атак, змінюючи їхні характеристики в реальному часі для уникнення виявлення та дешифрування. Наприклад, якщо криптографічна система визначає, що певний тип атаки на її шифрування став успішним, вона може негайно змінити параметри шрифтів, що ускладнить повторення атаки. Така динамічність шрифтів дозволяє криптографічним системам автоматично підлаштовуватися під нові загрози, підвищуючи їхню стійкість.

Ще одним важливим аспектом є інтеграція адаптивних шрифтів у багаторівневі криптографічні системи, де вони можуть використовуватися як додатковий рівень захисту на візуальному рівні. Це дозволить знизити ймовірність того, що атаки на рівень шифрування будуть успішними, оскільки кожен рівень шифрування буде мати свої власні, змінювані шрифтові характеристики. Крім того, шрифти можуть варіюватися залежно від типу переданих даних, надаючи більше гнучкості та точності у забезпеченні безпеки.

Адаптивні шрифти мають величезний потенціал для майбутніх криптографічних систем, пропонуючи нові способи підвищення безпеки, ефективності та стійкості до атак. Вони можуть забезпечити більш високий рівень захисту, адаптуючись до змінюваних загроз і вимог, що дозволяє створювати криптографічні системи, які не тільки відповідають сучасним стандартам безпеки, але й здатні передбачити та відреагувати на новітні виклики криптоаналізу та технологічного розвитку.

ВИСНОВКИ

У ході проведеного дослідження було розглянуто важливість вибору шрифтів для аналогового криптографічного перетворення даних. Визначено, що шрифти мають значний вплив на ефективність криптографічних операцій та стійкість систем до атак. Особливу увагу було приділено характеристикам шрифтів, таким як засічки, варіації накреслень та жирності, а також візуальні особливості, які можуть ускладнити процес криптоаналізу.

Обґрунтовано важливість використання шрифтів з нерівними пропорціями букв, що створює додаткові труднощі для автоматизованих систем, що здійснюють криптоаналіз. Зроблено висновок, що для забезпечення високого рівня безпеки необхідно обирати шрифти, які дозволяють ускладнити застосування методів частотного аналізу та інших класичних криптоаналітичних технік.

В ході тестування придатності шрифтів було виявлено, що адаптивні шрифти, які змінюють свої характеристики в залежності від криптографічних параметрів, мають значний потенціал для підвищення стійкості до атак. Найкращі результати продемонстрував шрифт Open Sans, який зберігав високу читабельність та стабільність форми в усіх тестових ситуаціях. Його поведінка при накладенні шуму, зміні стилів та під час симуляції умов дешифрування залишалася передбачуваною, що свідчить про високу придатність до застосування в криптографічному контексті. Шрифти Calibri, Arial та Roboto, які також отримали високу підсумкову оцінку (9/10), можуть ефективно використовуватись у більшості графічних сценаріїв. Водночас, під час роботи з ними слід враховувати певні нюанси. Наприклад, Arial втрачає частину деталей при сильному розмитті, а Calibri менш чітко передає стилі при мінімальному масштабі. Такі шрифти можуть бути інтегровані з новітніми криптографічними технологіями, такими як квантова криптографія, що дозволить забезпечити додатковий рівень захисту для інформаційних систем майбутнього.

Також було визначено перспективи розвитку криптографічних систем за допомогою адаптації шрифтів до змінюваних умов криптоаналізу та загроз. Це

дозволяє створити більш гнучкі та стійкі до атак системи шифрування, що відповідають сучасним вимогам безпеки.

Отже, поставленої мети було досягнуто.

Вибір та адаптація шрифтів є важливим елементом для забезпечення ефективного захисту інформації в аналогових криптографічних системах. Приділення належної уваги візуальним характеристикам шрифтів, а також їх адаптація до новітніх криптографічних стандартів, є необхідним кроком для покращення безпеки шифрування та зниження ймовірності успішних атак на систему.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Katz J., Lindell Y. Introduction to Modern Cryptography. – 2nd ed. – Chapman and Hall/CRC, 2015. – 603 p.

2. National Institute of Standards and Technology. Advanced Encryption Standard (AES): FIPS PUB 197. – Gaithersburg, MD, 2001. – 51 p.

3. National Institute of Standards and Technology. Recommendation for Key Management: Part 1 – General: NIST Special Publication 800-57 Part 1 Rev. 5. – 2020. – 142 p.

4. Kocher P., Jaffe J., Jun B. Differential Power Analysis // Advances in Cryptology – CRYPTO'99. – Lecture Notes in Computer Science, vol. 1666. – Springer, 1999. – P. 388–397.

5. National Institute of Standards and Technology. Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process: NISTIR 8413. – 2022. – 46 p.

6. Ferguson N., Schneier B., Kohno T. Cryptography Engineering: Design Principles and Practical Applications. – Wiley Publishing, 2010. – 384 p.

7. Stallings W. Cryptography and Network Security: Principles and Practice. 7th ed. Boston: Pearson, 2017. 840 p.

8. Menezes A. J., van Oorschot P. C., Vanstone S. A. Handbook of Applied Cryptography. Boca Raton: CRC Press, 2018. 810 p.

9. Diffie W., Hellman M. New Directions in Cryptography // IEEE Transactions on Information Theory. 1976. Vol. 22, No. 6. P. 644–654.

10. NIST Special Publication 800-57 Part 1 Revision 5. Recommendation for Key Management: Part 1 – General. Gaithersburg: National Institute of Standards and Technology, 2020. 142 p.

11. Barker E. Recommendation for Key Management – Part 2: Best Practices for Key Management Organization. NIST Special Publication 800-57 Part 2 Revision 1. Gaithersburg: National Institute of Standards and Technology, 2019. 79 p.

12. Hölzl M., Kemmerer R., Kossakowski K.-P. Cloud Key Management: A Literature Review // Journal of Cloud Computing. 2020. Vol. 9, No. 1. P. 1–17.

13. ISO/IEC 11770-1:2015. Information technology – Security techniques – Key management – Part 1: Framework. Geneva: International Organization for Standardization, 2015. 18 p.

14. Aumasson J.-P. Serious Cryptography: A Practical Introduction to Modern Encryption. San Francisco: No Starch Press, 2017. 312 p.

15. Боклаг, Д. М., Громико, І. О. Шрифти в аналоговій криптографії / Д. М. Боклаг, І. О. Громико – Харків: Харківський національний університет імені В. Н. Каразіна, 2025.

16. Ніконов, С. П. Теорія криптографії / С. П. Ніконов. — Київ : Вища школа, 2015. — 432 с.

17. Мішин, І. В. Методи криптографії та їх застосування / І. В. Мішин. — Львів : Наука і техніка, 2016. — 214 с.

18. Криптографія в комп’ютерних системах: підручник / за ред. В. М. Шарова. — Харків : Фоліо, 2017. — 340 с.

19. Black, J. The Handbook of Applied Cryptography / J. Black, A. Menezes, P. van Oorschot. — 2nd ed. — Boca Raton : CRC Press, 2019. — 1072 p.

20. Мінц, В. П. Алгоритми та структури даних: підручник / В. П. Мінц. — Київ : Наукова думка, 2018. — 360 с.

21. Шарова, В. М. Криптографія в інформаційних системах / В. М. Шарова, І. І. Голосніченко. — Одеса : ОНУ, 2020. — 215 с.

22. Горбенко, І. Д. Криптологія. Теорія. Практика. Застосування: монографія / І. Д. Горбенко, Ю. І. Горбенко – Краматорськ: ДДМА, 2019. – 326 с.

23. Щербина, В. А. Комп’ютерна криптографія: навч. посібник / В. А. Щербина – Харків: ХНУРЕ, 2015. – 284 с.

24. Xiao, C., Zhang, C., Zheng, C. FontCode: Embedding Information in Text Documents using Glyph Perturbation // ACM TOG, 2018.

ДОДАТОК А

```
import tkinter as tk
from tkinter import ttk
from PIL import Image, ImageDraw, ImageTk, ImageFont,
ImageFilter
import numpy as np
import random
import os

# Автоматично шукаємо всі ttf шрифти в папці
font_options = [f for f in os.listdir() if
f.lower().endswith(".ttf")]
if not font_options:
    font_options = ["arial.ttf"]

# Функція підбору шрифту зі стилем
def get_font_path(base_font, style):
    name, ext = os.path.splitext(base_font)
    style_suffix = {
        "normal": "",
        "bold": "bd",
        "italic": "i",
        "bold italic": "bi"
    }
    styled_font = f"{name}{style_suffix[style]}{ext}"
    if os.path.exists(styled_font):
        return styled_font
    else:
        return base_font  # fallback

# Функція генерації зображення з текстом і шумом
def generate_image(text, font_name, font_size, style,
noise_level, noise_type, blur_amount, simulate):
    width, height = 700, 250
    image = Image.new("RGB", (width, height), "white")
    draw = ImageDraw.Draw(image)

    font_path = get_font_path(font_name, style)
    try:
        font = ImageFont.truetype(font_path, font_size)
    except:
```

```
        font = ImageFont.load_default()

    text_bbox = draw.textbbox((0, 0), text, font=font)
    text_width = text_bbox[2] - text_bbox[0]
    text_height = text_bbox[3] - text_bbox[1]
    position = ((width - text_width) // 2, (height -
text_height) // 2)

    draw.text(position, text, fill="black", font=font)

    pixels = image.load()

    if noise_type in ['Точки', 'Комбінований']:
        for _ in range(noise_level * 20):
            x, y = random.randint(0, width-1),
random.randint(0, height-1)
            color = tuple(np.random.randint(0, 255, 3))
            draw.ellipse((x, y, x+4, y+4), fill=color)

    if noise_type in ['Лінії', 'Комбінований']:
        for _ in range(noise_level * 3):
            x1, y1 = random.randint(0, width),
random.randint(0, height)
            x2, y2 = random.randint(0, width),
random.randint(0, height)
            color = tuple(np.random.randint(0, 255, 3))
            draw.line((x1, y1, x2, y2), fill=color,
width=2)

    if noise_type in ['Сітка', 'Комбінований']:
        step = max(10, 200 // max(1, noise_level))
        for i in range(0, width, step):
            draw.line((i, 0, i, height),
fill="lightgray")
        for j in range(0, height, step):
            draw.line((0, j, width, j), fill="lightgray")

    if blur_amount > 0:
        image =
image.filter(ImageFilter.GaussianBlur(blur_amount))

    if simulate:
```

```
        overlay = Image.new("RGB", (width, height), (255,
255, 255))
        for _ in range(noise_level * 5):
            x, y = random.randint(0, width-1),
random.randint(0, height-1)
            overlay.putpixel((x, y), (random.randint(0,
255), random.randint(0, 255), random.randint(0, 255)))
        image = Image.blend(image, overlay, 0.3)

    return image

# Оновлення зображення
def update_image(*args):
    text = text_entry.get()
    font_name = font_var.get()
    font_size = size_var.get()
    style = style_var.get()
    noise_level = noise_var.get()
    noise_type = noise_var_type.get()
    blur_amount = blur_var.get()
    simulate = simulate_var.get()

    image = generate_image(text, font_name, font_size,
style, noise_level, noise_type, blur_amount, simulate)
    img_tk = ImageTk.PhotoImage(image)
    canvas.config(width=image.width, height=image.height)
    canvas.create_image(0, 0, anchor="nw", image=img_tk)
    canvas.image = img_tk

# Головне вікно
root = tk.Tk()
root.title("Crypto Text Visualizer — Desktop + Стиль")

# Поле для тексту
text_entry = tk.Entry(root, width=40)
text_entry.insert(0, "Введіть текст")
text_entry.pack(pady=5)
text_entry.bind("<Return>", update_image)

# Вибір шрифту
font_var = tk.StringVar(value=font_options[0])
```

```
font_menu = ttk.Combobox(root, textvariable=font_var,
values=font_options)
font_menu.pack()

# Вибір стилю
style_var = tk.StringVar(value="normal")
style_menu = ttk.Combobox(root, textvariable=style_var,
values=["normal", "bold", "italic", "bold italic"])
style_menu.pack()

# Повзунок розміру
size_var = tk.IntVar(value=50)
size_slider = tk.Scale(root, from_=10, to=150,
orient="horizontal", label="Розмір", variable=size_var,
command=update_image)
size_slider.pack(fill='x', padx=10)

# Повзунок щільності шуму
noise_var = tk.IntVar(value=20)
noise_slider = tk.Scale(root, from_=0, to=100,
orient="horizontal", label="Щільність шуму",
variable=noise_var, command=update_image)
noise_slider.pack(fill='x', padx=10)

# Вибір типу шуму
noise_var_type = tk.StringVar(value="Точки")
noise_menu = ttk.Combobox(root,
textvariable=noise_var_type, values=["Точки", "Лінії",
"Сітка", "Комбінований"])
noise_menu.pack()

# Повзунок розмиття
blur_var = tk.DoubleVar(value=0.0)
blur_slider = tk.Scale(root, from_=0, to=10,
resolution=0.5, orient="horizontal", label="Розмиття",
variable=blur_var, command=update_image)
blur_slider.pack(fill='x', padx=10)

# Симуляція дешифрування
simulate_var = tk.BooleanVar()
```

```
simulate_check = tk.Checkbutton(root, text="Симуляція
дешифрування", variable=simulate_var,
command=update_image)
simulate_check.pack()

# Полотно для зображення
canvas = tk.Canvas(root, width=700, height=250)
canvas.pack()

# Старт
update_image()

# Запуск
root.mainloop()
```