МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

Спеціальність: 123 «Комп'ютерна інженерія»

Освітньо-професійна програма: «Комп'ютерна інженерія»

Група: 2БКС-29

КВАЛІФІКАЦІЙНА РОБОТА

здобувача освіти денної форми навчання

БКС.29.16.000.КРБ

МОЙСЄЄВА ВІКТОРА ВІКТОРОВИЧА

м. Одеса
2025 р.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

Спеціальність: **123 «Комп'ютерна інженерія»**
Освітньо-професійна програма: **«Комп'ютерна інженерія»**
Група: **2БКС-29**

ПОЯСНЮВАЛЬНА ЗАПИСКА

До кваліфікаційної роботи бакалавра на тему: **«Аналіз сучасних криптографічних алгоритмів та їх ефективності у захисті конфіденційної інформації»**

Проектний матеріал складається з пояснювальної записки на 61 сторінках та графічного (презентаційного) матеріалу на 12 аркушах (слайдах)

Виконавець _____ (Мойсєєв В.В.)
Керівник проекту _____ (Кільдішев В.Й.)

Консультанти:
з розділу охорони праці та техніки безпеки _____ (Чорновол Н.І.)
з нормоконтролю _____ (Петрашова В.І.)
старший консультант _____ (Кривченко Ю.В.)

До захисту допущений
Завідувач кафедри _____ (Іванова Л.В.)
Завідувач відділенням _____ (Краснокутська К.Г.)

Захист «25» 06 2025 р. Протокол ЕК № 1
Оцінка ЕК 5 (відмінно) / 90

Секретар ЕК _____

АНОТАЦІЯ

Метою даної роботи є аналіз сучасних криптографічних алгоритмів та оцінка їх ефективності щодо забезпечення захисту конфіденційної інформації в умовах зростання кіберзагроз і підвищених вимог до інформаційної безпеки.

Вивчено закономірності функціонування блочних та потокових шифрів, зокрема AES-128, AES-256, а також національного алгоритму «Калина». Досліджено особливості застосування цих алгоритмів у різних режимах шифрування, а також їхню стійкість до сучасних типів криптоаналітичних атак.

Отримані кількісні результати експериментального тестування шифрування і розшифрування, що дали змогу порівняти швидкодію та ресурсну ефективність алгоритмів. Визначено переваги AES-256 у плані продуктивності в певних умовах, незважаючи на його вищу криптографічну складність.

Створено програмне забезпечення для практичного дослідження криптографічних алгоритмів із можливістю вимірювання часу обробки даних та інтерактивного введення інформації. Реалізовано тестові сценарії для оцінювання ефективності методів шифрування у різних режимах.

Розглянуто питання з охорони праці та техніки безпеки при роботі з комп’ютерною технікою під час виконання досліджень, зокрема дотримання ергономічних вимог, норм електробезпеки та правил організації безпечного інформаційного середовища.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

Відділення *Комп'ютерних систем* Кафедра *Комп'ютерної інженерії*

Спеціальність *123 «Комп'ютерна інженерія»*

Освітньо-професійна програма *«Комп'ютерна інженерія»*

ЗАТВЕРДЖУЮ:

Заст. дир. з НВР *Беркань І.В.*

"28" 05 2025 р.

ЗАВДАННЯ

на кваліфікаційну роботу бакалавра

здобувачеві освіти *Мойсєєва Віктора Вікторовича*

(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи *Аналіз сучасних криптографічних алгоритмів та їх ефективності у захисті конфіденційної інформації*

затверджена наказом по коледжу від "14" листопада 2025 р. №246

2. Термін здачі студентом кваліфікаційної роботи

3. Вихідні дані до роботи *1. Порівняння швидкодії, стійкості до атак та використання ресурсів; 2. Методики оцінки криптостійкості алгоритмів; 3. Аналіз загроз та атак на сучасні алгоритми шифрування; 4. Рекомендації щодо вибору криптографічних методів для захисту інформації*

4. Зміст розрахунково-пояснювальної записки (перелік питань, що їх належить розробити)

Огляд стандартів шифрування та їх застосування у сучасних інформаційних системах; Аналіз сучасних криптографічних алгоритмів; Оцінка ефективності криптографічних алгоритмів у захисті конфіденційної інформації; Аналіз загроз та атак на сучасні алгоритми шифрування

5. Перелік графічного матеріалу (слайдів мультимедійної презентації) *Класифікація криптографічних алгоритмів; Порівняльний аналіз ефективності симетричних алгоритмів шифрування; Відмінності системи шифрування Калина від AES; Порівняльний аналіз ефективності асиметричних алгоритмів шифрування; Класифікація атак на алгоритми шифрування; Порівняльна характеристика систем шифрування; Загальні результати тестування систем шифрування AES 128 і AES 256 ; Показники основних криптографічних алгоритмів за трьома критеріями: швидкодія, стійкість до атак і використання ресурсів*

6. Консультанти по кваліфікаційній роботі, із зазначенням розділів, що їх стосуються

Розділ	Консультант	ПІДПИС	
		Завдання видав	Завдання прийняв
Основний розділ	*Кільдішев В.Й.*		
Розділ охорони праці	*Чорновол Н.І.*		
Нормоконтроль	*Петрашова В.І.*		
Старший консультант	*Кривченко Ю.В.*		

7. Дата видачі завдання 29.04.2025

Керівник роботи *Кільдішев В.Й.* _____
(підпис)

Завдання прийняв до виконання _____
(підпис)

КАЛЕНДАРНИЙ ПЛАН

Пор. №	Назва етапів кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1.	Вступ. Аналіз технічного завдання	21.05.2025	Виконав
2.	Теоретичні основи криптографічного захисту інформації	22.05.2025	Виконав
3.	Класифікація криптографічних алгоритмів	24.05.2025	Виконав
4.	Огляд стандартів шифрування та їх застосування у сучасних інформаційних системах	26.05.2025	Виконав
5.	Аналіз сучасних криптографічних алгоритмів	28.05.2025	Виконав
6.	Аналіз ефективності асиметричних алгоритмів	30.05.2025	Виконав
7.	Порівняння швидкодії, стійкості до атак та використання ресурсів	02.06.2025	Виконав
8.	Оцінка ефективності криптографічних алгоритмів у захисті конфіденційної інформації	05.06.2025	Виконав
9.	Методики оцінки криптостійкості алгоритмів	07.06.2025	Виконав
10.	Аналіз загроз та атак на сучасні алгоритми шифрування	09.06.2025	Виконав
11.	Рекомендації щодо вибору криптографічних методів для захисту інформації	10.06.2025	Виконав
12.	Розробка питань з охорони праці та техніки безпеки	12.06.2025	Виконав
13.	Підготовка матеріалів мультимедійної презентації	14.06.2025	Виконав

Здобувач освіти _____
(підпис)

Керівник роботи _____
(підпис)

Формат	Зона	Поз.	Позначення	Назва	Кіл.	Примітка
				Документація		
			БКС 29. 16 000. 00 КРБ	Випускна робота		
А4			БКС 29. 16 000. 00 КРБ ПЗ	Пояснювальна записка	1	

Зм.	Арк.	№ докум.	Підпис	Дата	БКС 29. 16 000. 00 КРБ		
Розробив		Мойсєєв В.В,			Аналіз сучасних криптографічних алгоритмів та їх ефективності у захисті конфіденційної інформації	Літ.	Аркуш 4 / Аркушів 61
Перевірив		Кільдішев В.Й.				НДП	
Н. Контр.		Петрашова В.І.				ВСП "ОТФК ОНТУ" гр.2БКС-29	
Затверд.		Іванова Л.В.					

ЗМІСТ

ВСТУП

У сучасному цифровому світі питання захисту конфіденційної інформації набуває особливої актуальності. Зростаючий обсяг даних, які передаються та зберігаються у відкритих інформаційних системах, потребує надійних методів криптографічного захисту. Кіберзлочинність, хакерські атаки та витоки даних є серйозними викликами для організацій, державних установ та звичайних користувачів. Тому дослідження сучасних криптографічних алгоритмів і оцінка їхньої ефективності є важливим завданням для забезпечення інформаційної безпеки.

Розвиток інформаційних технологій супроводжується вдосконаленням як методів шифрування, так і способів їх злому. Традиційні алгоритми, такі як DES і RSA, поступово замінюються більш надійними та швидкими методами, зокрема AES, ECC та постквантовими алгоритмами. Проте вибір оптимального методу захисту залежить від багатьох факторів: швидкодії, стійкості до атак, вимог до апаратних ресурсів. Аналіз сучасних криптографічних алгоритмів дозволить визначити їхні переваги та недоліки, що є важливим для створення ефективних механізмів захисту даних.

Метою роботи є аналіз сучасних криптографічних алгоритмів та оцінка їхньої ефективності для захисту конфіденційної інформації.

Для досягнення цієї мети в роботі поставлено такі завдання:

- дослідити основні принципи та класифікацію криптографічних алгоритмів;
- проаналізувати ефективність сучасних методів шифрування;
- оцінити криптостійкість алгоритмів та їхню здатність протистояти атакам;
- розробити рекомендації щодо вибору криптографічних методів залежно від сфери їх застосування.

Об’єктом дослідження є сучасні криптографічні алгоритми. Предметом дослідження є ефективність криптографічних методів у захисті конфіденційної інформації.

1 ОСНОВНИЙ РОЗДІЛ

1.1 Теоретичні основи криптографічного захисту інформації

1.1.1 Історичний огляд розвитку криптографічних протоколів»

Історія криптографії починається з давніх часів, коли люди намагалися захистити свої повідомлення від сторонніх. Одним із найдавніших методів була шифрування Цезаря — простий метод заміни, що зсуває літери алфавіту на фіксовану кількість позицій. У Стародавній Греції використовували скітали – спеціальні циліндри для шифрування військових повідомлень. Подібні методи з часом ускладнювались, але залишались досить простими й ручними.

У середньовіччі криптографія використовувалась переважно для дипломатичної та військової кореспонденції. Одним із видатних прикладів є шифр Віженера (XVI ст.) – поліалфавітний метод шифрування, який вважався незламним протягом кількох століть. Цей період заклав основи систематичного підходу до створення шифрів, хоча криптографія ще не була формалізованою наукою.

Під час Першої та Другої світових воєн криптографія зробила величезний стрибок у розвитку. Особливо відома машина Enigma, яку використовувала нацистська Німеччина. Її зламали союзники завдяки роботі Алана Тюрінга та інших криптоаналітиків. З цього моменту криптографія починає стрімко еволюціонувати як дисципліна, заснована на математиці та логіці.

Слід відзначити період 1970–1980-ті роки як становлення сучасної криптографії.

У 1976 році було опубліковано роботу Вітфілда Діффі та Мартіна Геллмана, у якій запропоновано метод відкритого обміну ключами, що започаткував еру асиметричної криптографії. У 1977 році з’явився алгоритм RSA, заснований на труднощах факторизації великих чисел. Це дало змогу

створювати надійні криптографічні протоколи, які не вимагали попереднього обміну секретами.

Паралельно в 1977 році США затверджують DES (Data Encryption Standard) як державний стандарт симетричного шифрування, що згодом був замінений на більш стійкий AES (Advanced Encryption Standard) у 2001 році.

Для XXI століття характерним є протоколи безпечного обміну в цифрову епоху.

З розповсюдженням Інтернету та мобільних технологій зросла потреба в розробці криптографічних протоколів, які можуть забезпечити захист інформації в реальному часі. З'являються SSL/TLS, IPSec, PGP, Signal Protocol та інші, які реалізують захищені з'єднання, електронний підпис, автентифікацію та шифрування повідомлень.

Також зростає інтерес до квантової криптографії, яка базується на законах квантової фізики і може забезпечити принципово новий рівень захисту.

Таким чином, еволюція криптографії від простих методів до складних математичних протоколів відображає розвиток потреб у безпеці даних. Сьогодні криптографічні протоколи — це серцевина безпечних комунікацій, без яких неможливе існування електронної комерції, електронного врядування та конфіденційного зв'язку.

Розвиток криптографії тісно пов'язаний із прогресом обчислювальної техніки. Основні особливості цього розвитку пов'язані з наступними епохами:

1) механічної;

2) електромеханіки;

3) цифрова;

4) Інтернет та мережеві протоколи;

5) мобільні пристрої та IoT;

6) квантова;

Механічна епоха (до 1940-х років), за якої було характерним наступне:

– використання інструментів – прості ручні та механічні пристрої (наприклад, шифр Цезаря, скитала, шифрувальні таблиці);

– мала обчислювальна складність, основний фокус – на секретності алгоритму.

Епоха електромеханіки (1930–1940-ті) за якої використовували:

– пристрій – машина Енігма (Німеччина, Друга світова війна);

– значення – вперше криптографія почала вимагати аналізу із застосуванням технічних засобів (наприклад, машин "Бомба" або "Колоссус").

Для цифрової епохи характерним є поява комп’ютерів (1950–1970-ті), що дало:

– появу нових можливостей – цифрові обчислення дозволили реалізовувати складні алгоритми;

– появу нових алгоритмів – створення DES (1977), RSA (1977);

– парадигма – з’явився принцип “секретність повинна базуватись на ключі, а не на алгоритмі” (принцип Керкгоффса).

Наступний період пов’язаний з Інтернет та мережевими протоколами (1980–2000-ті):

– потреби – захист інформації в комп’ютерних мережах;

– протоколи – SSL/TLS, IPSec, PGP, SSH;

– алгоритми – удосконалення асиметричної криптографії, перехід до ECC.

Наступний період пов’язаний з мобільними пристроями та IoT (2010-ті):

– з’явилися проблеми, щщо пов’язані з обмеженими ресурсами пристроїв, тобто потреба в легких алгоритмах (наприклад, ECC, ChaCha20);

– безпечні месенджери – поява Signal Protocol (end-to-end шифрування, forward secrecy).

Квантова епоха (2020-ті і далі) виявило наступне:

– з’явилися загрози – квантові комп’ютери можуть зламати RSA та ECC (алгоритм Шора);

– реакція – розробка постквантових алгоритмів (Kyber, NTRU, McEliece);

– нова криптографія: квантова криптографія (Quantum Key Distribution – QKD).

На рис. 1.1 наведено залежності зростання довжини ключів для різних криптографічних алгоритмів (RSA, AES, ECC).

Ця діаграма, що ілюструє зростання довжини ключів для різних криптографічних алгоритмів (RSA, AES, ECC) у відповідь на розвиток обчислювальної техніки та зростання потреб у безпеці:

– RSA – довжина ключа постійно зростає через підвищення обчислювальних потужностей, які дозволяють ефективніше зламувати старі ключі.

– AES – має сталі довжини ключів (128, 192, 256 біт), але в практиці застосування поступово переходять до більш довгих ключів (256 біт).

– ECC (еліптична криптографія) – почала активно використовуватись після 2000 року, забезпечуючи сильний захист при меншій довжині ключа у порівнянні з RSA.

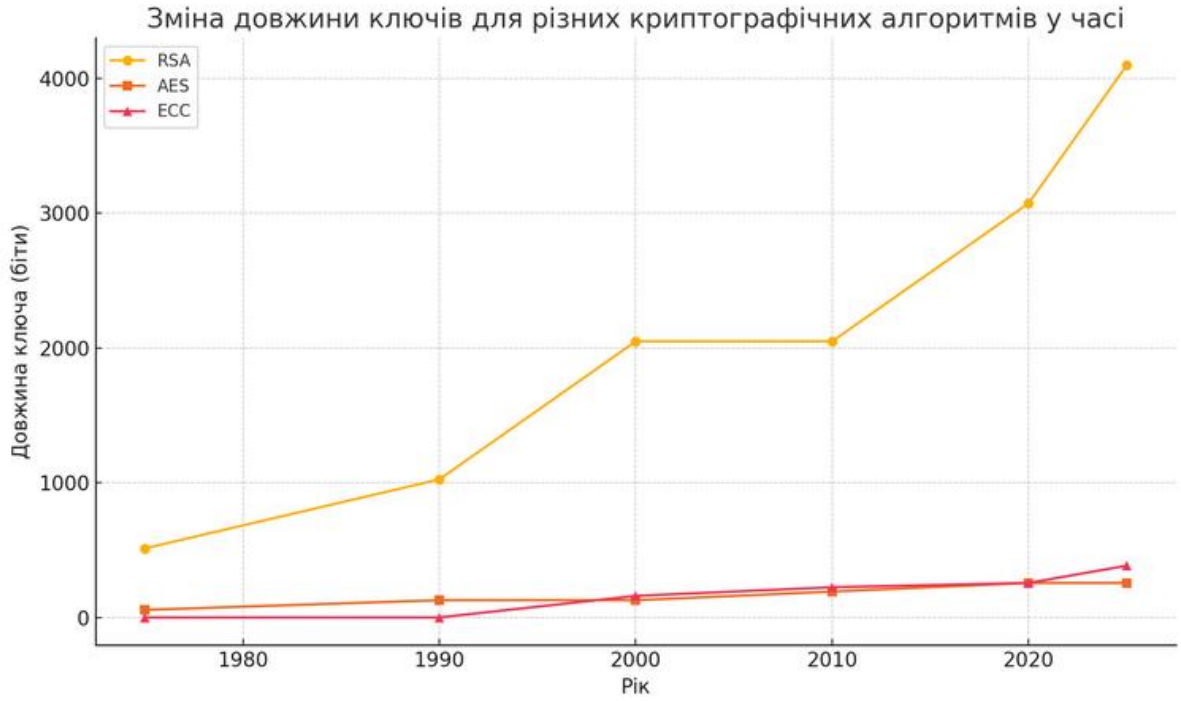


Рисунок 1.1 Залежності зростання довжини ключів для різних криптографічних алгоритмів (RSA, AES, ECC)

Цей графік ілюструє ключову тенденцію: із розвитком обчислювальної техніки криптографічні протоколи еволюціонують, збільшуючи складність алгоритмів і довжину ключів для збереження належного рівня захисту.

Розглянемо огляд розвитку криптографії в Україні, зосереджений на основних етапах і особливостях:

1) Довоєнний період та часи СРСР:

– до 1991 року криптографія в Україні розвивалася в межах СРСР, де всі роботи у цій сфері були суворо засекречені;

– основні дослідження здійснювались у структурах КДБ, а також у військових установах — зокрема в Києві, Харкові та Львові;

– українські науковці брали участь у створенні шифрувальних пристроїв та методик, однак вся діяльність була централізована в Москві.

2) Незалежна Україна (з 1991 року):

– після здобуття незалежності виникла потреба у створенні власної національної криптографічної школи;

– у 1994 році було утворено Державну службу спеціального зв’язку та захисту інформації України (ДССЗЗІ), яка стала відповідальною за розвиток і регулювання криптографії;

– з'явились вітчизняні криптоалгоритми, наприклад:

  - DSTU 4145-2002 – аналог ECC;
  - DSTU GOST 28147-2009 – симетричне шифрування;
  - DSTU 7624:2014 – сучасний блочний шифр "Каліна", частково орієнтований на AES.

3) Академічний розвиток:

– починаючи з 2000-х років, кафедри інформаційної безпеки у вишах (КПІ, Харківський політехнічний, Львівська політехніка) почали активно досліджувати криптографію;

– розвиваються напрямки:

  - квантова криптографія;
  - хаотичні сигнали;

- стеганографія та гібридні методи захисту.

4. Інтеграція з міжнародними стандартами:

– Україна поступово адаптує міжнародні криптографічні стандарти (AES, RSA, ECC, PQC) у свої державні норми:

– З 2020-х років відбувається перехід на постквантові алгоритми (NIST PQC), особливо в сфері оборони та державних систем.

5) Сучасний стан і війна:

– після 2014 року та особливо з 2022 року зростає увага до кібербезпеки та криптографічного захисту даних в умовах воєнного часу;

– з'явилися стартапи, що працюють над власними рішенями, а також тісна співпраця з європейськими та американськими компаніями;

– Україна активно бере участь у програмі Digital NATO Interoperability, де криптозасоби є критично важливими.

В табл. 1.1 наведено основні етапи розвитку криптографії в Україні.

Таблиця 1.1 Основні етапи розвитку криптографії в Україні

Період	Події та особливості
До 1991	Засекречені роботи в рамках СРСР
1991–2000	Формування національного криптонапрямку
2000–2010	Впровадження державних стандартів (DSTU)
2010–2020	Розвиток академічних досліджень, інтеграція зі світом
2020–до тепер	Впровадження постквантових алгоритмів, війна

1.1.2 Основні поняття криптографії та принципи захисту даних

Криптографія – це наука про методи перетворення інформації з метою забезпечення її конфіденційності, цілісності та автентичності. Основною метою криптографії є захист даних від несанкціонованого доступу та можливих загроз під час їхнього зберігання або передавання.

Сучасна криптографія базується на математичних алгоритмах та обчислювальних методах, що забезпечують безпеку даних. Основними завданнями криптографії є: конфіденційність; цілісність; автентифікація; незаперечність.

Конфіденційність спрямована на забезпечення доступу до інформації лише для авторизованих користувачів. Цілісність призначена для гарантування того, що дані не були змінені під час передавання або зберігання. Автентифікація використовується для підтвердження особи або джерела інформації. Незаперечність – це неможливість відмови від факту передавання або отримання інформації. Для ефективного захисту інформації криптографія використовує такі поняття: шифрування; розшифрування; криптографічний ключ; атаки на криптосистеми; криптостійкість. Шифрування є процес перетворення відкритого тексту у зашифрований вигляд (шифротекст) за допомогою криптографічного алгоритму та ключа. Розшифрування є зворотний процес отримання відкритого тексту із зашифрованих даних за допомогою відповідного ключа. Криптографічний ключ це є секретна інформація, що використовується для шифрування та розшифрування даних. Атаки на криптосистеми реалізуються на основі методів, які використовуються зловмисниками для розкриття або модифікації інформації (наприклад, атака грубої сили, атака по сторонніх каналах, квантові атаки). Криптостійкість – це здатність алгоритму протистояти криптоаналізу та атакам протягом визначеного періоду часу.

Розробка та використання криптографічних систем ґрунтується на певних фундаментальних принципах, які забезпечують їхню надійність: Принцип керування ключами; принцип мінімізації довіри; принцип відкритої криптографії; принцип багаторівневого захисту; принцип регулярного оновлення алгоритмів та ключів. Принцип керування ключами будується на безпеці алгоритму, який значною мірою залежить від захисту ключа. Навіть найстійкіший алгоритм буде вразливим, якщо ключі передаються або зберігаються неналежним чином. Принцип мінімізації довіри полягає в необхідності мінімізувати коло осіб, які мають доступ до криптографічних

ключів і механізмів захисту. Принцип відкритої криптографії (принцип Керкгоффса) полягає в тому, що безпека криптосистеми не повинна залежати від секретності алгоритму, а лише від секретності ключа. Принцип багаторівневого захисту полягає в тому, що застосування кількох методів безпеки одночасно (наприклад, шифрування, автентифікація та контроль доступу) забезпечує більшу стійкість системи до атак. Принцип регулярного оновлення алгоритмів та ключів полягає в тому, що застарілі методи шифрування можуть ставати вразливими, тому важливо періодично оновлювати криптографічні алгоритми та змінювати ключі. Основні принципи захисту даних у криптографії надано на рис.1.2.

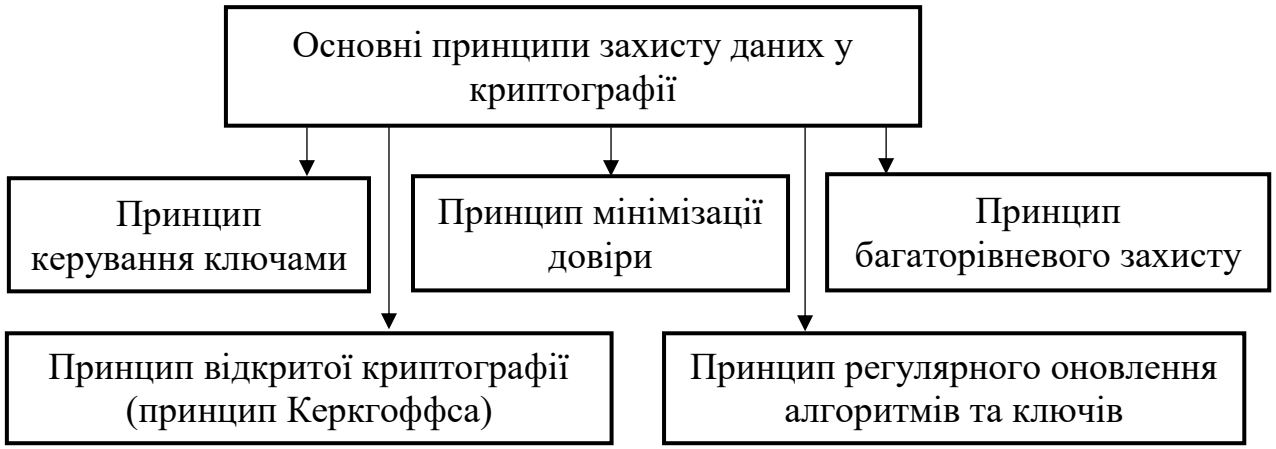


Рисунок 1.2. Основні принципи захисту даних у криптографії

Таким чином, криптографія є невід'ємною складовою сучасних інформаційних систем, забезпечуючи захист даних від несанкціонованого доступу, модифікації та підробки. Основні принципи криптографії та ефективне управління криптографічними ключами є ключовими факторами для створення надійних систем інформаційної безпеки. Подальші розділи дослідження розглянуть конкретні алгоритми та їхню ефективність у сучасних умовах.

1.1.3 Класифікація криптографічних алгоритмів

Криптографічні алгоритми відіграють ключову роль у захисті інформації від несанкціонованого доступу. Вони поділяються на кілька основних категорій залежно від принципів роботи та використання ключів. Основними типами

криптографічних алгоритмів є симетричні алгоритми, асиметричні алгоритми та алгоритми хешування.

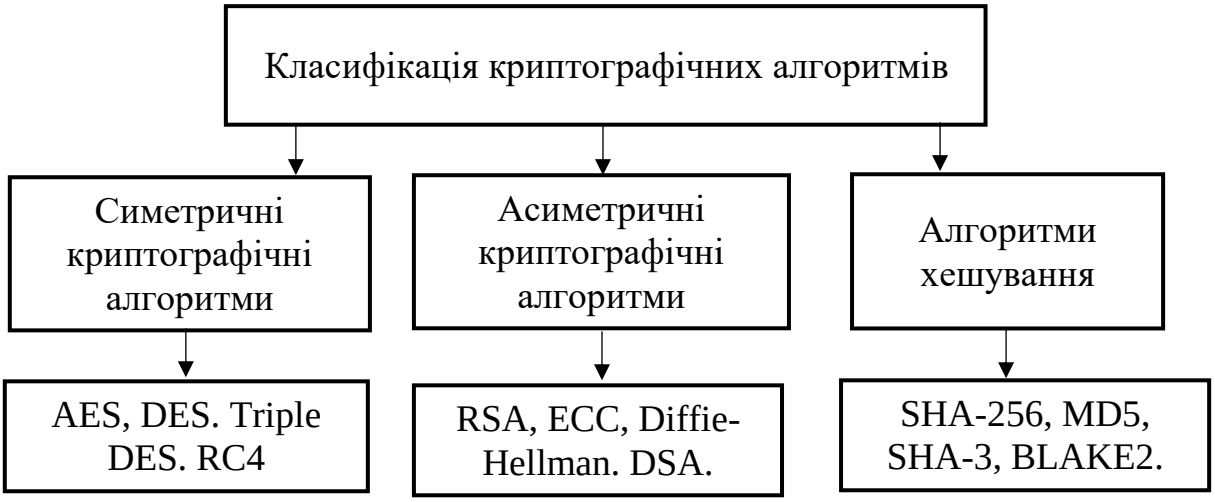


Рисунок 1.3. Класифікація криптографічних алгоритмів

Симетричні алгоритми шифрування (також відомі як алгоритми з секретним ключем) використовують один і той самий ключ як для шифрування, так і для розшифрування даних. Принцип роботи симетричних алгоритмів шифрування полягає в наступному: відкритий текст перетворюється у зашифрований (шифротекст) за допомогою секретного ключа. Для розшифрування отриманих даних застосовується той самий ключ. Перевагами таких методів є висока швидкість шифрування та розшифрування, а також менші обчислювальні витрати у порівнянні з асиметричними алгоритмами.

До недоліків слід віднести проблема безпечного розповсюдження ключів Тобто, якщо ключ скомпрометовано, всі передані дані стають вразливими. Приклади симетричних алгоритмів є: AES; DES; Triple DES; RC4.

Алгоритм AES (Advanced Encryption Standard) є сучасним стандартом шифрування, який використовується в державних і комерційних системах безпеки. Алгоритм DES (Data Encryption Standard) є застарілим алгоритмом шифрування, який нині вважається ненадійним через низьку криптостійкість. Алгоритм 3DES (Triple DES) є вдосконаленою версію DES, яка використовує потрійне шифрування для підвищення захищеності. Алгоритм RC4 є потоковим

алгоритмом шифрування, який раніше використовувався у мережевих протоколах, але нині вважається ненадійним.

Асиметричні криптографічні алгоритми (або алгоритми з відкритим ключем) використовують два різних ключі: відкритий ключ; приватний ключ. Відкритий ключ (public key) використовується для шифрування, а приватний ключ (private key) – для розшифрування. Принцип роботи асиметричних криптографічних алгоритмів полягає в наступному. Відправник шифрує повідомлення відкритим ключем отримувача. Отримувач розшифровує повідомлення за допомогою приватного ключа.

Переваги такого методу шифрування є відсутня необхідність безпечної передачі ключів між сторонами. Також цей метод забезпечує автентифікацію та цифровий підпис.

До недоліків слід віднести вищу обчислювальну складність у порівнянні з симетричними алгоритмами, а також повільніша швидкість роботи.

Приклади асиметричних алгоритмів є наступні системи шифрування: RSA; ECC; Diffie-Hellman; DSA. Алгоритм RSA (Rivest-Shamir-Adleman) є одним із найпоширеніших алгоритмів, що використовується для шифрування та цифрового підпису. Алгоритм ECC (Elliptic Curve Cryptography) – це криптографія на еліптичних кривих, що забезпечує вищу стійкість при меншій довжині ключа. Алгоритм Diffie-Hellman – це алгоритм для безпечного обміну ключами в незащищеному каналі. Алгоритм DSA (Digital Signature Algorithm) – це алгоритм, призначений для цифрових підписів.

Алгоритми хешування – це процес обчислення унікального цифрового відбитка (хеш-значення) для даних. Алгоритми хешування не є алгоритмами шифрування, оскільки вони не передбачають зворотного перетворення хешу у вихідний текст. Принцип роботи алгоритму хешування полягає в наступному. Вхідні дані обробляються алгоритмом хешування, а на виході отримується унікальний хеш-код фіксованої довжини.

До переваг алгоритмів хешування слід віднести висока швидкість обчислення, а також – гарантія цілісності даних (навіть незначна зміна даних повністю змінює хеш-код).

До недоліки слід віднести можливість колізій (дві різні вхідні послідовності мають однаковий хеш), а також – хеш не можна розшифрувати (використовується тільки для перевірки даних).

Приклади алгоритмів хешування наступні: SHA-256; MD5; SHA-3; BLAKE2. Алгоритм хешування SHA-256 (Secure Hash Algorithm 256-bit) – один із найпопулярніших алгоритмів, використовується у блокчейні та цифрових підписах. Алгоритм MD5 (Message Digest Algorithm 5) – застарілий алгоритм, який вважається вразливим через можливість колізій. Алгоритм SHA-3 – новітній стандарт хешування, що має підвищену стійкість до атак. Алгоритм BLAKE2 – швидкий і безпечний алгоритм хешування, що є альтернативою SHA-3.

Отже, криптографічні алгоритми поділяються на три основні категорії: симетричні алгоритми, які забезпечують швидке шифрування, асиметричні алгоритми, що використовуються для безпечного обміну ключами та цифрових підписів, та алгоритми хешування, які гарантують цілісність даних. Вибір конкретного методу залежить від вимог до безпеки, продуктивності та області застосування.

1.1.4 Огляд стандартів шифрування та їх застосування у сучасних інформаційних системах

Сучасні інформаційні системи потребують надійного шифрування для захисту конфіденційності, цілісності та автентичності даних. Використання загальноприйнятих криптографічних стандартів гарантує високу безпеку інформації у різних сферах – від електронної комерції та банківської справи до військових і державних систем. У цьому розділі розглянемо основні міжнародні стандарти шифрування, їх особливості та сфери застосування.

До основних міжнародних стандартів шифрування відносяться: AES; RSA; ECC; SHA. Алгоритм AES – один із найпоширеніших стандартів симетричного шифрування, затверджений Національним інститутом стандартів і технологій США (NIST) у 2001 році. Він замінив застарілий DES і забезпечує високу стійкість до криптоаналізу. Основні характеристики алгоритму AES наступні:

- довжина ключа: 128, 192 або 256 біт;
- блокова структура: 16 байт (128 біт);
- висока швидкість шифрування;
- захищений від багатьох атак (наприклад, диференційного та лінійного криптоаналізу);

Сфери застосування алгоритму AES наступні:

- захист даних у державних установах (FIPS-197);
- банківські операції та електронна комерція;
- Wi-Fi-захист (WPA2, WPA3);
- шифрування файлових систем (BitLocker, VeraCrypt).

RSA – стандартний алгоритм асиметричного шифрування, який базується на труднощах факторизації великих чисел. Використовується для захисту даних, цифрових підписів та аутентифікації. Основні характеристики алгоритму RSA наступні**:**

- довжина ключа: 1024, 2048, 4096 біт (рекомендовано мінімум 2048 біт);
- висока безпека, але повільніше шифрування порівняно з AES;
- використовується для передачі ключів у гібридних системах.

Сфери застосування алгоритму RSA наступні:

- протоколи безпечного зв’язку (TLS/SSL, HTTPS);
- цифрові підписи (PKI, PGP, електронний документообіг);
- автентифікація користувачів (смарт-карти, токени).

Криптографія на еліптичних кривих (ECC) є більш ефективною альтернативою RSA завдяки меншій довжині ключа при збереженні високої стійкості. Основні характеристики алгоритму RSA наступні:

- довжина ключа: 256 біт ECC ≈ 3072 біт RSA;

– вища продуктивність та менше використання ресурсів;

– використовується в обмежених за потужністю пристроях (IoT, мобільні технології).

Сфери застосування алгоритму RSA наступні:

– блокчейн-технології (Bitcoin, Ethereum);

– протоколи безпеки (TLS 1.3, Signal);

– електронні цифрові підписи (ECDSA).

SHA – це сімейство алгоритмів хешування, що використовується для перевірки цілісності даних та цифрових підписів. Основні версії цього сімейства наступні:

– SHA-1 (застарілий, небезпечний через колізії);

– SHA-2 (SHA-256, SHA-384, SHA-512) – широко застосовується;

– SHA-3 – новітній стандарт, що забезпечує кращу стійкість.

Сфери застосування алгоритмів хешування наступні**:**

– перевірка цілісності файлів (Git, SSL-сертифікати);

– хешування паролів (bcrypt, PBKDF2);

– блокчейн-технології.

Криптографічні алгоритми широко використовуються в сучасних технологіях для забезпечення безпеки даних. В табл. 1.2 наведено основні напрямки їх застосування.

Таким чином, сучасні криптографічні стандарти, такі як AES, RSA, ECC та SHA, забезпечують надійний захист інформації в різних сферах – від державного управління до фінансового сектору. Вибір конкретного алгоритму залежить від вимог до безпеки, продуктивності та особливостей системи. Тому сучасні інформаційні технології активно використовують комбінації цих методів для забезпечення максимального рівня захисту.

Таблиця 1.2. Основні напрямки застосування криптографічних алгоритмів

№	Сфера застосування	Алгоритми шифрування
1	Банківська сфера	AES, RSA, ECC, SHA-256
2	Мобільні комунікації	AES (WPA2, WPA3), ECC (Signal, WhatsApp)
3	VPN та захист мереж	AES (IPSec, OpenVPN), RSA (TLS)
4	Електронна комерція	RSA (HTTPS), SHA-2 (SSL-сертифікати)
5	Хмарні технології	AES (AWS KMS, Google Cloud Security)
6	Блокчейн та криптовалюти	ECC (Bitcoin, Ethereum), SHA-256

1.2 Аналіз сучасних криптографічних алгоритмів

1.2.1 Аналіз ефективності симетричних алгоритмів

Симетричні криптографічні алгоритми є основою сучасного шифрування даних. Вони забезпечують високу швидкість обробки інформації та використовуються в багатьох інформаційних системах. Основна характеристика таких алгоритмів – використання одного ключа для шифрування та розшифрування. У цьому підрозділі розглянемо ефективність основних симетричних алгоритмів, таких як AES, DES і ChaCha20, з урахуванням їх безпеки, швидкодії та стійкості до атак.

Стандарт шифрування AES є найбільш поширеним блоковим алгоритмом, що прийшов на зміну застарілому DES. Він підтримує ключі довжиною 128, 192 або 256 біт і працює з блоками по 128 біт. До його переваг слід віднести:

- висока безпека завдяки складній структурі (S-блоки, перетворення стану);
- стійкість до основних атак (диференційного, лінійного криптоаналізу);
- висока швидкість на апаратному рівні (апаратне прискорення AES-NI).

До недоліків системи шифрування AES слід віднести:

– вразливість до атак на рівні реалізації (наприклад, атаки сторонніми каналами);

– висока складність при реалізації на пристроях з обмеженими ресурсами.

Продуктивність алгоритму AES полягає в наступному:

– програмна реалізація: висока швидкість у процесорах із підтримкою AES-NI;

– апаратна реалізація: висока ефективність у захищених сховищах, VPN та хмарних сервісах.

Розглянемо ефективності алгоритму шифрування DES. Цей старий стандарт шифрування, що використовує 56-бітний ключ і блочну структуру з 64-бітними блоками. Основні проблеми DES є**:**

– мала довжина ключа (56 біт) – піддається атаці повного перебору (brute force);

– вразливість до диференційного та лінійного криптоаналізу.

Поліпшені версії DES полягає в наступному**:**

– 3DES (Triple DES) використовує три послідовних проходи DES, що значно збільшує стійкість;

– недолік 3DES: повільніший, ніж AES, та менш ефективний через триразове застосування алгоритму.

Слід відзначити невисоку продуктивності DES: відносно низька швидкість у сучасних системах; майже не використовується в нових розробках.

Наддамо оцінку ефективності ChaCha20, який є сучасним потоковим алгоритмом шифрування і швидшою та безпечнішою альтернативою RC4.

До переваг ChaCha20 слід віднести:

– висока швидкість роботи навіть без апаратного прискорення;

– стійкість до диференційного криптоаналізу;

– використовує 256-бітний ключ, що забезпечує високий рівень безпеки.

До недоліків слід віднести відсутність широкого апаратного прискорення (у порівнянні з AES-NI).

Оцінка продуктивності побудована на основі за допомогою наступних чинників:

– програмна реалізація: вищий рівень продуктивності на мобільних пристроях;

– апаратна реалізація: не підтримує спеціальне прискорення, але працює швидше за AES у деяких сценаріях.

Зробимо порівняльний аналіз ефективності алгоритмів шифрування. Для кращого розуміння ефективності розглянемо порівняльну табл. 1.3 основних характеристик симетричних систем шифрування.

Таблиця 1.3. Порівняльний аналіз ефективності симетричних алгоритмів шифрування

Алгоритм	Тип	Довжина ключа	Розмір блоку	Швидкість (програмно)	Швидкість (апаратно)	Безпека
AES	Блоковий	128/192/256 біт	128 біт	Висока	Дуже висока (AES-NI)	Висока
DES	Блоковий	56 біт	64 біт	Низька	Низька	Дуже низька
3DES	Блоковий	168 біт	64 біт	Низька	Низька	Середня
ChaCha20	Потоковий	256 біт	-	Висока	Відсутня підтримка	Висока

Таким чином, можна зробити наступний висновок:

1) система шифрування AES є найефективнішим алгоритмом, який забезпечує баланс між швидкістю та безпекою, особливо на рівні апаратного прискорення;

2) система шифрування DES є застарілим алгоритмом, який не відповідає сучасним вимогам безпеки;

3) алгоритм шифрування ChaCha20 – це сучасна альтернатива AES для програмних реалізацій, що забезпечує високу швидкість та безпеку.

Таким чином, для більшості застосувань рекомендується AES або ChaCha20, тоді як DES і 3DES слід уникати через їх низьку безпеку.

Шифр «Калина» – це український національний симетричний криптографічний алгоритм, який був розроблений як частина ініціативи створення національних стандартів у сфері інформаційної безпеки. Він є аналогом та альтернативою іноземним шифрам, таким як AES, і використовується для захисту конфіденційної інформації в державних і комерційних структурах України.

Шифр «Калина» має наступні характеристики:

- симетричний блочний шифр;
- розробник – криптографічна група при Інституті проблем прикладної математики і механіки НАН України;
- стандарт – затверджено як національний криптографічний стандарт України – ДСТУ 7624:2014;
- розмір блоку: 128 біт;
- розмір ключа: 128, 192 або 256 бі;т
- побудований за типом SP-мережі (S-box + Permutation)

Шифр побудований за принципом Substitution-Permutation Network (SPN), подібно до AES. Це означає, що він складається з кількох раундів, де на кожному виконуються такі операції:

- підстановка (S-box) – заміна кожного байта згідно з фіксованою таблицею;
- перестановка (Permutation) – перестановка байтів у блоку;
- додавання ключа (Key addition) – побітове XOR з раундовим ключем;
- лінійна трансформація – для змішування бітів (аналог MixColumns в AES).

Шифр калина забезпечує наступний рівень безпека:

- криптостійкість – дослідження не виявили ефективних атак на Калина, які б могли зламати її швидше за повний перебір ключів;

– розмір ключа – використання ключів до 256 біт дозволяє протистояти атакам перебору навіть в умовах появи квантових комп'ютерів;

– резистентність до атак – стійкий до диференціального та лінійного криптоаналізу.

Відмінності системи шифрування Калина від AES надано в табл. 1.4.

Таблиця 1.4. Відмінності системи шифрування Калина від AES

Характеристика	AES	Калина
Розмір блоку	128 біт	128 біт
Розмір ключа	128/192/256 біт	128/192/256 біт
Стандартизація	NIST (США)	ДСТУ (Україна)
Відкритість	Повністю відкритий	Повністю відкритий
Використання	Глобально	В основному в Україні
Принцип побудови	SP-мережа	SP-мережа
Ефективність	Висока	Оптимізована під українські потреби

Шифр Калина застосування в наступних системах та установах:

– системи електронного документообігу органів влади;

– державні інформаційні ресурси;

– банківська система;

– криптографічні пристрої українського виробництва;

– військові комунікації та безпечні канали передачі даних.

Шифр «Калина», згідно з національним стандартом України ДСТУ 7624:2014, підтримує кілька режимів криптографічного перетворення, що забезпечують як конфіденційність, так і цілісність та автентичність даних. Ці режими визначені відповідно до міжнародної практики використання блочних шифрів.

Основні режими, у яких може використовуватись шифр Калина:

1) ECB (Electronic Codebook) – електронна книжка кодів, тобто

– кожен блок шифрується незалежно;

– не рекомендовано для передавання даних, оскільки однакові блоки відкритого тексту дають однакові блоки шифрованого тексту;

– використовується лише в спеціалізованих задачах (наприклад, шифрування ключів).

2). CBC (Cipher Block Chaining) – зчеплення блоків шифротексту:

– кожен блок XOR'иться з попереднім шифрованим блоком перед шифруванням.

– потребує ініціалізаційного вектора (IV).

– добре підходить для захисту файлів та передавання повідомлень.

3) CFB (Cipher Feedback Mode) – режим зворотного зв’язку шифротексту:

– створює потік псевдовипадкових байтів для шифрування/розшифрування потоків даних;

– підтримує шифрування менших одиниць, ніж блок (байт, біт);

– аикористовується для шифрування потокових даних, наприклад в телекомунікаціях.

4) OFB (Output Feedback Mode) – режим зворотного зв’язку по виходу:

– схожий на CFB, але генерує потік незалежно від відкритого тексту;

– відсутність розповсюдження помилок між блоками;

– підходить для передачі потокових даних, наприклад, голосових повідомлень.

5) CTR (Counter Mode) – лічильниковий режим:

– шифрує лічильник, а не сам текст, і XOR'иться з даними;

– підтримує паралельну обробку, що дає високу продуктивність;

– один з найбільш рекомендованих режимів для високопродуктивних систем.

6) MAC (Message Authentication Code) – генерація і перевірка коду автентичності:

– забезпечує цілісність і автентичність переданих даних;

– реалізується за допомогою алгоритму на основі блочного шифру.

7) Galois/Counter Mode (GCM) — (як альтернатива CTR+MAC):

– поки не визначений у стандарті Калина, але є потенційним для подальшого розширення.

В табл. 1.5 надано режими роботи системи шифрування «Калина».

Таблиця 1.5. Режими роботи системи шифрування «Калина»

Режим	**Призначення**	**Переваги**	**Недоліки**
ECB	Прості операції	Легко реалізується	Небезпечний для даних із повтореннями
CBC	Захист даних блоками	Стійкий до аналізу	Неможливість паралельної обробки
CFB	Потокове шифрування	Підтримка бітового шифрування	Уразливість до помилок
OFB	Потокове шифрування	Незалежність від відкритого тексту	Не виявляє помилок
CTR	Висока продуктивність	Паралельність, гнучкість	Потрібен унікальний лічильник
MAC	Перевірка цілісності	Автентичність даних	Не забезпечує конфіденційність

Отже, шифр «Калина» підтримує всі основні режими, які дозволяють використовувати його для:

– захисту збережених даних (CBC);

– захисту потоків даних у реальному часі (CFB, OFB, CTR)4

– генерації цифрових підписів та контролю цілісності (MAC).

Таким чином, «Калина» – це сучасний, безпечний і надійний український шифр, який став важливим елементом національної криптографічної незалежності. Його поява зміцнила безпеку критичних інфраструктур і стала частиною стратегії інформаційного суверенітету України.

1.2.2 Аналіз ефективності асиметричних алгоритмів

Асиметричні криптографічні алгоритми є основою сучасних систем безпеки, що забезпечують конфіденційність, автентифікацію та цілісність даних. На відміну від симетричних алгоритмів, асиметричні використовують пару ключів: відкритий для шифрування та закритий для розшифрування. У цьому підрозділі розглянемо ефективність RSA, ECC та постквантових алгоритмів.

Проведемо аналіз ефективності алгоритму RSA. Цей алгоритм базується на складності факторизації великих чисел. Безпека алгоритму визначається довжиною ключа: наприклад, 2048-бітний ключ забезпечує достатній рівень захисту, проте з появою квантових комп'ютерів його стійкість під загрозою. До його переваг слід віднести: широке використання в цифрових підписах, сертифікатах, VPN; висока надійність при великих довжинах ключів. До недоліків слід віднести: низька продуктивність у порівнянні з ECC; вразливість до квантових атак (алгоритм Шора).

Цей алгоритм має наступну продуктивності:

- низька швидкість шифрування;
- помірна швидкість розшифрування;
- висока стійкість проти класичних атак, але слабка проти квантових.

Проведемо аналіз ефективності алгоритму ECC. Цей алгоритм (Elliptic Curve Cryptography) заснований на складності обчислення дискретного логарифму на еліптичних кривих. Використовує коротші ключі порівняно з RSA при аналогічному рівні безпеки. До переваг можна віднести: менший розмір ключів: ECC-256 еквівалентний RSA-3072; вища продуктивність і менші обчислювальні ресурси; підходить для мобільних пристроїв і IoT. До недоліків слід віднести: складніша реалізація; вразливість до атак сторонніми каналами

при неправильному впровадженні. Продуктивність цього алгоритму наступна: висока швидкість шифрування; висока швидкість розшифрування; стійкість до атак вища за RSA, але вразливий до квантових атак.

Виконаємо аналіз ефективності постквантових алгоритмів. Вони розробляються для протидії квантовим атакам. Найперспективніші є наступні алгоритми: CRYSTALS-Kyber, NTRU, McEliece. До їх переваг слід віднести: захист від атак квантових комп'ютерів; підтримка в нових криптографічних стандартах (NIST PQC). До недоліків слід віднести: відносно нові та не до кінця перевірені; високі вимоги до обчислювальних ресурсів. Постквантови алгоритми мають середню швидкість шифрування (залежить від алгоритму); середня швидкість розшифрування; високу стійкість до атак з урахуванням квантових загроз.

Виконаємо порівняльний аналіз ефективності асиметричних алгоритмів шифрування на основі показників, які надані в табл. 1.6.

Таблиця 1.6. Порівняльний аналіз ефективності асиметричних алгоритмів шифрування

Алгоритм	Ключова особливість	Довжина ключа	Швидкість	Безпека	Стійкість до квантових атак
RSA	Факторизація чисел	2048+ біт	Низька	Висока	Ні
ECC	Еліптичні криві	256 біт (≈ RSA-3072)	Висока	Вища за RSA	Ні
Kyber	Решітчасті проблеми	768+ біт	Середня	Висока	Так
NTRU	Поліноми	700+ біт	Висока	Висока	Так

Таким чином, на основі даних табл. 1.6 можна зробити наступні висновки:

1) RSA – використовується широко, але має низьку продуктивність і вразливий до квантових атак;

2) ECC – ефективніший за RSA, забезпечує вищу продуктивність, але також вразливий до квантових атак;

3) постквантові алгоритми – єдиний варіант, що гарантує захист у майбутньому, проте потребує подальших досліджень.

Перехід на постквантову криптографію неминучий, але на даний момент ECC залишається оптимальним вибором серед класичних алгоритмів.

1.2.3 Порівняння швидкодії, стійкості до атак та використання ресурсів

Порівняльна оцінка криптографічних алгоритмів дозволяє визначити їхню практичну доцільність залежно від цільового середовища — чи це серверні системи, мобільні пристрої, або системи Інтернету речей (IoT). У цьому підрозділі узагальнимо дані щодо продуктивності, безпеки та ресурсозатратності найпоширеніших алгоритмів. Для цього дома наступні показники:

1) швидкодію;

2) стійкість до атак;

3) використання ресурсів.

Розглянемо швидкодію наступних систем шифрування:

1) RSA має відносно низьку швидкість шифрування, особливо при використанні довгих ключів. Підходить для одноразового обміну ключами, але не для масового шифрування даних.

2) ECC забезпечує високу швидкодію як у шифруванні, так і у розшифруванні. Особливо ефективний на обмежених пристроях;

3) постквантові алгоритми – продуктивність варіюється. Наприклад, Kyber демонструє помірну швидкодію, McEliece – повільніший через великі ключі;

Охарактеризуємо стійкість до атак систем шифрування:

1) RSA захищений від класичних атак при довжині ключа ≥2048 біт, але вразливий до квантових алгоритмів (алгоритм Шора);

2) ECC забезпечує вищу безпеку при меншій довжині ключа, але також нестійкий до квантових атак;

3) постквантові алгоритми: розроблені з урахуванням квантових атак, мають високу стійкість у майбутньому, але потребують більшої перевірки на практиці.

Використання ресурсів систем шифрування має такі особливості:

1) RSA потребує більше обчислювальних ресурсів і пам’яті, що ускладнює його використання в обмежених системах;

2) ECC має мінімальне споживання пам’яті та процесора. Ідеально підходить для мобільних пристроїв;

3) постквантові алгоритми вимагають більше пам’яті (особливо McEliece – до кількох мегабайт для публічного ключа), що обмежує їх застосування в IoT.

1.3 Оцінка ефективності криптографічних алгоритмів у захисті конфіденційної інформації

1.3.1 Методики оцінки криптостійкості алгоритмів

Криптостійкість – це здатність криптографічного алгоритму протистояти спробам несанкціонованого доступу до інформації, навіть якщо зловмисник має часткову інформацію або значні обчислювальні ресурси. Оцінка криптостійкості є важливим етапом при виборі або впровадженні алгоритму у захищених системах. Існує кілька загальноприйнятих методик та критеріїв такої оцінки.

Теоретична криптостійкість базується на математичній складності задач, що лежать в основі алгоритму. Для прикладу:

1) RSA базується на задачі факторизації великих чисел;

2) ECC – на задачі дискретного логарифмування на еліптичних кривих;

3) постквантові алгоритми – на задачах ґраткової алгебри, кодів, багаточленів тощо.

Оцінюється час та обчислювальні ресурси, які необхідно витратити на злам алгоритму при сучасному та прогнозованому рівні розвитку обчислювальної техніки.

Криптоаналіз – це практичний підхід, що включає випробування алгоритму на стійкість до різних типів атак:

1) атака повного перебору (brute-force) – оцінюється час, потрібний для перебору всіх можливих ключів;

2) аналіз з відкритим текстом (known plaintext attack) – перевіряється, чи може знання частини відкритого тексту допомогти знайти ключ;

3) диференційний та лінійний криптоаналіз – застосовуються до симетричних алгоритмів, щоб виявити закономірності у шифруванні;

4) атаки сторонніми каналами (side-channel attacks) – досліджують можливість добування ключів за допомогою спостереження за енергоспоживанням, часом виконання, електромагнітними випромінюваннями.

3. Оцінка за міжнародними стандартами (NIST, ISO, ETSI) визначають мінімальні вимоги до криптостійкості:

1) рекомендовані довжини ключів (напр., 128 біт для симетричних, 2048 біт для RSA, 256 біт для ECC);

2) алгоритми, допущені до використання у державних і промислових системах;

3) період перегляду та оновлення стандартів з урахуванням появи нових атак.

Моделювання зловмисника передбачає надання оцінки алгоритму в умовах моделі зловмисника:

1) обмежений зловмисник: має лише зашифрований текст.

2) зловмисник з відкритим текстом: знає частину відкритих і зашифрованих даних;

3) квантовий зловмисник: володіє квантовим комп’ютером та використовує квантові алгоритми (напр., алгоритм Шора, Гровера).

Емпіричне тестування систем шифрування полягає у запуску алгоритму на тестових даних та аналізі результатів:

1) перевірка рівномірності розподілу шифрованого тексту;

2) тестування на наявність закономірностей;

3) випробування на симуляторах атак.

Отже, оцінка криптостійкості є багаторівневим процесом, що поєднує математичний аналіз, практичні тести та стандартизовані критерії. Надійний криптографічний алгоритм повинен бути стійким як до класичних, так і до новітніх загроз, включаючи квантові атаки. Тому сучасна тенденція зосереджена на гібридних та постквантових рішеннях, які проходять ретельну перевірку за різними методиками.

1.3.2 Аналіз загроз та атак на сучасні алгоритми шифрування

У сучасних умовах цифрової трансформації та глобальної взаємодії зростає актуальність аналізу стійкості алгоритмів шифрування до різних типів атак. Навіть найбільш криптостійкі алгоритми, як-от AES, RSA або ECC, можуть бути вразливими до специфічних сценаріїв атак, зокрема при неправильному впровадженні або використанні.

Класифікація атак на алгоритми шифрування має неступні категорії:

1) атаки з повним доступом до шифротексту (ciphertext-only attack): зловмисник має лише доступ до шифрованого тексту;

2) атаки з доступом до відкритого та шифрованого тексту (known-plaintext attack): відомі деякі пари відкритого та шифрованого тексту;

3) атаки з вибором відкритого тексту (chosen-plaintext attack): зловмисник може вибрати повідомлення для шифрування;

Атаки з вибором шифротексту (chosen-ciphertext attack): зловмисник може вибрати шифротекст для розшифрування.

Класифікація атак на алгоритми шифрування представлена на рис. 1.4.

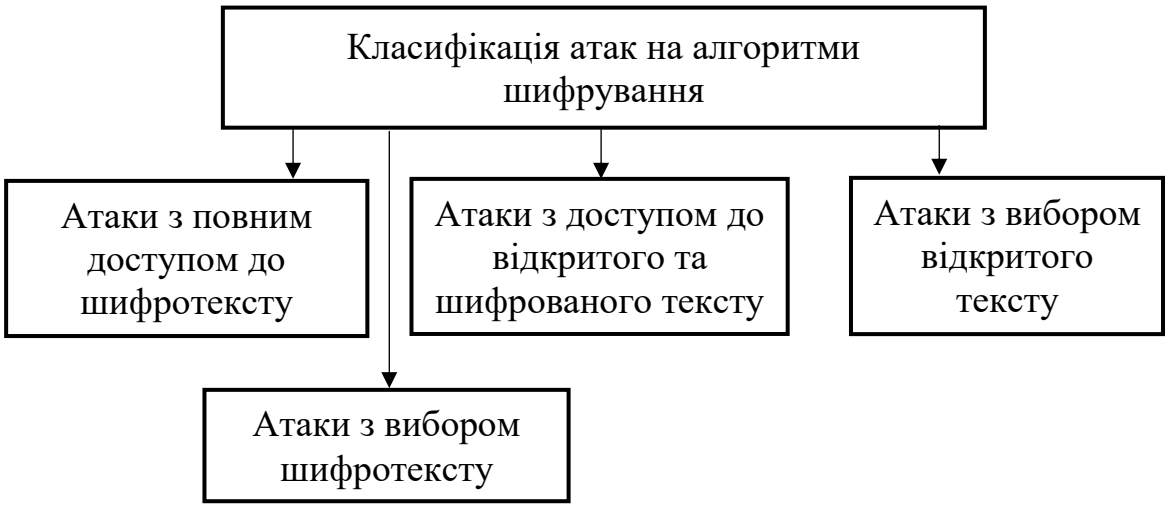


Рисунок 1.4. Класифікація атак на алгоритми шифрування

Типові загрози для сучасних алгоритмів передбачає наступні атаки:

1) атаки на основі аналізу побічних каналів;

2) квантові атаки;

3) аналіз ключів методом повного перебору або часткового знання;

4) криптоаналітичні атаки;

Атаки на основі аналізу побічних каналів використовують витоки інформації через споживання енергії, електромагнітні випромінювання, час виконання тощо. Наприклад: атака через час виконання операцій (timing attacks), атака через споживання струму (power analysis).

Квантові атаки актуальні для алгоритмів з відкритим ключем. Алгоритми як RSA та ECC стають вразливими до квантового алгоритму Шора. У відповідь розробляються постквантові криптографічні алгоритми (NIST PQC).

Аналіз ключів методом повного перебору або часткового знання: у випадку слабких або передбачуваних ключів можливий брутфорс або dictionary attack. Для симетричних алгоритмів рекомендована довжина ключа повинна бути не менше 128 бітів.

Криптоаналітичні атаки передбачає використання диференційного криптоаналізу (Differential cryptanalysis), лінійного криптоаналізу (Linear cryptanalysis). Ці атаки були ефективними проти старих стандартів шифрування (DES), але сучасні алгоритми, як AES, мають захист проти них.

Навіть стійкий алгоритм може стати вразливим через: використання статичного IV (ініціалізаційного вектора) в режимах CBC або GCM; повторне використання ключів або IV; неправильне використання режимів шифрування (наприклад, ECB); відсутність автентифікації шифрованих повідомлень (що дозволяє атаки типу "ciphertext malleability").

Можна визначити наступні приклади атак на систему шифрування AES:

1) Side-channel attacks (побічні канали) – реалізація AES у програмному забезпеченні без захисту може бути вразливою до аналізу часу або електромагнітного випромінювання;

2) Fault injection – умисне внесення помилок у криптографічну операцію може дозволити зловмиснику вивести частину ключа;

3) Криптоаналітичні атаки на спрощені версії AES (AES-192 та AES-256 у деяких специфічних режимах) неефективні в практиці, але досліджуються академічною спільнотою.

Порівняльна характеристика систем шифрування представлена в табл. 1.7.

Таблиця 1.7. Порівняльна характеристика систем шифрування

Алгоритм	Швидкодія	Стійкість до атак	Ресурси (пам’ять/процесор)	Придатність для IoT
RSA	Низька	Висока (без квантових)	Високі	Обмежена
ECC	Висока	Вища за RSA (без квантових)	Низькі	Висока
Kyber	Середня	Висока (з квантовим захистом)	Середні	Залежить від реалізації
McEliece	Низька	Дуже висока	Дуже високі	Низька

Бачимо, що для систем із обмеженими ресурсами найкраще підходить ECC, що поєднує швидкодію і відносну безпеку. RSA залишається придатним для класичних систем, де немає загрози з боку квантових атак. Постквантові алгоритми, зокрема Kyber, є перспективними для майбутнього, але потребують адаптації до різних середовищ.

Отже, сучасні алгоритми шифрування демонструють високу криптостійкість при правильному впровадженні. Основні загрози походять не від математичної слабкості, а від помилок у реалізації, людського фактору, побічних каналів та майбутніх квантових загроз. Тому важливо не лише обирати надійний алгоритм, але й дотримуватись криптографічних стандартів та практик безпечної реалізації.

1.3.3 Тестування системи шифрування AES

Розглянемо програму на мові програмування Python для тестування системи симетричного шифрування AES із використанням бібліотеки cryptography. Вона дозволяє:

1) зашифрувати текст;

2) розшифрувати його;

3) заміряти час виконання.

Код програми відповідної приграм має наступний вид:

```
from cryptography.hazmat.primitives.ciphers import Cipher, algorithms, modes
from cryptography.hazmat.backends import default_backend
from cryptography.hazmat.primitives import padding
import os
import time


# Генерація ключа та IV (ініціалізаційного вектора)
key = os.urandom(32)  # 256-бітний ключ для AES
iv = os.urandom(16)   # 128-бітний IV
```

```
        # Функція шифрування
        def encrypt(data):
            padder = padding.PKCS7(128).padder()
            padded_data = padder.update(data.encode()) + padder.finalize()

            cipher = Cipher(algorithms.AES(key), modes.CBC(iv),
backend=default_backend())
            encryptor = cipher.encryptor()
            return encryptor.update(padded_data) + encryptor.finalize()

        # Функція розшифрування
        def decrypt(ciphertext):
            cipher = Cipher(algorithms.AES(key), modes.CBC(iv),
backend=default_backend())
            decryptor = cipher.decryptor()
            padded_data = decryptor.update(ciphertext) + decryptor.finalize()

            unpadder = padding.PKCS7(128).unpadder()
            return (unpadder.update(padded_data) + unpadder.finalize()).decode()

        # Введення тексту
        plaintext = input("Введіть текст для шифрування: ")

        # Шифрування
        start = time.perf_counter()
        ciphertext = encrypt(plaintext)
        end = time.perf_counter()
        print("\nЗашифровано (в hex):", ciphertext.hex())
        print(f"Час шифрування: {end - start:.6f} секунд")
```

```
# Розшифрування
start = time.perf_counter()
decrypted = decrypt(ciphertext)
end = time.perf_counter()
print("\nРозшифровано:", decrypted)
print(f"Час розшифрування: {end - start:.6f} секунд")
```

В цій програмі використовується AES-256 у режимі CBC. При цьому додається PKCS7-паддінг для обробки тексту, довжина якого не кратна блоку. Програма виводить:

1) зашифрований текст у hex-форматі;

2) розшифрований результат;

3) час на шифрування і розшифрування.

Розроблена програма для системи шифрування AES-128, яка дає змогу ввести текст вручну і порівняти швидкодію з AES-256. Основна відмінність — ключ має довжину 16 байтів (128 біт):

```
from cryptography.hazmat.primitives.ciphers import Cipher, algorithms, modes
from cryptography.hazmat.backends import default_backend
from cryptography.hazmat.primitives import padding
import os
import time

# Генерація ключа 128 біт (16 байтів) і IV (ініціалізаційного вектора)
key = os.urandom(16)  # AES-128
iv = os.urandom(16)   # 128-бітний IV

# Функція шифрування
def encrypt(data):
    padder = padding.PKCS7(128).padder()
    padded_data = padder.update(data.encode()) + padder.finalize()
```

```
        cipher = Cipher(algorithms.AES(key), modes.CBC(iv),
backend=default_backend())
        encryptor = cipher.encryptor()
        return encryptor.update(padded_data) + encryptor.finalize()

    # Функція розшифрування
    def decrypt(ciphertext):
        cipher = Cipher(algorithms.AES(key), modes.CBC(iv),
backend=default_backend())
        decryptor = cipher.decryptor()
        padded_data = decryptor.update(ciphertext) + decryptor.finalize()

        unpadder = padding.PKCS7(128).unpadder()
        return (unpadder.update(padded_data) + unpadder.finalize()).decode()

    # Введення тексту
    plaintext = input("Введіть текст для шифрування (AES-128): ")

    # Шифрування
    start = time.perf_counter()
    ciphertext = encrypt(plaintext)
    end = time.perf_counter()
    print("\nЗашифровано (в hex):", ciphertext.hex())
    print(f"Час шифрування: {end - start:.6f} секунд")

    # Розшифрування
    start = time.perf_counter()
    decrypted = decrypt(ciphertext)
    end = time.perf_counter()
```

```
print("\nРозшифровано:", decrypted)
print(f"Час розшифрування: {end - start:.6f} секунд")
```

На рис. 1.5 представлено результати тестування швидкодії шифрування та розшифрування невеликого тексту системи шифрування AES 256. Для шифрування та розшифрування використовувалася текст невеликого об'єму. Бачимо, що на процес шифрування була витрачено 0,037 секунд. Процес шифрування був занадто швидким, що програма не надала цей результат.

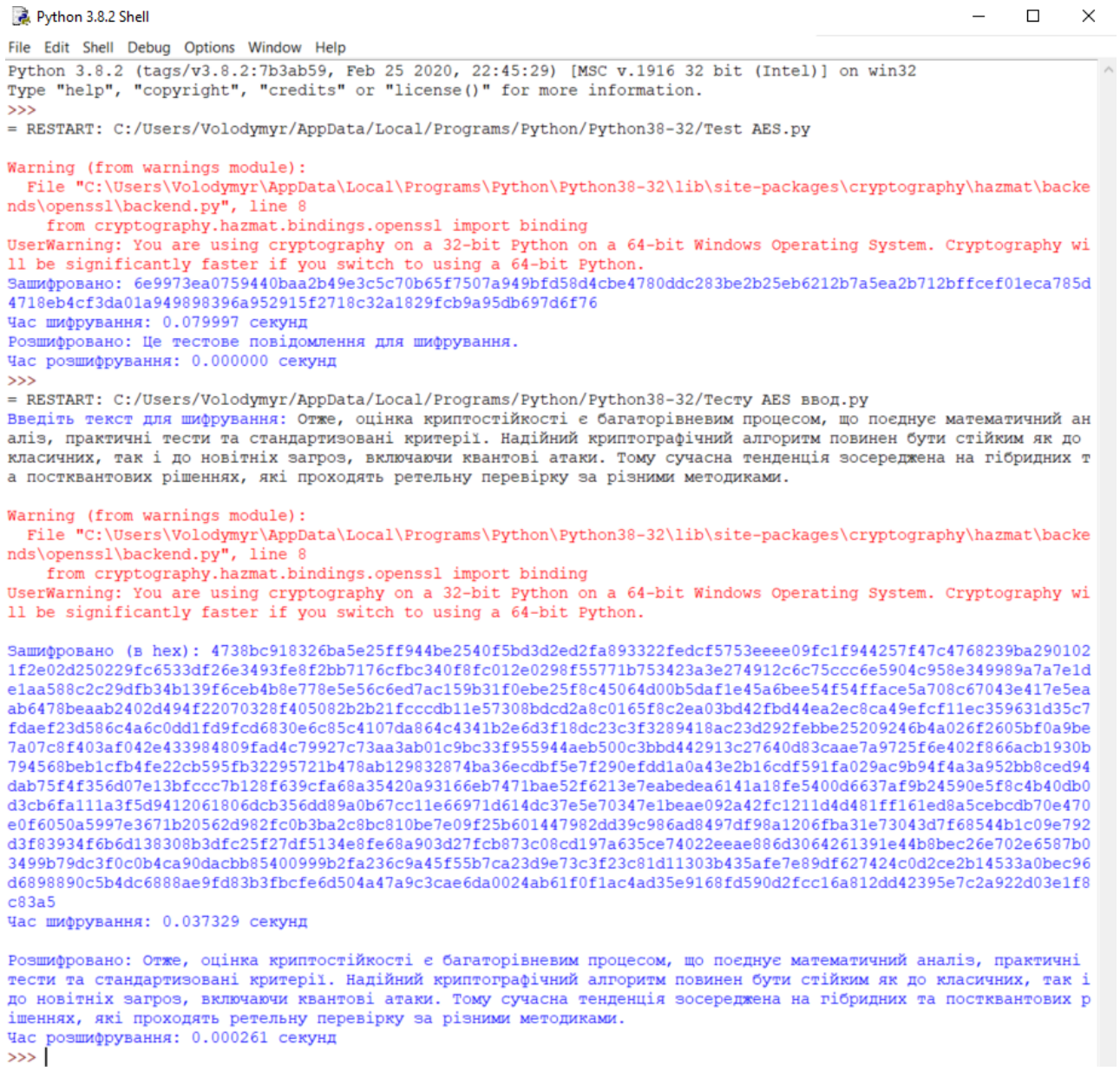


Рисунок 1.5. Результати тестування швидкодії шифрування та розшифрування невеликого тексту системи шифрування AES 256

Для порівняльного аналізу на рис. 1.6 представлено результат тестування системи шифрування AES 128. Час шифрування AES 128 складає 0,0592, а розшифрування – 0,000311. Бачимо, що система AES 256 має більшу швидкодію шифрування та розшифрування ніж система AES 128.

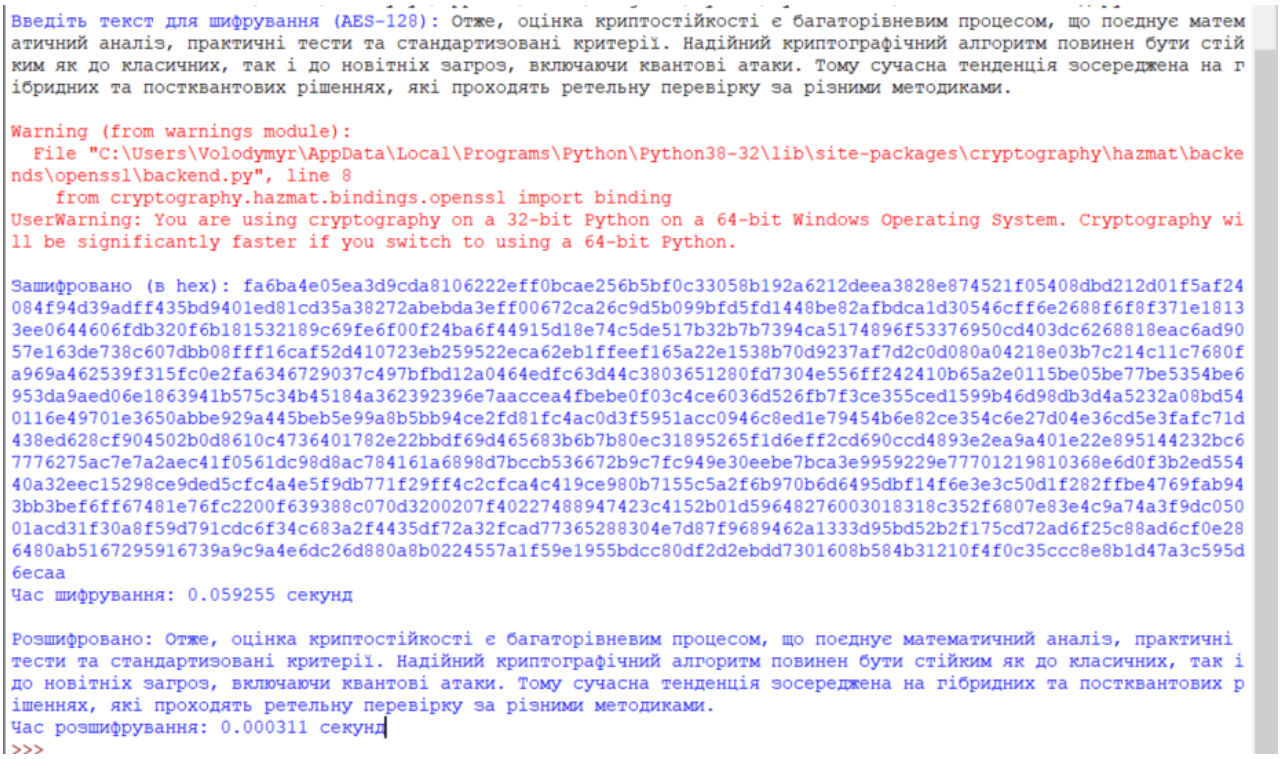


Рисунок 1.6. Результати тестування швидкодії шифрування та розшифрування невеликого тексту системи шифрування AES 128

Для оцінки швидкодії шифрування та розшифрування систем AES 128 та AES 256 розглянемо для цього тестування з використання тексту об’ємом 1 Мбайт.

Нижче наведена програма для об'єктивного порівняння продуктивності AES-128 та AES-256 на великому обсязі тексту, з розрахунком середнього часу шифрування та розшифрування на 100 ітераціях:

```
from cryptography.hazmat.primitives.ciphers import Cipher, algorithms, modes
from cryptography.hazmat.backends import default_backend
from cryptography.hazmat.primitives import padding
import os
```

```
import time

# Функція шифрування
def encrypt(data, key, iv):
    padder = padding.PKCS7(128).padder()
    padded_data = padder.update(data.encode()) + padder.finalize()

    cipher = Cipher(algorithms.AES(key), modes.CBC(iv),
backend=default_backend())
    encryptor = cipher.encryptor()
    return encryptor.update(padded_data) + encryptor.finalize()

# Функція розшифрування
def decrypt(ciphertext, key, iv):
    cipher = Cipher(algorithms.AES(key), modes.CBC(iv),
backend=default_backend())
    decryptor = cipher.decryptor()
    padded_data = decryptor.update(ciphertext) + decryptor.finalize()

    unpadder = padding.PKCS7(128).unpadder()
    return (unpadder.update(padded_data) + unpadder.finalize()).decode()

# Тестовий текст
plaintext = "Тестове повідомлення. " * 50000  # Приблизно 1 МБ тексту

def test_aes(key_size_bits):
    key = os.urandom(key_size_bits // 8)
    iv = os.urandom(16)

    total_encrypt_time = 0
```

```
        total_decrypt_time = 0
        ciphertext = b""

        for _ in range(100):
            start = time.perf_counter()
            ciphertext = encrypt(plaintext, key, iv)
            total_encrypt_time += (time.perf_counter() - start)

            start = time.perf_counter()
            decrypted = decrypt(ciphertext, key, iv)
            total_decrypt_time += (time.perf_counter() - start)

        print(f"\nAES-{key_size_bits} Результати:")
        print(f"Середній час шифрування: {total_encrypt_time / 100:.6f} секунд")
        print(f"Середній час розшифрування: {total_decrypt_time / 100:.6f}
секунд")

    # Запуск тестів для AES-128 і AES-256
    test_aes(128)
    test_aes(256)
```

Результати тестування надано на рис. 1.7.

```
Warning (from warnings module):
  File "C:\Users\Volodymyr\AppData\Local\Programs\Python\Python38-32\lib\site-packages\cryptography\hazmat\backe
nds\openssl\backend.py", line 8
    from cryptography.hazmat.bindings.openssl import binding
UserWarning: You are using cryptography on a 32-bit Python on a 64-bit Windows Operating System. Cryptography wi
ll be significantly faster if you switch to using a 64-bit Python.

AES-128 Результати:
Середній час шифрування: 0.010840 секунд
Середній час розшифрування: 0.008566 секунд

AES-256 Результати:
Середній час шифрування: 0.010162 секунд
Середній час розшифрування: 0.008259 секунд
>>>
```

Рисунок 1.7. Результати тестування швидкодії шифрування та розшифрування великого тексту (1 Мбайт) системи шифрування AES 128

Загальні результати тестування систем шифрування AES 128 і AES 256 надано в табл. 1.8. Бачимо, що середній час шифрування для AES 128 тексту великого об’єму (1 Мбайт) має середній час шифрування 0,010840 секунд, середній час розшифрування складає 0,008566.

Для системи AES 256 середній час шифрування 0,010162 секунд, середній час розшифрування складає 0,008259.

Результати дало змогу з’ясувати, що середній час шифрування та розшифрування для AES 128 та AES 256 тексту великого об’єму (1 Мбайт) приблизно однакові, що з точки зори криптостійкості доцільно використовувати шифр AES 256.

Таблиця 1.8. Загальні результати тестування систем шифрування AES 128 і AES 256

Розмір текст	AES 128		AES 256	
	Шифрування	Розшифрування	Шифрування	Розшифрування
малий	0,059255	0,000311	0,037329	0,000261
Великий – 1 Мбайт	0,010840	0,008566	0,010162	0,008259

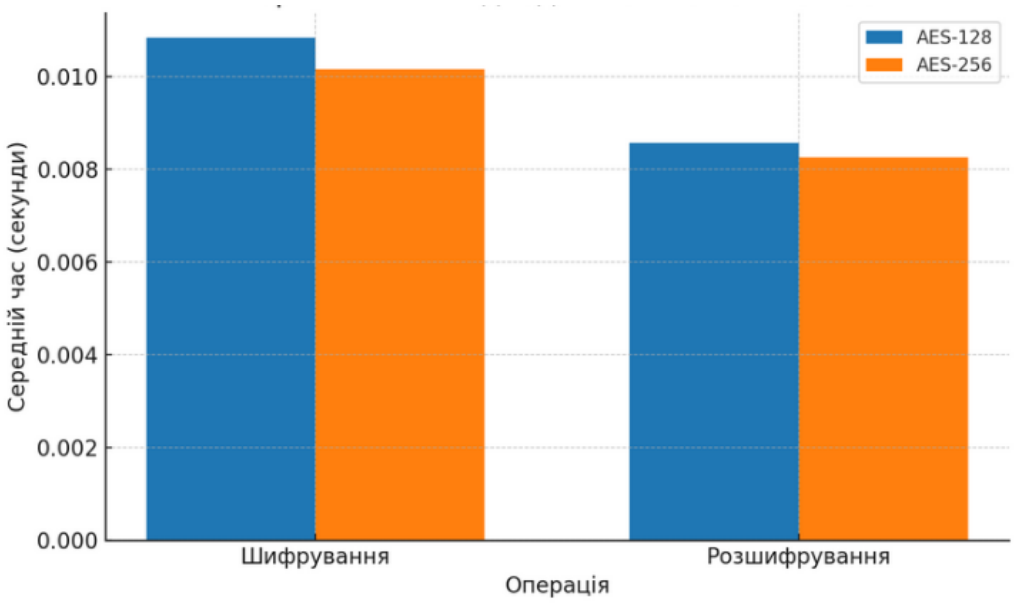


Рисунок 1.8. Порівняння швидкодії AES-128 та AES-256

Діаграма ілюструє порівняння середнього часу виконання операцій шифрування та розшифрування для алгоритмів AES-128 та AES-256.

1) по осі X розміщені типи операцій: Шифрування та Розшифрування;

2) по осі Y — середній час виконання операції у секундах;

3) сині стовпчики відображають результати для AES-128, помаранчеві — для AES-256.

Згідно з графіком, AES-256 трохи швидший, ніж AES-128 для обох типів операцій у проведеному тесті. Такий результат є нетиповим, оскільки зазвичай AES-256 повільніший через більшу довжину ключа, але в реальності це може залежати від реалізації бібліотеки, розміру даних, оптимізації на рівні процесора та конфігурації системи.

1.3.4 Рекомендації щодо вибору криптографічних методів для захисту інформації

Забезпечення конфіденційності, цілісності та автентичності інформації вимагає ретельного підбору криптографічних методів. Вибір залежить від особливостей інформаційної системи, моделі загроз, рівня критичності даних, обчислювальних ресурсів та нормативно-правових вимог. Охарактеризуємо це з урахуванням прийняття наступних рішень:

1) вибір симетричних алгоритмів шифрування;

2) вибір алгоритмів з відкритим ключем (асиметричних);

3) хеш-функції та цифрові підписи;

4) загальні рекомендації;

5) впровадження криптографічних методів.

Симетричні алгоритми застосовуються для захисту великих обсягів даних завдяки високій швидкодії. Можна рекомендувати наступні алгоритми:

1) AES-256 – є найкращий варіант для більшості задач із високими вимогами до безпеки. Режими використання: GCM, CBC з унікальним IV;

2) ChaCha20-Poly1305: рекомендований для пристроїв з обмеженими обчислювальними ресурсами (наприклад, IoT).

Можна зазначити наступні рекомендації для забезпечення безпеки шифрування секретних даних:

1) уникати застарілих алгоритмів типу DES, 3DES, RC4;

2) не використовувати режим ECB;

3) генерувати унікальні ключі та IV для кожного сеансу.

Вибір алгоритмів з відкритим ключем (асиметричних) – використовуються для розповсюдження ключів, цифрового підпису, автентифікації. Тут можна рекомендувати наступні алгоритми:

1) RSA (не менше 3072 біт), хоча поступово замінюється більш ефективними ECC;

2) Elliptic Curve Cryptography (ECC) – зокрема Curve25519 або secp256r1;

3) Post-Quantum Cryptography (PQC) – у перспективі для критичних систем (алгоритми, відібрані NIST, наприклад, CRYSTALS-Kyber, Dilithium).

В цьому випадку можна надати наступні рекомендації:

1) перевагу надавати ECC, де це можливо, через менші розміри ключів і швидшу обробку;

2) використовувати гібридні схеми для поступового переходу до PQC.

Можна надати наступні рекомендації для хеш-функцій та цифрових підписів:

1) використовувати лише SHA-2 (SHA-256, SHA-512) або SHA-3;

2) уникати використання MD5 та SHA-1 — вони більше не вважаються безпечними;

3) Цифрові підписи:

– ECDSA, RSA-PSS, EdDSA – сучасні алгоритми для цифрового підпису;

– використання з хеш-функцією SHA-256 або новішими.

Загальні рекомендації з приводу використання криптографічних методів захисту інформації наведені в табл. 1.9.

Таблиця 1.9. Загальні рекомендації з приводу використання криптографічних методів захисту інформації

Компонент системи	Рекомендований криптографічний метод
Передача даних	TLS 1.3 із AES-256-GCM або ChaCha20
Хмарні сервіси	AES-256, ECC, токенізація
Мобільні додатки	ChaCha20-Poly1305, Curve25519, SHA-256
IoT/вбудовані системи	ECC (X25519), ChaCha20, легкі хеш-функції
Захист файлів	AES-256 з автентифікацією (наприклад, AES-GCM)
Цифровий підпис	EdDSA, RSA-PSS, ECDSA

Визначимо наступні рекомендації, які пов’язані із впровадженням криптографічних методів:

1) регулярно оновлювати криптографічні бібліотеки;

2) застосовувати апаратне прискорення шифрування (AES-NI, TPM);

3) проводити аудит безпеки реалізованих алгоритмів та протоколів;

4) використовувати бібліотеки з відкритим вихідним кодом, що активно підтримуються: OpenSSL, Libsodium, BoringSSL тощо.

Отже, вибір криптографічних засобів повинен базуватись на принципах актуальності, криптостійкості та відповідності галузевим стандартам (ISO/IEC 27001, NIST SP 800-57, RFC 8446 тощо). Лише системний підхід до проєктування та впровадження шифрувальних рішень дозволить ефективно протидіяти сучасним кіберзагрозам.

На рис. 1.9 надано графік, що наочно порівнює основні криптографічні алгоритми за трьома критеріями: швидкодія, стійкість до атак і використання ресурсів.

На діаграмі представлено порівняння середнього часу шифрування та розшифрування для двох алгоритмів симетричного шифрування – AES-128 та AES-256.

Графік побудовано на основі результатів експериментального тестування, під час якого кожен алгоритм використовувався для обробки однакового обсягу текстових даних протягом 100 ітерацій.

По осі X відображені типи операцій – шифрування та розшифрування, по осі Y – середній час виконання операції у секундах.

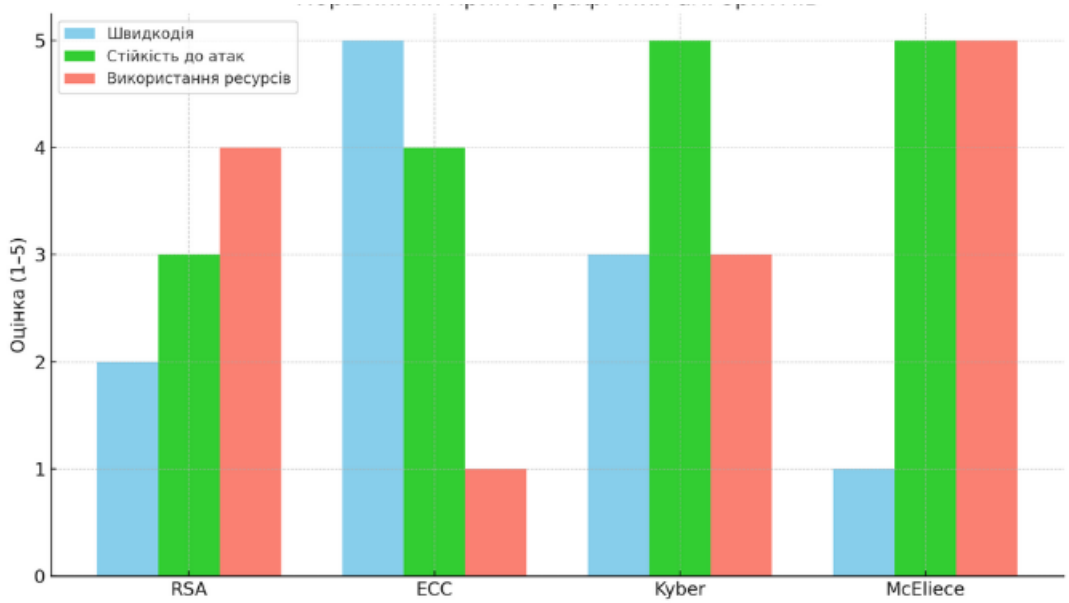


Рисунок 1.9. Показники основних криптографічних алгоритмів за трьома критеріями: швидкодія, стійкість до атак і використання ресурсів

З графіка бачимо, що:

1) AES-256 продемонстрував трохи кращу швидкодію, ніж AES-128 як під час шифрування (0.01016 с проти 0.01084 с), так і під час розшифрування (0.00826 с проти 0.00857 с);

2) різниця в часі виконання є незначною (менше 1 мілісекунди) та може бути обумовлена особливостями програмної реалізації, архітектурою процесора, або обмеженнями середовища запуску (у даному випадку – 32-бітова версія Python на 64-бітній системі).

Цей результат свідчить, що AES-256, попри використання довшого ключа, не поступається AES-128 у продуктивності при певних умовах, а за рахунок вищого рівня криптостійкості є рекомендованим до використання у критично важливих інформаційних системах.

2 РОЗДІЛ ОХОРОНИ ПРАЦІ ТА ТЕХНІКИ БЕЗПЕКИ

Забезпечення безпеки життя та здоров’я громадян під час виконання ними трудових обов’язків, а також створення умов, що не шкодять здоров’ю, є одним із пріоритетних завдань держави. Кожне робоче місце повинно бути оснащене таким чином, щоб гарантувати зручність і безпеку співробітників. Наприклад, виробниче обладнання, обслуговування якого вимагає переміщення персоналу, слід обладнати надійними і зручними проходами, майданчиками, сходами та поручнями. Водночас експлуатація устаткування не повинна перевищувати встановлені норми викидів шкідливих речовин і створювати загрози пожеж або вибухів.

Метою роботи є аналіз сучасних криптографічних алгоритмів та оцінка їхньої ефективності для захисту конфіденційної інформації.

2.1 Аналіз небезпечних і шкідливих факторів, що впливають на програміста при розробці даного програмного комплексу

При розробці програмного комплексу проводиться ретельний аналіз можливого впливу виробничих чинників, які можуть зашкодити здоров’ю програміста. Згідно зі стандартом ГОСТ 12.1.003-74, до небезпечних факторів належать ті, що можуть спричинити раптове погіршення здоров’я або навіть летальний результат під час роботи.

Аналіз також враховує різні якісні характеристики робочого середовища – фізичні параметри приміщень, такі як температура, вологість, електричний опір підлоги, а також дані щодо концентрації іонів і забруднювачів у повітрі.

2.2 Гігієнічні вимоги до виробничого середовища

Сучасне виробництво вимагає створення оптимальних санітарних умов, які забезпечують плідну роботу співробітників без надмірного навантаження. Це досягається організацією комфортного робочого місця з чистим повітрям, правильною освітленістю, а також заходами щодо захисту від шумових та вібраційних впливів.

2.2.1 Мікроклімат

Недотримання норм мікроклімату негативно позначається на здоров'ї людини, що може призвести до зниження працездатності або її повної втрати. Показники мікроклімату мають відповідати нормам, визначеним у ДСН 3.3.6.042-99. Згідно з чинними нормативними документами (ДСанПіН 3.3.2-007-98), у холодні періоди температура повітря повинна перебувати від –22 до +24°С, швидкість руху повітря – близько 0,1 м/с, а відносна вологість – у межах 40–60%.

В теплий сезон допустимі значення температури складають 23–25°С при збереженні вологості та швидкості повітря (0,1–0,2 м/с) на тих же рівнях. Підвищення кількості позитивних іонів у робочій зоні також може негативно впливати на здоров'я, тому оптимальний рівень аероіонізації вважається в межах від 150 до 5000 легких аерофонів на 1 см³.

Вплив на покращення складу робочого повітря здійснюється примусовою вентиляцією, застосуванням захисних екранів із заземленням або іонізаторів, а також можливістю регулювання основних параметрів мікроклімату.

2.2.2 Освітлення

Правильно організоване освітлення позитивно впливає на центральну нервову систему, сприяє зниженню енергетичних витрат організму під час виконання завдань і покращує продуктивність праці. Надмірне або недостатнє освітлення може призводити до перенапруження зору, втоми, зниження швидкості робочих процесів та, з часом, до розвитку захворювань очей, таких як короткозорість.

Тому освітлення робочих приміщень має відповідати нормам СниП II.4-79. Забезпечення рівномірного світлового потоку досягається за допомогою відбитого або розсіяного світла, яке слід поєднувати з природним освітленням, дотримуючись нормативного рівня в 300–500 лк. При цьому необхідно уникати відблисків від клавіатури, екрана та інших пристроїв, спрямованих у бік очей користувача.

2.2.3 Шум

Деякі пристрої, що працюють з ВДТ, можуть стати джерелами різних звукових коливань – як у чутному, так і в ультразвуковому діапазоні. Постійний або тривалий вплив такого шуму спричиняє зниження працездатності, погіршення концентрації, збільшення кількості помилок, зорову втому, зміну сприйняття кольорів та появу головного болю.

Нормативним показником для робочого місця є рівень шуму до 50 дБ, а для його зниження слід застосовувати заходи, як-от усунення причин шуму на етапі проектування, використання звукопоглинаючих матеріалів та оптимізація планування виробничих приміщень.

2.2.4 Вимоги до організації робочого місця працівника

Під час виконання паяльних робіт потрібно суворо дотримуватися норм організації робочого місця. Кожен елемент робочої зони має бути розташований так, щоб забезпечити максимальний комфорт і безпеку, усуваючи зайві предмети, які можуть створювати перешкоди.

Паяльне обладнання, робочі інструменти і деталі, а також засоби індивідуального захисту повинні перебувати у справному стані та відповідати стандартам охорони праці. Паяльні роботи проводяться з використанням електропаяльника, який живиться від мережі 220 В і має споживання не більше 100 Вт. Використання кислот або рідин на основі кислотних розчинів суворо заборонено.

Під час ремонтних робіт обладнання повинно бути повністю відключене від електроживлення (штк. вилка вилучається з розетки), а всі доступні елементи – ізольовані від мережі. Через застосування різних припоїв і флюсів, що містять шкідливі компоненти (свинець, цинк, літій, калій, натрій, кадмій тощо), робочі місця паяльників повинні бути обладнані додатковими локальними витяжними системами.

2.2.5 Електробезпека

Для запобігання ураженню електричним струмом необхідно чітко дотримуватися правил безпечного виконання робіт і експлуатації техніки. Оператор повинен бути захищений від доступу до частин обладнання, що працюють під високою напругою, а також до неізольованих елементів, які не підключені до захисного заземлення. Електроживлення комп'ютерної техніки має підключатися виключно через спеціальні штекери із заземленням.

2.3 Пожежна безпека

До систем гасіння пожеж належать як внутрішні пожежні водопроводи (крани-ПК), так і різні типи вогнегасників, зокрема вуглекислотні, порошкові, а також сухий пісок. У будівлях пожежні крани розташовують у коридорах та на сходових майданчиках; кожен кран комплектується пожежним рукавом і встановлюється у спеціальних ящиках, розташованих на певній висоті від підлоги.

На початкових стадіях пожеж застосовують вогнегасники, найбільш ефективними серед яких є вуглекислотні пристрої, що дозволяють не лише гасити загоряння, але й зберігати електрообладнання. Такі засоби мають бути розміщені у легкодоступних місцях, на відповідній висоті від підлоги. Крім того, виробничі приміщення повинні мати запасні виходи, де двері мають бути позначені освітленим написом «Запасний вихід», а схема евакуації – розміщена біля основного виходу.

До засобів гасіння пожежі відносяться внутрішні пожежні водопроводи, вогнегасники (вуглекислотні та порошкові), сухий пісок тощо. В будівлях пожежні крани встановлюють в коридорах, на майданчиках сходових кліток. Кожний пожежний кран укомплектований пожежним рукавом і розміщений у відповідних ящиках, які знаходяться на висоті 1,35 м від полу.

Пожежна безпека є комплексною системою заходів, спрямованих на запобігання займання, своєчасне виявлення пожежі та ефективне ліквідування загоряння. До основних засобів цього захисту відносяться як внутрішні пожежні

водопроводи, так і різноманітні типи вогнегасників: вуглекислотні, порошкові, а також засоби за основою сухого піску. У будівлях пожежні крани зазвичай розташовують у коридорах та на сходових майданчиках; кожен кран комплектується пожежним рукавом і встановлюється в спеціально обладнаних ящиках, оптимально розміщених на висоті приблизно 1,35 м від підлоги. Таке розташування забезпечує легкий доступ до засобів гасіння у разі надзвичайної ситуації.

На початкових стадіях загоряння застосовують вогнегасники, найбільш ефективними з яких є вуглекислотні пристрої. Вони дозволяють не лише швидко знищити загоряння, але й мінімізувати можливі пошкодження електрообладнання, що особливо важливо у виробничих приміщеннях. Водночас, стандартними засобами гасіння пожежі можуть виступати і порошкові вогнегасники, а також сухий пісок, які використовуються для локалізації загоряння до прибуття аварійних служб. Застосування цих пристроїв обов’язково повинно відповідати нормам безпеки та бути розміщено у відкритих, легкодоступних місцях.

Окрім технічних засобів, надзвичайне значення має організаційний аспект пожежної безпеки. Виробничі та громадські приміщення повинні бути забезпечені запасними виходами. Двері цих виходів повинні бути позначені яскравим, освітленим знаком «Запасний вихід», а поблизу – розміщеним планом евакуації, який чітко окреслює маршрути безпечного виходу з приміщення.

Сучасні технології протипожежного захисту передбачають встановлення систем автоматичного пожежного оповіщення та сигналізації. Детектори диму, теплові сенсори, а іноді й газоаналізатори, дозволяють оперативно виявити загоряння та розпочати автоматичну активацію систем гасіння. Такі системи значно скорочують час реагування і сприяють оперативному інформуванню всіх осіб, що знаходяться у приміщенні, що є критично важливим для збереження життя та мінімізації матеріальних збитків.

ВИСНОВКИ

У процесі дослідження було проведено комплексний аналіз сучасних криптографічних алгоритмів, що використовуються для захисту конфіденційної інформації в інформаційних системах. Робота охоплювала як теоретичні основи криптографії, так і практичні аспекти ефективності шифрування на прикладі симетричних (AES, DES, ChaCha20), асиметричних (RSA, ECC, постквантові алгоритми) та хеш-функцій.

За результатами аналізу встановлено, що:

1) симетричні алгоритми (особливо AES) демонструють високу швидкодію та надійність, тому широко застосовуються для шифрування великих обсягів даних;

2) асиметричні алгоритми ефективні для захисту каналів передачі ключів і цифрових підписів, проте поступаються симетричним за продуктивністю;

3) постквантові алгоритми набувають актуальності у зв’язку з розвитком квантових обчислень, хоча потребують додаткової стандартизації та оптимізації.

Практичне тестування показало, що навіть у межах одного типу алгоритмів швидкодія може залежати від довжини ключа, реалізації та обчислювального середовища. Було також розглянуто основні методики оцінки криптостійкості та типові загрози, серед яких: криптоаналітичні атаки, атаки сторонніми каналами, а також загрози з боку квантових обчислень.

Можна надати наступне рекомендація для використання систем шифрування:

1) для повсякденного захисту інформації в більшості систем рекомендується використовувати AES-256 з надійною генерацією ключів4

2) для забезпечення автентифікації і безпечного обміну ключами – ECC або гібридні схеми;

3) при підвищених вимогах до стійкості в майбутньому – поступовий перехід на постквантову криптографію (наприклад, CRYSTALS-Kyber, NTRU).

ПЕРЕЛІК ВИКОРИСТАНИХ ІНФОРМАЦІЙНИХ ДЖЕРЕЛ

1. Гулак Г.М. Методологія захисту інформації. Аспекти кібербезпеки: підручник/ Г.М. Гулак – К.: Видавництво НА СБ України, 2020. – 256 с.

2. Остапов С. Е. Технології захисту інформації: навчальний посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2013. – 476 с.

3. Методи та засоби захисту інформації: Навчальний посібник для студентів вищих навчальних закладів./А.М. Олейніков. –Харків: НТМТ, 2014. –298с.

4. Фізичні основи захисту інформації в радіоелектронній апаратурі: навч. посіб./ Д.В. Євграфов. –К.:НТУУ"КПІ", 2014. –176с.

5. Тестування на проникнення: навч. посіб. Ч.1 / [Є.О. Живило]; за ред. Є.О. Живило. –П.: ПНТУ “Полтавська політехніка ім. Юрія Кондратюка”,2024.–134 с.

6. Моніторинг інформаційних технологій [Електронний ресурс] – Режим доступу до ресурсу: https://pidru4niki.com/75828/ekonomika/monitoring_informatsiynih_tehnologiy.

7. Аудит інформаційних систем [Електронний ресурс] – Режим доступу до ресурсу: http://www.infocity.kharkov.ua/uk/static/audit-informatsiynih-sistem-49.html.

8. Ilyenko A. сучасні методи аудиту та моніторингу в задачах захисту інформації [Електронний ресурс] / Anna Ilyenko // Researchgate. – 2018. – Режим доступу до ресурсу: https://www.researchgate.net/publication/328828497_sucasni_metodi_auditu_ta_monitoringu_v_zadacah_zahistu_informacii.

9. Методи та засоби захисту інформації [Навчальний посібник] / В.А. Лахно, Є.В. Василіу, В.М. Гладких, В.М. Домрачев, Н.М. Сивкова. – К. : ФОП Ямчинський О.В., 2020. – 445 с.

10. Ряба Л.С. Основи кібербезпеки: навчальний посібник. Рівне: Вище професійне училище №1, 2021, 170 с.

11. Основи інформаційної безпеки: навч. посібник/ В.Б. Вишня, О.С. Гавриш, Е.В. Рижков. Дніпро: Дніпроп. держ. ун-т внутріш. справ, 2020,128 с.

ДОДАТОК А

Слайди мультимедійної презентації

1

АНАЛІЗ СУЧАСНИХ КРИПТОГРАФІЧНИХ АЛГОРИТМІВ ТА ЇХ ЕФЕКТИВНОСТІ У ЗАХИСТІ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ

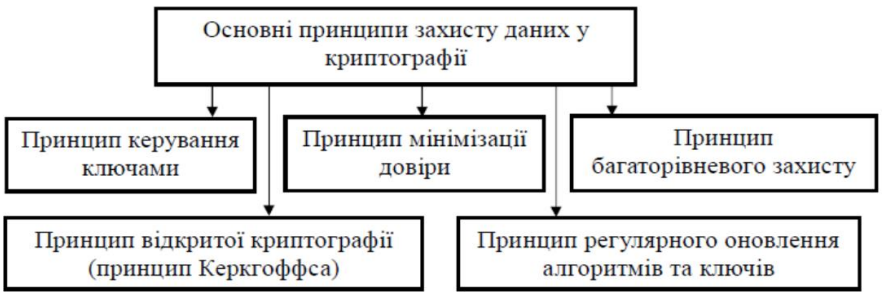
КВАЛІФІКАЦІЙНА РОБОТА

Дипломник: Мойсєєв В.В.
Керівник: Кільдішев В.Й.

2025

Основні принципи захисту даних у криптографії

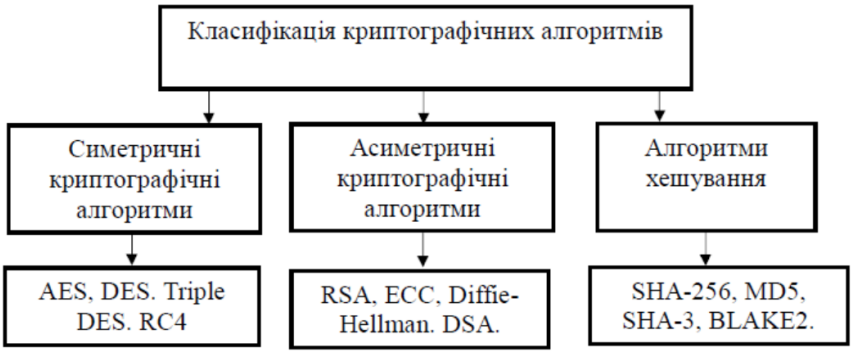
Розробка та використання криптографічних систем ґрунтується на певних фундаментальних принципах, які забезпечують їхню надійність: Принцип керування ключами; принцип мінімізації довіри; принцип відкритої криптографії; принцип багаторівневого захисту; принцип регулярного оновлення алгоритмів та ключів.



2

Класифікація криптографічних алгоритмів

Криптографічні алгоритми поділяються на кілька основних категорій залежно від принципів роботи та використання ключів. Основними типами криптографічних алгоритмів є симетричні алгоритми, асиметричні алгоритми та алгоритми хешування.



Порівняльний аналіз ефективності симетричних алгоритмів шифрування

AES – сучасний стандарт;
DES – застарілий;
3DES – покращений, але все ще повільний;
ChaCha20 – швидкий потоковий алгоритм, зручний для мобільних пристроїв;

Алгоритм	Тип	Довжина ключа	Розмір блоку	Швидкість (програмно)	Швидкість (апаратно)	Безпека
AES	Блоковий	128/192/256 біт	128 біт	Висока	Дуже висока (AES-NI)	Висока
DES	Блоковий	56 біт	64 біт	Низька	Низька	Дуже низька
3DES	Блоковий	168 біт	64 біт	Низька	Низька	Середня
ChaCha20	Потоковий	256 біт	-	Висока	Відсутня підтримка	Висока

Відмінності системи шифрування Калина від AES

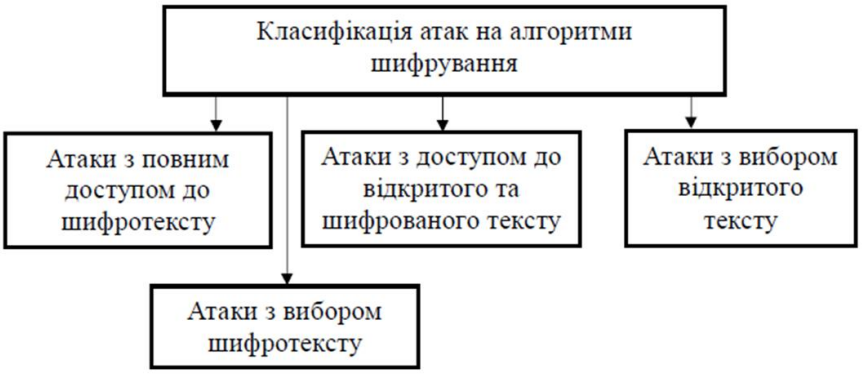
Характеристика	AES	Калина
Розмір блоку	128 біт	128 біт
Розмір ключа	128/192/256 біт	128/192/256 біт
Стандартизація	NIST (США)	ДСТУ (Україна)
Відкритість	Повністю відкритий	Повністю відкритий
Використання	Глобально	В основному в Україні
Принцип побудови	SP-мережа	SP-мережа
Ефективність	Висока	Оптимізована під українські потреби

Порівняльний аналіз ефективності асиметричних алгоритмів шифрування

RSA – поширений, але має низьку продуктивність;
ECC – більш ефективний за RSA, менші ключі за тієї ж стійкості, ефективний для мобільних систем;
Kyber, NTRU – новітні постквантові алгоритми;

Алгоритм	Ключова особливість	Довжина ключа	Швидкість	Безпека	Стійкість до квантових атак
RSA	Факторизація чисел	2048+ біт	Низька	Висока	Ні
ECC	Еліптичні криві	256 біт (≈ RSA-3072)	Висока	Вища за RSA	Ні
Kyber	Решітчасті проблеми	768+ біт	Середня	Висока	Так
NTRU	Поліноми	700+ біт	Висока	Висока	Так

Класифікація атак на алгоритми шифрування



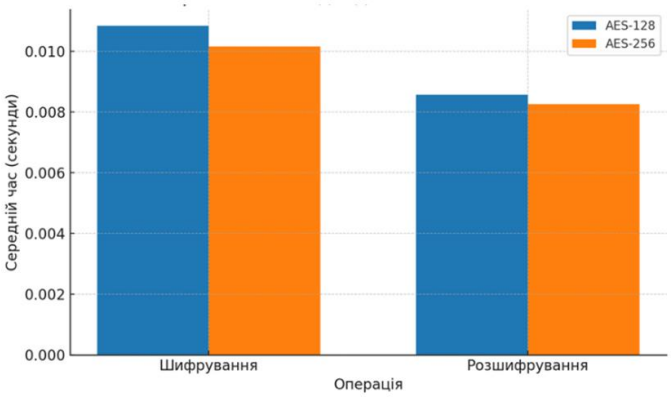
Порівняльна характеристика систем шифрування

Сучасні алгоритми шифрування демонструють високу криптостійкість при правильному впровадженні. Основні загрози походять не від математичної слабкості, а від помилок у реалізації, людського фактору, побічних каналів та майбутніх квантових загроз. Тому важливо не лише обирати надійний алгоритм, але й дотримуватись криптографічних стандартів та практик безпечної реалізації.

Алгоритм	Швидкодія	Стійкість до атак	Ресурси (пам'ять/процесор)	Придатність для IoT
RSA	Низька	Висока (без квантових)	Високі	Обмежена
ECC	Висока	Вища за RSA (без квантових)	Низькі	Висока
Kyber	Середня	Висока (з квантовим захистом)	Середні	Залежить від реалізації
McEliece	Низька	Дуже висока	Дуже високі	Низька

Загальні результати тестування систем шифрування AES 128 і AES 256

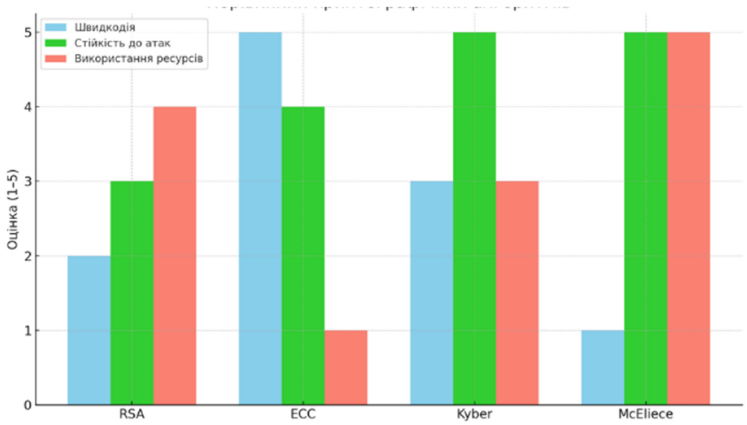
Розмір текст	AES 128		AES 256	
	Шифрування	Розшифрування	Шифрування	Розшифрування
малий	0,059255	0,000311	0,037329	0,000261
Великий – 1 Мбайт	0,010840	0,008566	0,010162	0,008259



Загальні рекомендації з приводу використання криптографічних методів захисту інформації

Компонент системи	Рекомендований криптографічний метод
Передача даних	TLS 1.3 із AES-256-GCM або ChaCha20
Хмарні сервіси	AES-256, ECC, токенізація
Мобільні додатки	ChaCha20-Poly1305, Curve25519, SHA-256
IoT/вбудовані системи	ECC (X25519), ChaCha20, легкі хеш-функції
Захист файлів	AES-256 з автентифікацією (наприклад, AES-GCM)
Цифровий підпис	EdDSA, RSA-PSS, ECDSA

Показники основних криптографічних алгоритмів за трьома критеріями: швидкодія, стійкість до атак і використання ресурсів



Дякую за увагу

ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

РЕЦЕНЗІЯ

на кваліфікаційну роботу бакалавра
відділення комп'ютерних систем

Мойсєєва Віктора Вікторовича

(прізвище, ім`я та по батькові)

Спеціальність *123 «Комп'ютерна інженерія»*

Керівник дипломного проекту (роботи) *Кільдішев Віталій Йосипович*

(прізвище, ім`я та по батькові)

Тема кваліфікаційної роботи бакалавра: *Аналіз сучасних криптографічних алгоритмів та їх ефективності у захисті конфіденційної інформації*

Обсяг розрахунково-пояснювальної записки *61* сторінок

Обсяг графічної частини проекту *12* аркушів

ХАРАКТЕРИСТИКА ДИПЛОМНОГО ПРОЄКТУ (РОБОТИ)

а) Висновок про ступінь відповідальності виконаного кваліфікаційної роботи бакалавра завданню

Робота відповідає технічному завданню до дипломного проекту. Виконана у відповідності з вимогами.

б) Характеристика виконання кожного розділу проекту ступеню використання дипломником останніх досягнень науки та техніки, передових методів на виробництві

При виконанні дипломної роботи студент продемонстрував уміння використовувати останні досягнення науки та техніки, уміння працювати з літературою. Так, студент грамотно дослідив та проаналізував криптографічні алгоритми та їх ефективність у захисті конфіденційної інформації.

в) Оцінка якості виконання графічної частини проєкту (роботи) і пояснювальної записки

Графічна частина відповідає вимогам, виконана якісно та відображає основні елементи проектування системи. Розглянуто роль і значення захисту інформації у сфері кібербезпеки, з акцентом на важливість шифрування даних.

г) Перелік позитивних якостей кваліфікаційної роботи бакалавра

Тема дипломної роботи є актуальною, виконана у достатньому обсязі, якісно, відповідно до поставленого завдання.

д) Основні недоліки кваліфікаційної роботи бакалавра

Присутні недоліки в оформлення пояснювальної записки та графічної частини. Для підвищення ефективності захисту конфіденційної інформації було б доцільним застосувати гібридні схеми автентифікації і безпечного обміну ключами. Було б доцільним більш детально розглянути особливості постквантової криптографії.

Оцінка розрахункової частини *Добре*

Оцінка графічної частини *Добре*

Загальна оцінка *Добре*

Прізвище, ім`я по батькові *к.т.н. Рудніченко Микола Дмитрович*

23.06.25 р.

Місце роботи і посада рецензента *Національний університет «Одеська політехніка», доцент кафедри інформаційних технологій*

ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

ВІДГУК

керівника на кваліфікаційну роботу бакалавра

відділення комп'ютерних систем

Мойсєєва Віктора Вікторовича

(прізвище, ім`я та по батькові)

Спеціальність *123 «Комп'ютерна інженерія»*

Тема кваліфікаційної роботи бакалавра

Аналіз сучасних криптографічних алгоритмів та їх ефективності у захисті конфіденційної інформації

ХАРАКТЕРИСТИКА ДИПЛОМНОГО ПРОЄКТУ (РОБОТИ)

а) Обсяг і якість виконання роботи (графічного матеріалу і розрахунково-пояснювальної записки)

Пояснювальна записка виконана якісно, у достатньому обсязі, відповідно до індивідуального завдання та теми дипломного проекту, розділи пояснювальної записки відповідають етапам рішення завдання, поставленого у дипломному проекті

Графічний матеріал виконано якісно, у достатньому обсязі. Графічний матеріал наочно демонструє результати роботи.

б) Самостійність роботи над проєктом (роботою)

Студент самостійно обрав напрям та тематику дипломного проекту. Провів аналіз існуючих рішень і зробив необхідні висновки для реалізації проекту. Виявив навички самостійно опрацьовувати новий матеріал та виконувати пошук необхідної літератури та інших джерел інформації.

в) Теоретична підготовка дипломника_____
відповідає вимогам, що надаються до бакалавра зі спеціальності_____
«Комп'ютерна Інженерія»_____

г) Вміння розв`язувати виробничі і конструкторські питання на базі останніх досліджень науки і техніки, передових методів виробництва_____
У кваліфікаційній роботі досліджуються сучасні криптографічні алгоритми. Предметом дослідження є ефективність криптографічних методів у захисті конфіденційної інформації. У роботі застосовуються методи теоретичного аналізу літературних джерел, порівняльний аналіз криптографічних алгоритмів, методи математичного моделювання та практичне тестування продуктивності алгоритмів.

Оцінка розрахункової частини 4 (чотири)
Оцінка графічної частини 4 (чотири)
Загальна оцінка 4 (чотири)

Прізвище, ім`я, по батькові Кільдішев Віталій Йосипович

Місто роботи і посада керівника роботи к.т.н., доцент кафедри кібербезпеки та технічного захисту інформації ДУІТЗ

Підпис _____
«20» червня 2025р.

ДОЗВІЛ
НА РОЗМІЩЕННЯ
ВИПУСКНОЇ КВАЛІФІКАЦІЙНОЇ РОБОТИ
В ЕЛЕКТРОННОМУ РЕПОЗИТАРІЇ ВСП «ОТФК ОНТУ»

Ми, що нижче підписалися,

Мойсєєв Віктор Вікторович,

здобувач освіти гр. 2БКС-29, та

Кільдішев Віталій Йосипович,
керівник випускної кваліфікаційної роботи,

не заперечуємо щодо розміщення електронного варіанту пояснювальної записки до випускної кваліфікаційної роботи бакалавра на тему:

«Аналіз сучасних криптографічних алгоритмів та їх ефективності у захисті конфіденційної інформації» (автор роботи – Мойсєєв В.В., керівник роботи – Кільдішев В.Й.)

виконаного у ВСП «Одеський технічний фаховий коледж Одеського національного технологічного університету» в 2025 році, у повному обсязі в електронному репозитарії ВСП «ОТФК ОНТУ» для вільного доступу через мережу Інтернет.

Несемо відповідальність за ідентичність електронного та друкованого варіантів випускної кваліфікаційної роботи і даємо згоду на обробку персональних даних.

Виконавець _____ / Мойсєєв В.В. /

Керівник _____ / Кільдішев В.Й. /

«18» червня 2025 р.

ДОВІДКА

кафедри комп'ютерної інженерії
про допуск до захисту кваліфікаційної роботи
здобувача (здобувачки) освіти II курсу
відділення комп'ютерних систем групи 2БКС-29

Мойсєєва Віктора Вікторовича

на тему *Аналіз сучасних криптографічних алгоритмів та їх ефективності у захисті конфіденційної інформації*

Висновок відповідальної особи за проведення нормоконтролю:

пояснювальна записка до кваліфікаційної роботи виконана з деякими порушеннями ДСТУ та оформлена відповідно до вимог Положення про дипломне проєктування

(підпис)	*23.06.2025* (дата)	*Петрашова В.І.* (П.І.Б.)

Висновок відповідальної особи за перевірку роботи на наявність академічного плагіату *згідно звіту про перевірку від 15.06.2025 р. значення коефіцієнту подібності в роботі становить 8,23%, коефіцієнт цитування – 1,39%.*

(підпис)	*23.06.2025* (дата)	*Краснокутська К.Г.* (П.І.Б.)

Попередня експертиза (малий захист) кваліфікаційної роботи

здобувача (здобувачки) освіти *Мойсєєва В.В.* (П.І.Б.)

проведена «*23*» *червня* 20*25* р.

Висновки *Пояснювальна записка до кваліфікаційної роботи виконана у повному обсязі. Випускна кваліфікаційна робота відповідає вимогам Положення про дипломне проєктування та рекомендована до захисту.*

Зав. кафедри КІ _____ (підпис) *Іванова Л.В.* (П.І.Б.)

StrikePlagiarism.com

Дата звіту 6/15/2025
Дата редагування 6/15/2025

Документ прийнятий

Звіт подібності

метадані

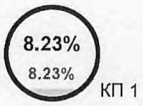
Назва організації
Odesa Technical Professional College of Odesa National University of Technology
Заголовок
Аналіз сучасних криптографічних алгоритмів та їх ефективності у захисті конфіденційної інформації

Автор Науковий керівник / Експерт
Мойсєєв Віктор ВікторовичКільдішев Віталій Йосипович

підрозділ
Відокремлений структурний підрозділ "Одеський технічний фаховий коледж Одеського національного технологічного університету"

Обсяг знайдених подібностей

Коефіцієнт подібності визначає, який відсоток тексту по відношенню до загального обсягу тексту було знайдено в різних джерелах. Зверніть увагу, що високі значення коефіцієнта не автоматично означають плагіат. Звіт має аналізувати компетентна / уповноважена особа.



КП 1

КЦ

25
Довжина фрази для коефіцієнта подібності 2

10914
Кількість слів

89878
Кількість символів

Тривога

У цьому розділі ви знайдете інформацію щодо текстових спотворень. Ці спотворення в тексті можуть говорити про МОЖЛИВІ маніпуляції в тексті. Спотворення в тексті можуть мати навмисний характер, але частіше характер технічних помилок при конвертації документа та його збереженні, тому ми рекомендуємо вам підходити до аналізу цього модуля відповідально. У разі виникнення запитань, просимо звертатися до нашої служби підтримки.

Заміна букв	ß	6
Інтервали	A→	0
Мікропробіли	·	0
Білі знаки	ß	0
Парафрази (SmartMarks)	a	42

Подібності за списком джерел

Нижче наведений список джерел. В цьому списку є джерела із різних баз даних. Колір тексту означає в якому джерелі він був знайдений. Ці джерела і значення Коефіцієнту Подібності не відображають прямого плагіату. Необхідно відкрити кожне джерело і проаналізувати зміст і правильність оформлення джерела.

10 найдовших фраз — Колір тексту

ПОРЯДКОВИЙ НОМЕР	НАЗВА ТА АДРЕСА ДЖЕРЕЛА URL (НАЗВА БАЗИ)	КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ)
1	https://card-file.ontu.edu.ua/server/api/core/bitstreams/d5a3d14f-d5cb-460f-9c49-cba3f9d50554/content	103 0.94 %
2	https://card-file.ontu.edu.ua/bitstreams/361286d7-8a03-4221-ad05-db5133ab5f79/download	52 0.48 %
3	https://card-file.ontu.edu.ua/bitstreams/035f6436-20b4-4ee6-8e99-bede670e308b/download	45 0.41 %
4	https://card-file.ontu.edu.ua/bitstreams/361286d7-8a03-4221-ad05-db5133ab5f79/download	32 0.29 %
5	https://nubip.edu.ua/sites/default/files/u34/rp_ziks_2023-2024_125_bak.pdf	26 0.24 %

6	https://card-file.ontu.edu.ua/bitstreams/0e6c3361-ffbf-4469-86a1-fe84a1fe21cd/download	23 0.21 %
7	https://www.wunu.edu.ua/opp/fkit/kiberbezpeka_bakalavr/normatuvni/1-year/OsnovyKiberbezpeky/Work.pdf	21 0.19 %
8	https://bmet.org.ua/biblioteka/spetsialnist-122-komp-yuterni-nauki/vibirkovi-distsiplini/	20 0.18 %
9	https://card-file.ontu.edu.ua/bitstreams/549ee9fe-7574-4ae5-b500-9fe2711f33e6/download	19 0.17 %
10	http://ptcsi.chnu.edu.ua/wp-content/uploads/2020/05/%D0%97%D0%B1%D1%96%D1%80%D0%BD%D0%B8%D0%BA%D0%9F%D1%80%D0%B0%D1%86%D1%8C%D0%86%D0%A4%D0%A2%D0%9A%D0%9D19.pdf	18 0.16 %

з домашньої бази даних (0.13 %)

ПОРЯДКОВИЙ НОМЕР	ЗАГОЛОВОК	КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ)
1	Розробка 3D-гри у жанрі survival-horror з налаштуваннями рівнів складності [redacted] 6/12/2025 Odesa Technical Professional College of Odesa National University of Technology (Відокремлений структурний підрозділ "Одеський технічний фаховий коледж Одеського національного технологічного університету")	8 (1) 0.07 %
2	Розробка системи авторизації користувача на web-сервері за допомогою nrf-модулю [redacted] 6/15/2025 Odesa Technical Professional College of Odesa National University of Technology (Відокремлений структурний підрозділ "Одеський технічний фаховий коледж Одеського національного технологічного університету")	6 (1) 0.05 %

з програми обміну базами даних (2.68 %)

ПОРЯДКОВИЙ НОМЕР	ЗАГОЛОВОК	КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ)
1	Парфьонов_Ярослав_КНТ4курс_Диплом6 [redacted] 6/9/2024 Interregional Academy of Personnel Management (Інститут комп'ютерно-інформаційних технологій та дизайну)	253 (26) 2.32 %
2	Галалай_Превисокова [redacted] 12/7/2024 Vasyl Stefanyk Precarpathian National University (VSPNU) (VSPNU)	15 (1) 0.14 %
3	Домрачев-диплом(1) [redacted] 3/26/2025 Interregional Academy of Personnel Management (Інститут комп'ютерно-інформаційних технологій та дизайну)	12 (1) 0.11 %
4	Сябрай Максим ВКБР Програмне забезпечення обміну повідомленнями з шифруванням н.кер. Захаренков Д.Ю. [redacted] 5/23/2025 European University (European University)	12 (1) 0.11 %

з Інтернету (5.42 %)

ПОРЯДКОВИЙ НОМЕР	ДЖЕРЕЛО URL	КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ)
1	**https://card-file.ontu.edu.ua/bitstreams/361286d7-8a03-4221-ad05-db5133ab5f79/download**	**105 (5) 0.96 %**
2	**https://card-file.ontu.edu.ua/server/api/core/bitstreams/d5a3d14f-d5cb-460f-9c49-cba3f9d50554/content**	**103 (1) 0.94 %**
3	**https://card-file.ontu.edu.ua/bitstreams/035f6436-20b4-4ee6-8e99-bede670e308b/download**	**45 (1) 0.41 %**

4	https://card-file.ontu.edu.ua/bitstreams/fe683780-2cc9-4de1-8add-77245c815d4a/download	45 (5) 0.41 %
5	https://bmet.org.ua/biblioteka/spetsialnist-122-komp-yuterni-nauki/vibirkovi-distsiplini/	35 (2) 0.32 %
6	**https://nubip.edu.ua/sites/default/files/u34/rp_ziks_2023-2024_125_bak.pdf**	**33 (2) 0.30 %**
7	https://card-file.ontu.edu.ua/bitstreams/0e6c3361-ffbf-4469-86a1-fe84a1fe21cd/download	32 (2) 0.29 %
8	http://ptcsi.chnu.edu.ua/wp-content/uploads/2020/05/%D0%97%D0%B1%D1%96%D1%80%D0%BD%D0%B8%D0%BA%D0%9F%D1%80%D0%B0%D1%86%D1%8C%D0%86%D0%A4%D0%A2%D0%9A%D0%9D19.pdf	30 (3) 0.27 %
9	https://www.wunu.edu.ua/opp/fkit/kiberbezpeka_bakalavr/normatuvni/1-year/OsnovyKiberbezpeky/Work.pdf	21 (1) 0.19 %
10	https://ur.knute.edu.ua/bitstreams/87306f7d-5199-48a9-b4b9-44a707c9bbad/download	19 (2) 0.17 %
11	https://card-file.ontu.edu.ua/bitstreams/549ee9fe-7574-4ae5-b500-9fe2711f33e6/download	19 (1) 0.17 %
12	https://nuos.edu.ua/wp-content/uploads/2024/12/VK4_semestr-4_Informacijna-bezpeka-derzhavi_Bortnik.pdf	17 (1) 0.16 %
13	https://cryptology.school/blog/kriptografiia-ta-sifruvannia	16 (2) 0.15 %
14	https://card-file.ontu.edu.ua/bitstreams/538ada8a-2c79-4b1e-b7d2-b0c97f68bc1c/download	13 (1) 0.12 %
15	https://www.mogroup.com.ua/?p=855	12 (1) 0.11 %
16	https://card-file.ontu.edu.ua/bitstreams/7b1e10b9-0ac2-4b07-afc4-8cdfff7db780/download	11 (1) 0.10 %
17	https://card-file.ontu.edu.ua/bitstreams/f789da43-3034-4ad8-bf34-640a47414f93/download	10 (1) 0.09 %
18	https://studfile.net/preview/5200038/	10 (1) 0.09 %
19	https://vnu.edu.ua/sites/default/files/2024-01/%D0%9E%D0%9A_17_%D0%A2%D0%B5%D1%85%D0%BD_%D0%B7%D0%B0%D1%85_%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC_2020.pdf	10 (2) 0.09 %
20	https://card-file.ontu.edu.ua/bitstreams/e69af76d-3a8e-40fc-90cc-64aee3d75f68/download	6 (1) 0.05 %

Список прийнятих фрагментів (немає прийнятих фрагментів)

ПОРЯДКОВИЙ НОМЕР	ЗМІСТ	КІЛЬКІСТЬ ОДНАКОВИХ СЛІВ (ФРАГМЕНТІВ)

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

Спеціальність: 123 «Комп'ютерна інженерія»_
Освітньо-професійна програма: **«Комп'ютерна інженерія» Група:** 2БКС- 29

КВАЛІФІКАЦІЙНА
РОБОТА

здобувача **освіти денної форми навчання** БКС. 29.16.000. КРБ

МОЙСЄЄВА ВІКТОРА
ВІКТОРОВИЧА

м. Одеса
2025 р. **МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»**

Спеціальність: 123 «Комп'ютерна інженерія»_