ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Технології застосування криптографічних алгоритмів з відкритим та закритим ключем в інформаційній системі організації»

зі спеціальності *125 Кібербезпека та захист інформації*
(код, найменування спеціальності)

освітньо-професійної програми *Інформаційна та кібернетична безпека*
(назва програми)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Данило БИШУК
(підпис)

Виконав: здобувач вищої освіти групи БСДМ-61
БИШУК Данило
(прізвище, ім'я)

Керівник д.т.н., професор КОЖУХІВСЬКИЙ Андрій
(науковий ступінь, вчене звання, прізвище, ім'я)

Рецензент _____
(науковий ступінь, вчене звання, прізвище, ім'я)

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

Кафедра Систем та технологій кібербезпеки
Ступінь вищої освіти Магістр
Спеціальність 125 Кібербезпека та захист інформації
Освітньо-професійна програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ
Завідувач кафедри
Систем та технологій
кібербезпеки
_____ Галина ГАЙДУР
“___” жовтня 2024 року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

БИШУКУ Данилу Вікторовичу
(прізвище, ім’я)

1. Тема кваліфікаційної роботи: «Технології застосування криптографічних алгоритмів з відкритим та закритим ключем в інформаційній системі організації»

керівник кваліфікаційної роботи Кожухівський Андрій Дмитрович, д.т.н., проф.
(прізвище, ім’я, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від « 15 » жовтня 2024 року № 320 .

2. Строк подання здобувачем вищої освіти кваліфікаційної роботи 15.12.2024 р.

3. Вихідні дані до кваліфікаційної роботи
інформаційні ресурси організації;
платформи та рішення для використання криптоалгоритмів;
наукова та технічна література, експлуатаційна документація, нормативні документи, міжнародні стандарти.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Дослідження теоритичної основи використання криптографічних алгоритмів у інформаційних системах.
2. Аналіз практичного застосування криптографічних алгоритмів з відкритим та закритим ключем у інформаційних системах.

3. Технології впровадження криптографічних алгоритмів.

5. Перелік графічного матеріалу
1. Тема кваліфікаційної роботи.
2. Об’єкт, предмет, мета та наукові завдання.
3. Результати дослідження теоритичої основи використання критографічних алгоритмів.
4. Результати аналізу практичного застосування критографічних алгоритмів з відриктим та закритим ключем у інформаційних системах.
5. Демонстрація технолгій впровадження криптографічних алгоритмів.
6. Рекомендації щодо імлементації криптографічних алгоритмів у Інформаційну систему організації.
7. Висновки на основі досліджень.

6. Дата видачі завдання 01.10.2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Визначення актуальності проблеми захисту інформаційних систем організації.	01.10.2024 р.	
2.	Аналіз наукової та технічної літератури з питань теми кваліфікаційної роботи.	12.10.2024 р.	
3.	Аналіз методів та засобів захисту з використанням криптографічних алгоритмів.	27.10.2024 р.	
4.	Технології впровадження криптографічних алгоритмів.	03.11.2024 р.	
5.	Розроблення рекомендацій щодо застосування криптографічних алгоритмів в інформаційних системах.	15.11.2024 р.	
6.	Оформлення результатів дослідження.	26.11.2024 р.	
7.	Підготовка доповіді до захисту.	15.12.2024 р.	

Здобувач вищої освіти _____ Данило Бишук
(підпис) *(ім’я, прізвище)*

Керівник кваліфікаційної роботи _____ Андрій КОЖУХІВСЬКИЙ
(підпис) *(ім’я, прізвище)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну роботу

здобувача БИШУКА Данила

на тему: «Технології застосування криптографічних алгоритмів з відкритим та закритим ключем в інформаційній системі організації»

Актуальність: Зростання кіберзагроз і несанкціонованого доступу до даних ставить під загрозу інформаційну безпеку організацій. У цих умовах впровадження криптографічних алгоритмів є критично важливим для забезпечення конфіденційності, цілісності та доступності даних. Постійна еволюція кіберзагроз вимагає вдосконалення методів захисту, що робить розробку рекомендацій і впровадження сучасних криптографічних рішень актуальною та необхідною для забезпечення стійкості інформаційних систем.

Необхідно зауважити, що впровадження та використання технологій застосування криптографічних алгоритмів стає необхідною для забезпечення ефективного захисту інформації в організації, враховуючи постійну еволіцію кіберзагроз у сучасному світі. Тому, тема кваліфікаційної роботи є актуальною та своєчасною.

Позитивні сторони:

1. На основі проведеного аналізу, в роботі було встановлено зміст процесу захисту інформації за допомогою криптографічних алгоритмів, визначено мету та завдання різних видів шифрування, а також його складові частини.
2. Досліджено методи та засоби захисту даиих із застосуванням криптографічниї алгоритмів з відкритим та закритим ключем в інформаційній системі організації.
3. Розглянуто приклади використання криптоалгоритмів в реальних інформаціних системах та рекомендації щодо їх імплементації.
4. Текст викладено достатньо грамотно, послідовно. Сформульовано чіткі та змістовні висновки. Графічний матеріал оформлено якісно. Список науково-технічної літератури свідчить про вміння користуватись матеріалами за темою кваліфікаційної роботи.

Недоліки:

1. У кваліфікаційній роботі бажано було б провести детальний аналіз умови застосування криптографічних алгоритмів з відкритим та закритим ключем у конкретних корпоративних додатках.
2. Запропонований порядок застосування технології застосування криптографічних алгоритмів з відритим та закритим ключем бажано було б показати на прикладі конкретної організації.

Відзначені зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: Враховуючи недоліки, кваліфікаційна робота заслуговує оцінку **“добре”**, а здобувач(ка) **БИШУК Данило** – присвоєння кваліфікації магістр з кібербезпеки за освітньо-професійною програмою інформаційна та кібернетична безпека.

Рецензент:

(науковий ступінь, вчене звання)	*(підпис)*	*(ім’я, прізвище)*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ

Направляється здобувач БИШУК Данило до захисту кваліфікаційної роботи
(прізвище, ім'я)
спеціальності 125 Кібербезпека та захист інформації
освітньо-професійної програми Інформаційна та кібернетична безпека
(шифр і назва спеціальності)
на тему: «Технології застосування криптографічних алгоритмів з відкритим та закритим ключем в інформаційній системі організації».
Кваліфікаційна робота і рецензія додаються.

Директор інституту _____ Євгенія ІВАНЧЕНКО
(підпис) *(ім'я, прізвище)*

Висновок керівника кваліфікаційної роботи

Здобувач ***БИШУК Данило*** обрав тему роботи, метою якої було дослідити зміст технологій застосування криптографічних алгоритмів з відкритим та закритим ключем в інформаційній системі організації та розробка рекомендацій щодо їх реалізації. Перелік використаних джерел свідчить про вміння здобувачем розбиратись в наукових питаннях та застосовувати їх при дослідженнях. Під час виконання кваліфікаційної роботи ***БИШУК Данило*** показав добру теоретичну та практичну підготовку, вміння самостійно вирішувати питання і робити висновки. Роботу виконував сумлінно, акуратно та вчасно за планом.

Все це дозволяє оцінити виконану кваліфікаційну роботу здобувача ***БИШУКА Данила*** на оцінку **"добре"** та присвоїти йому кваліфікацію магістр з кібербезпеки за освітньою програмою інформаційна та кібернетична безпека.

Керівник кваліфікаційної роботи _____ Андрій Кожухівський
(підпис) *(ім'я, прізвище)*
"____" _____ 2024 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач **БИШУК Данило** допускається до захисту даної кваліфікаційної роботи в Екзаменаційній комісії.

Завідувач кафедри Систем та технологій кібербезпеки
(назва)
_____ Галина ГАЙДУР
(підпис) *(ім'я, прізвище)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи: 75 сторінка, 8 рисунків, 1 таблиця, 24 джерела.

Об'єкт дослідження – застосування криптографічних алгоритмів в інформаційних системах організацій.

Предмет дослідження – технології застосування криптографічних алгоритмів з відкритим та закритим ключем для захисту інформації.

Мета роботи – дослідити ефективність використання криптографічних алгоритмів з відкритим та закритими ключем та розробити рекомендації щодо їх застосування в інформаційних системах організацій.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння.

У кваліфікаційній роботі висвітлено основні аспекти застосування криптографічних алгоритмів у забезпеченні інформаційної безпеки організацій. Розглянуто концепції та класифікацію криптографічних алгоритмів, включаючи симетричні та асиметричні методи шифрування.

Досліджено нормативно-правову базу у сфері криптографії та визначено перспективи її розвитку з урахуванням сучасних викликів кібербезпеки. Виконано аналіз основних загроз інформаційній безпеці в інформаційних системах, зокрема вразливості, що можуть виникати при застосуванні криптографічних протоколів.

У роботі проведено оцінку ефективності алгоритмів, таких як RSA та AES, а також протоколів SSL/TLS, у реальних умовах їх застосування. Досліджено можливості інтеграції криптографічних алгоритмів у програмне забезпечення для захисту корпоративних інформаційних систем.

На основі досліджень, проведених в роботі, розроблено рекомендації для вибору та впровадження криптографічних алгоритмів у організаціях, зокрема щодо створення політики управління ключами, захисту від компрометації ключів та застосування сучасних протоколів безпеки..

Галузь використання – кібербезпека інформаційних ресурсів організації.

ІНФОРМАЦІЙНІ РЕСУРСИ ОРГАНІЗАЦІЇ, КРИПТОГРАФІЧНІ АЛГОРИТМИ, СИМЕТРИЧНЕ ТА АСИМЕТРИЧНЕ ШИФРУВАННЯ, ПОЛІТИКА УПРАВЛІННЯ КЛЮЧАМИ.

ABSTRACT

Text part of the qualification work: 75 pages, 8 figures, 1 table, 24 sources.

Object of research – the application of cryptographic algorithms in organizational information systems.

Subject of research – technologies for applying public and private key cryptographic algorithms for information protection.

The aim of research – to investigate the effectiveness of using cryptographic algorithms with public and private keys and develop recommendations for their application in organizational information systems.

Research methods – study of the literature on this topic, analysis of operational documentation, international standards and their comparison.

The thesis covers the key aspects of using cryptographic algorithms in ensuring the information security of organizations. The concepts and classification of cryptographic algorithms, including symmetric and asymmetric encryption methods, are discussed.

The regulatory framework in the field of cryptography is analyzed, and the prospects for its development are identified, considering the current challenges of cybersecurity. An analysis of the main threats to information security in information systems is performed, including vulnerabilities that may arise when using cryptographic protocols.

The work evaluates the effectiveness of algorithms such as RSA and AES, as well as SSL/TLS protocols, in real-world conditions of their application. The potential for integrating cryptographic algorithms into software to protect corporate information systems is explored.

Based on the research conducted, recommendations for the selection and implementation of cryptographic algorithms in organizations are developed, including the creation of key management policies, protection against key compromise, and the use of modern security protocols.

Field of application – cybersecurity of information resources of the organization.

INFORMATION RESOURCES OF THE ORGANIZATION, HYBRID WORK, SASE, TECHNOLOGY FOR ENSURING THE SECURE WORK OF HYBRID WORKERS

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

КА – Криптографічний Алгоритм

RSA – Rivest, Shamir и Adleman

NIST– Національний інститут стандартів і технологій

DES – Стандарт шифрування даних

TRIPLE DES – Потрійний стандарт шифрування даних

AES – Розширений стандарт шифрування

PKI – Інфраструктури відкритих ключів

SSL – Secure Sockets Layer

EV – Розширена перевірка

IDEA – Міжнародний алгоритм шифрування даних

VPN – Віртуальна приватна мережа

ЕЦП – Електронний цифровий підпис

ВСТУП

Актуальність дослідження.

У сучасному світі криптографічні алгоритми з відкритими та закритими ключами є основою захисту даних в інформаційних системах. Зростання обсягу цифрової інформації, її постійна циркуляція між різними системами, а також зростання загроз кібербезпеки вимагають впровадження ефективних методів шифрування для захисту конфіденційності, цілісності та доступності даних.

Сьогодні більшість організацій стикаються з проблемою підвищення рівня безпеки обміну даними. Розширення застосування таких технологій, як електронний цифровий підпис, захищені канали зв'язку та системи управління ключами, створює нові виклики для фахівців з інформаційної безпеки. Однак, багато організацій досі використовують застарілі або недостатньо ефективні моделі криптографічного захисту, що підвищує ризик компрометації інформації.

У світовій практиці застосування криптографічних алгоритмів стрімко розвивається, але для України впровадження цих технологій є ще актуальнішим у зв'язку зі значним збільшенням кіберзагроз, зокрема спрямованих на державні установи та підприємства. Недостатній рівень використання сучасних криптографічних методів в українських організаціях визначає потребу в поглибленому вивченні та розробці рекомендацій щодо їхнього застосування в інформаційних системах.

Актуальність даної роботи полягає в необхідності вдосконалення методів криптографічного захисту даних, що стає критично важливим для забезпечення безпеки інформаційних систем у цифровому світі. Використання криптографії з відкритими та закритими ключами у різних секторах дозволить не тільки ефективно захищати дані, але й забезпечити надійний захист в умовах цифрової трансформації, що є важливим для зміцнення глобального рівня інформаційної безпеки.

Вищесказане визначає актуальність теми даної кваліфікаційної роботи,

основний зміст якої становлять дослідження технологій застосування

криптографічних алгоритмів з відкритим та закритим ключем в інформаційній системі організації.

Об'єкт дослідження – застосування криптографічних алгоритмів в інформаційних системах організацій.

Предмет дослідження – технології застосування криптографічних алгоритмів з відкритим та закритим ключем для захисту інформації.

Мета роботи – дослідити ефективність використання криптографічних алгоритмів з відкритим та закритими ключем та розробити рекомендації щодо їх застосування в інформаційних системах організацій.

Наукові завдання:

провести аналіз сучасних проблем та загроз в області інформаційної безпеки.

розглянути основи функціонування криптографічних алгоритмів з відкритими та закритими ключами.

проаналізувати існуючі підходи до впровадження цих алгоритмів у практичній діяльності.

дослідити ефективність сучасних криптографічних рішень у контексті захисту даних.

розробити рекомендації для впровадження криптографічних алгоритмів в інформаційні системи організацій.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння.

Практичне значення одержаних результатів: запропоновано методику застосування криптографічних алгоритмів з відкритим та закритим ключем для забезпечення безпеки інформаційних систем організації, а також розроблено рекомендації фахівцям з кібербезпеки щодо ефективної її реалізації.

1 ДОСЛІДЖЕННЯ ТЕОРИТИЧНОЇ ОСНОВИ ВИКОРИСТАННЯ КРИПТОГРАФІЧНИХ АЛГОРИТМІВ У ІНФОРМАЦІЙЦНИХ СИСТЕМАХ

Криптографія є невід'ємною частиною сучасних інформаційних систем і відіграє ключову роль у забезпеченні безпеки даних постійно зростає, а разом з ними зростають і загрози кібербезпеки. Враховуючи такі виклики, роль криптографії у захисті інформації стає дедалі більш значущою. Шифрування даних з використанням різних криптографічних алгоритмів допомагає гарантувати конфіденційність, цілісність та автентичність переданої інформації, що є важливим аспектом для захисту як приватних даних, так і корпоративних систем.

Сучасні криптографічні методи включають як симетричні, так і асиметричні алгоритми, кожен з яких має свої переваги та недоліки, що залежить від конкретних умов їх використання. Симетричні алгоритми забезпечують високу швидкість шифрування, але мають обмеження в безпеці при неадекватному управлінні ключами. Асиметричні алгоритми, в свою чергу, використовують пару ключів, що дозволяє забезпечити більш високий рівень захисту, але є більш ресурсозатратними в плані часу обробки даних. Кожен з цих методів вимагає детального розуміння принципів криптографії та їх практичного застосування в інформаційних системах.

Зважаючи на постійне зростання складності атак, криптографія повинна розвиватися разом з технологічними досягненнями. Проте важливо зазначити, що ефективність криптографічного захисту також залежить від належного впровадження та налаштування механізмів безпеки, що включають використання сучасних стандартів і протоколів. Окрім цього, важливим аспектом є правильне управління криптографічними ключами, яке забезпечує високий рівень захисту даних у будь-якому середовищі

У цьому розділі буде здійснено детальний аналіз теоретичних основ використання криптографічних алгоритмів, зокрема їх класифікації та нормативно-правової бази, що регулює їх застосування. Особлива увага буде приділена

сучасним криптографічним алгоритмам, їх перевагам та проблемам, що виникають при їх впровадженні в організаційні інформаційні системи.

1.1 Поняття та класифікація криптографічних алгоритмів

Криптографія — це наука про математичні методи захисту інформації шляхом її перетворення в такий вигляд, що унеможливлює доступ до неї без відповідного ключа або спеціального методу дешифрування.

Криптографія може бути сильною або слабкою, сила криптографії вимірюється часом і ресурсами, необхідними для відновлення відкритого тексту. Результат сильної криптографії — це шифротекст, який надзвичайно складно розшифрувати без відповідного інструменту для декодування. З урахуванням сучасної обчислювальної потужності й доступного часу — навіть мільярд комп’ютерів, які виконують мільярд перевірок на секунду, не зможуть розшифрувати сильне шифрування до кінця існування Всесвіту.[1]

Криптографічний алгоритм — це математична функція, яка використовується у процесі шифрування та дешифрування. Криптографія передбачає використання спеціальних алгоритмів для трансформації відкритих даних (plaintext) у шифрований формат (ciphertext), який можна лише розшифрувати за допомогою певного ключа або методу. Процес шифрування та дешифрування залежить від типу криптографічного алгоритму, який використовується в конкретній ситуації.

Шифрування - це процес перетворення вихідної інформації (зрозумілої для користувача) у незрозумілий або нечитаний формат, який називається шифротекстом. Шифрування використовує різні алгоритми та ключі для перетворення даних таким чином, щоб вони могли бути прочитані або відновлені лише за допомогою відповідного ключа.

Криптографічні алгоритми використовуються для забезпечення конфіденційності, цілісності та автентичності даних у різних сферах, таких як телекомунікації, електронна комерція, захист персональних даних та державна безпека. Основною метою цих алгоритмів є перетворення відкритої інформації в зашифровану форму, що робить її доступною лише для осіб з відповідними правами доступу.

Основними елементами криптографії є:

- Конфіденційність: криптографічні алгоритми дозволяють шифрувати дані таким чином, що лише уповноважені особи можуть отримати доступ до вихідного вмісту. Шифрування забезпечує конфіденційність інформації шляхом перетворення її на незрозумілу форму для сторонніх осіб.
- Цілісність: криптографія також гарантує цілісність даних, тобто запобігає їх несанкціонованій зміні або пошкодженню в процесі передачі або зберігання. Цілісність забезпечується за допомогою хеш-функцій та цифрових підписів, які дозволяють перевіряти цілісність даних та виявляти будь-які зміни.
- Автентичність: криптографія забезпечує автентичність даних, тобто можливість перевірити справжність та джерело інформації. Цифрові підписи та протоколи автентифікації дозволяють переконатися, що дані були створені або підписані конкретним учасником системи.
- Неможливість відмови: криптографія забезпечує можливість доказу авторства повідомлення або проведеної операції. Це дозволяє запобігти можливості відмови від відповідальності з боку відправника чи одержувача.
- Стійкість до атак: криптографічні алгоритми розробляються з урахуванням захисту від різних атак, включаючи перебірний пошук ключа, аналіз шаблонів та інші методи криптоаналізу.

Криптографічні алгоритми поділяються на кілька основних категорій залежно від методів, які вони використовують для захисту даних. Зокрема, можна виділити два основні типи криптографії: симетричну і асиметричну. У симетричній криптографії для шифрування та дешифрування даних використовується один і той

самий ключ. Асиметрична криптографія, в свою чергу, використовує пару ключів: публічний ключ для шифрування та приватний для дешифрування. Класифікацію даних алгоритмів наведено на рис. 1.1

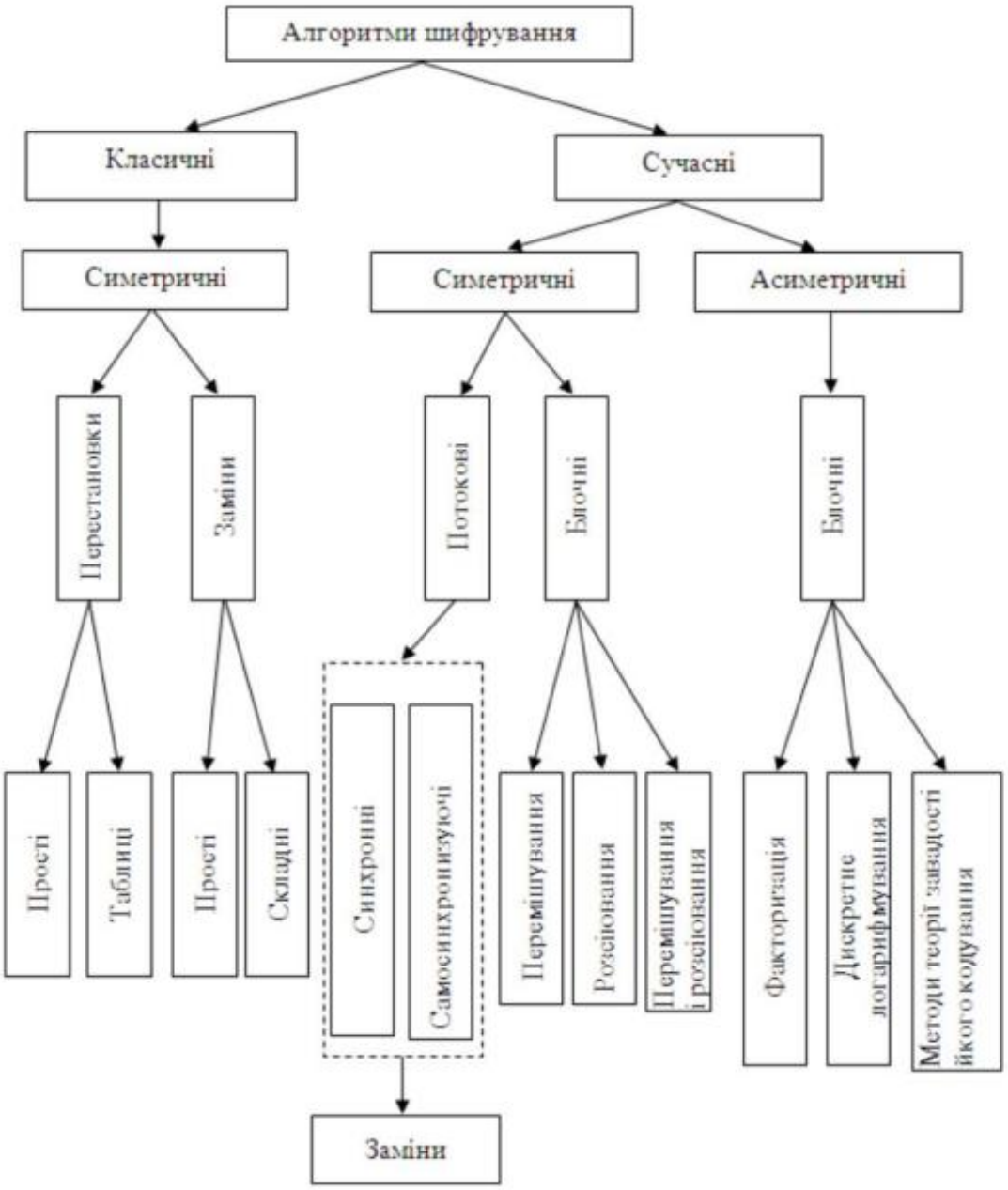


Рис. 1.1. Класифікація алгоритмів шифрування

Симетричні алгоритми є одними з найстаріших і найпоширеніших методів шифрування. У їхній основі лежить ідея, що для шифрування та дешифрування інформації використовується один і той самий секретний ключ. Цей ключ необхідно передавати безпечно між сторонами, що може створювати певні

труднощі в умовах відкритих мереж. Одним із основних недоліків симетричних алгоритмів є проблема безпечного обміну ключами між користувачами, адже у разі перехоплення ключа атакуючий може отримати доступ до всієї зашифрованої інформації. У симетричному шифруванні один і той самий ключ використовується для як шифрування, так і для дешифрування інформації. Симетричні алгоритми мають перевагу в тому, що не споживають багато обчислювальних потужностей і працюють з високою швидкістю. Процес симетричного шифрування здійснюється в двох режимах: блокове шифрування та поточне шифрування. У режимі блокового шифрування дані розбиваються на блоки, які обробляються на основі довжини блоку, і для кожного блоку використовується однаковий ключ для шифрування. У разі поточного шифрування дані розбиваються на одиничні біти, після чого виконується їх шифрування. Алгоритми симетричного шифрування є значно швидшими порівняно з асиметричними шифрувальними алгоритмами. До популярних симетричних алгоритмів відносяться DES (Data Encryption Standard), AES (Advanced Encryption Standard), RC4, а також алгоритм серії блокових шифрів, таких як Triple DES.

DES є симетричним алгоритмом шифрування, розробленим компанією IBM у 1977 році. Він використовує блок розміру 64 біти та довжину ключа 56 біт. DES завжди працює з рівними блоками та використовує як перестановки, так і заміни в алгоритмі. Він застосовує 16 раундів транспозиції та заміни для шифрування кожної групи з 8 (64 біти) символів відкритого тексту, і вихід з кожного раунду обробляється по черзі. Кількість раундів експоненційно пропорційна часу, необхідному для подолання ключа методом грубої сили. Однак, незважаючи на збільшення кількості раундів, безпека DES вже не є достатньо надійною для захисту від атак.

Triple DES є схожим на стандарт DES, але використовує три 64-бітні ключі, що забезпечує загальну довжину ключа 192 біти. Процес шифрування в Triple DES однаковий як у DES, але він повторюється тричі: спочатку шифрується першим ключем, потім дешифрується другим ключем і, нарешті, знову шифрується третім

ключем. Процес дешифрування відбувається за допомогою того ж алгоритму, але зворотно. Triple DES забезпечує вищий рівень безпеки порівняно з оригінальним DES

AES, або Rijndael, був обраний як стандарт шифрування даних у жовтні 2000 року. Він є симетричним блочним шифром, що працює з блоками розміром 128 біт і використовує ключі довжиною 128, 192 та 256 біт. Основні типи алгоритмів шифрування включають перестановки, заміни та комбінацію цих методів. Алгоритм AES використовує кругову функцію, що складається з чотирьох основних операцій: SubByte, ShiftRow, MixColumn та AddRoundKey. Кількість раундів залежить від довжини ключа: 10 раундів для 128-бітного ключа, 12 раундів для 192-бітного ключа та 14 раундів для 256-бітного ключа.

Асиметрична криптографія ґрунтується на використанні двох різних, але математично взаємопов'язаних ключів. Публічний ключ використовуються для шифрування даних, а приватний — для їх дешифрування. Це дозволяє забезпечити безпечний обмін даними без необхідності передавати ключі через незахищені канали зв'язку. Якщо першим публікується ключ шифрування, система забезпечує приватну комунікацію з користувачем, що має ключ для розшифрування. Якщо публікується ключ для дешифрування, система служить для перевірки підписів на документах, зашифрованих власником приватного ключа. Публічні ключі використовуються для безпечної передачі ключів шифрування та інших даних, навіть якщо сторони не мали можливості погодити спільний секретний ключ.

Одним із найбільш відомих асиметричних алгоритмів є RSA (Rivest-Shamir-Adleman), який широко застосовується для забезпечення безпеки в інтернеті, наприклад, у протоколі SSL/TLS для захисту веб-трафіку.

RSA є найбільш поширеним алгоритмом публічного ключа, який використовується як для шифрування, так і для цифрових підписів. Безпека RSA базується на складності факторизації великих чисел. Процес шифрування в RSA використовує відкритий ключ з експонентом "e", а дешифрування відбувається за

допомогою приватного ключа "d". RSA вважається надійним, якщо розмір ключа перевищує 1024 біти, хоча сучасні рекомендації говорять про використання ключів довжиною 2048 біт для забезпечення достатнього рівня безпеки.

Асиметричні алгоритми є більш складними за симетричні, однак вони забезпечують значно вищий рівень безпеки та зручність при обміні ключами. Вони також використовуються в системах цифрових підписів, де приватний ключ використовуються для підписування даних, а публічний — для перевірки підпису.[2]

Гібридні алгоритми були розроблені для комбінування переваг обох підходів, які використовують як симетричні, так і асиметричні методи шифрування. У таких системах асиметрична криптографія застосовується для безпечної передачі симетричного ключа, який в подальшому використовується для шифрування великих обсягів даних. Одним з найпоширеніших прикладів гібридної криптографії є протокол SSL/TLS, який використовується для забезпечення безпеки при передачі даних у мережі Інтернет. У цьому випадку RSA або інші асиметричні алгоритми застосовуються для безпечної передачі симетричного ключа (наприклад, за допомогою алгоритму AES), після чого для шифрування та дешифрування даних використовуються значно швидші симетричні методи.[3]

Протокол SSL/TLS є основою безпеки веб-сайтів, забезпечуючи конфіденційність, цілісність та автентичність даних, що передаються між браузером користувача та сервером. Перш за все, при з'єднанні через SSL/TLS ініціюється обмін публічними ключами між клієнтом і сервером, що дозволяє узгодити симетричний ключ для подальшої безпечної комунікації. Це дозволяє досягнути високої швидкості шифрування завдяки використанню ефективних симетричних алгоритмів, таких як AES, при одночасному забезпеченні надійної безпеки завдяки асиметричним алгоритмам. Завдяки поєднанню найкращих аспектів обох видів криптографії, гібридні системи забезпечують баланс між ефективністю та високим рівнем захисту даних, що робить їх невід'ємною частиною сучасної цифрової безпеки.

Хешування — це односторонній процес, при якому з вхідних даних будь-якої довжини генерується фіксоване значення, яке часто називають хешем або дайджестом. Однією з основних властивостей хеш-функцій є їх односторонність, що означає неможливість відновлення оригінальних даних з хешу, навіть якщо відома сама хеш-функція. Важливою особливістю є також детермінованість: однакові вхідні дані завжди генерують один і той самий хеш.

Основні області застосування хешування включають:

1. Перевірка цілісності даних. Хеш-функції використовуються для перевірки того, чи були дані змінені під час передачі або зберігання. Наприклад, під час завантаження файлів з Інтернету часто надається хеш цього файлу, і користувач може перевірити, чи не було змінено його вміст, порівнюючи отриманий хеш з оригінальним.

2. Цифрові підписи. У криптографії хешування застосовується для створення цифрових підписів. Це дозволяє підтвердити, що дані не були змінені після підписання і що вони дійсно походять від конкретного підписанта. У цьому процесі дані спочатку хешуються, а потім підписується тільки отриманий хеш.

3. Індексування даних. У базах даних хеш-функції використовуються для швидкого пошуку та індексації даних. Вони дозволяють ефективно зберігати великі обсяги даних у вигляді хешованих записів для прискорення операцій пошуку.

4. Паролі та безпека. У багатьох системах хешуються паролі користувачів перед зберіганням у базах даних. Це дозволяє захистити паролі від крадіжки, оскільки самі паролі не зберігаються в незашифрованому вигляді.

На практиці найпопулярнішими стали хеш-функції, що належать до так званого сімейства MD4. MD5, SHA та RIPEMD базуються на принципах MD4.

MD4 — це алгоритм створення дайджестів повідомлень, розроблений Рональдом Рівестом. MD4 був інноваційним рішенням, оскільки його було спеціально розроблено для високоефективної програмної реалізації. Він

використовує 32-бітні змінні, а всі операції виконуються через побітові булеві функції, такі як логічні AND, OR, XOR і заперечення. Усі наступні хеш-функції сімейства MD4 побудовані на цих принципах.

У 1991 році Рівест запропонував посилену версію MD4, названу MD5. Обидві функції обчислюють 128-бітний вихід, тобто мають стійкість до колізій близько 2^{64}. MD5 набув широкого поширення, наприклад, у протоколах безпеки Інтернету, для обчислення контрольних сум файлів або збереження хешів паролів. Однак ще на ранніх етапах з'явилися ознаки потенційних вразливостей. У 1993 році Національний інститут стандартів і технологій США (NIST) опублікував новий стандарт дайджесту повідомлень — Secure Hash Algorithm (SHA), який зараз називають SHA-0. У 1995 році SHA-0 був модифікований до SHA-1, в якому змінили графік функції стиснення для покращення криптографічної стійкості. Обидва алгоритми мають довжину виходу 160 біт. У 1996 році часткова атака на MD5, розроблена Гансом Доббертіним, призвела до рекомендацій замінити MD5 на SHA-1. З того часу SHA-1 набув широкого застосування у багатьох веб-продуктах і стандартах.

Максимальна стійкість до колізій SHA-0 та SHA-1 за відсутності аналітичних атак становить близько 2^{80}, що не є достатньо високим рівнем для використання разом із алгоритмами, такими як AES, що мають рівень безпеки 128–256 біт. У 2001 році NIST представив три нові варіанти SHA-1: SHA-256, SHA-384 та SHA-512 з довжинами дайджесту 256, 384 і 512 біт відповідно. У 2004 році було додано SHA-224, щоб забезпечити відповідність рівню безпеки Triple DES. Ці чотири функції зазвичай називають SHA-2.

SHA-256 — це одна з версій алгоритму SHA, яка генерує хеш із 256 біт. Хеш-функції використовуються в багатьох криптографічних додатках, таких як перевірка цілісності файлів і в блокчейн-технології.[4]

Для певних застосувань, таких як створення ключів або збереження паролів, MD5 залишається достатньо надійним, якщо потрібна лише стійкість до передзображення або другого передзображення, навіть попри існування колізій.

Завдяки своїй простоті і ефективності хешування стало невід'ємною частиною багатьох систем безпеки та зберігання даних, гарантує захист від несанкціонованих змін і підвищує рівень довіри до інформації, яка передається або зберігається.

1.2 Нормативно-правова база у сфері криптографії

Криптографія є одним з основних елементів інформаційної безпеки в сучасних інформаційних системах. Для забезпечення надійного захисту даних необхідне чітке регулювання використання криптографічних технологій. Різні нормативно-правові акти визначають основні принципи та вимоги до їх застосування як на міжнародному, так і на національному рівні. У цьому розділі розглянемо основні міжнародні та українські нормативи, стандарти, а також практичні рекомендації, що стосуються застосування криптографічних алгоритмів.

Одним з ключових аспектів нормативно-правової бази є стандартизація криптографії. У багатьох країнах та міжнародних організаціях існують стандарти, які визначають вимоги до криптографічних алгоритмів, засобів захисту інформації та процедур сертифікації криптографічних продуктів. Це стосується не тільки сфер, пов'язаних з національною безпекою, але й комерційних секторів, де використання криптографії для захисту даних є обов'язковим.

Міжнародна правова і нормативна база має визначальний вплив на розвиток криптографії, оскільки вона встановлює єдині правила і стандарти для захисту інформації у всіх країнах. Міжнародні організації, такі як Міжнародна організація зі стандартизації (ISO), Європейський Союз, Національний інститут стандартів і

технологій США (NIST) — це основні структури, що визначають міжнародні норми для криптографії.

ISO/IEC 27001 є стандартом для систем управління безпекою інформації (ISMS). Цей стандарт широко використовується в комерційному секторі, особливо в банківських установах та організаціях, що працюють із великими даними. Він визначає вимоги до впровадження захисних механізмів, включаючи криптографію, для забезпечення конфіденційності, цілісності та доступності інформації.

Цей стандарт приймає процесний підхід до розроблення, впровадження, функціонування, моніторингу, перегляду, підтримування та вдосконалення СУІБ організації. Для ефективної діяльності організації необхідно ідентифікувати та управляти багатьма видами діяльності. Будь-яку діяльність, що використовує ресурси та підлягає управлінню з метою забезпечення перетворення вхідних даних у вихідні, можна розглядати як процес. Часто вихідні дані одного процесу є безпосередньо вхідними даними для наступного. Застосування системи процесів у межах організації разом з ідентифікацією цих процесів та їх взаємодіями, а також управління ними можна розглядати як «процесний підхід».

Процесний підхід до управління інформаційною безпекою, запропонований цим стандартом, заохочує його користувачів робити наголос на важливості:

1) розуміння вимог інформаційної безпеки організації і необхідності розроблення політики та цілей інформаційної безпеки;

2) впровадження контролів та їх функціонуванні для управління ризиками інформаційної безпеки організації в контексті загальних бізнес-ризиків організації;

3) моніторингу та перегляді продуктивності та ефективності СУІБ;

4) постійному вдосконаленні, основаному на об’єктивному вимірюванні.

Цей стандарт приймає модель «Плануй-Виконуй-Перевіряй-Дій» («Plan-Do-Check-Act»), надалі ПВПД (PDCA), яку застосовують для структуризації всіх процесів СУІБ. Рис. 1.2 ілюструє, яким чином СУІБ, використовуючи як вхіднідані вимоги

інформаційної безпеки та очікування зацікавлених сторін, за допомогою необхідних дій і процесів виробляє вихідні дані інформаційної безпеки, що відповідають цим вимогам та очікуванням.

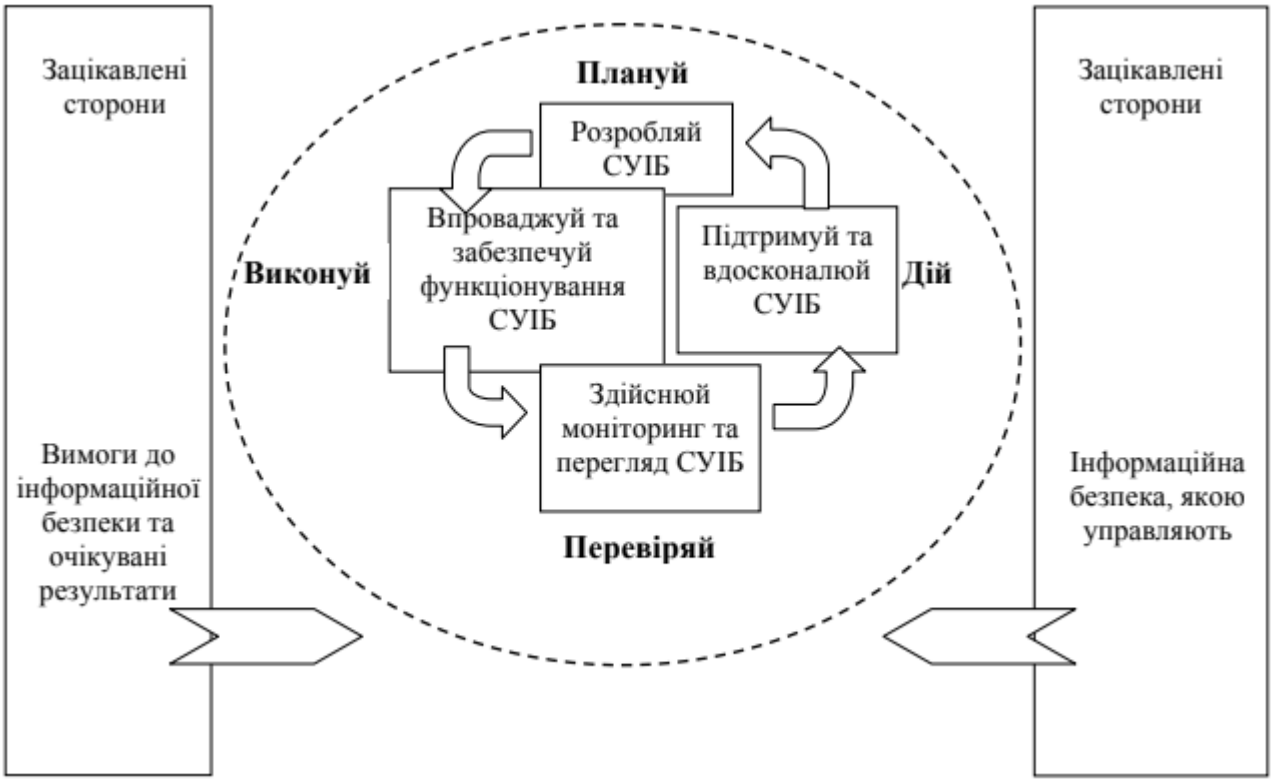


Рис. 1.2 - модель ПВПД (PDCA), застосована до процесів СУІБ

Прийняття моделі ПВПД (PDCA) буде також відображати принципи, які врегульовують безпеку інформаційних систем та мереж. Цей стандарт надає надійну модель для впровадження принципів цієї настанови, що впливають на оцінку ризиків, проектування і впровадження безпеки, управління безпекою та повторну її оцінку. [5]

ISO/IEC 27002 — це міжнародний стандарт, який надає рекомендації щодо управління безпекою інформації, охоплюючи найкращі практики щодо впровадження засобів захисту даних у організаціях. Він підтримує процеси оцінки та моніторингу інформаційної безпеки через системи управління ризиками. Стандарт визначає низку контролів, включаючи використання криптографії для захисту конфіденційності та цілісності інформації. У контексті криптографії ISO/IEC 27002 рекомендує застосовувати надійні алгоритми, сертифіковані

міжнародними органами, а також управляти криптографічними ключами відповідно до найкращих практик.

ISO/IEC 19790 фокусується на безпеці криптографічних модулів. Це одна з основних норм, яка визначає вимоги для продуктів, що реалізують криптографічні алгоритми. Цей стандарт визначає вимоги безпеки для криптографічних модулів, використовуваних у системах безпеки захисту конфіденційної інформації в комп'ютерних і телекомунікаційних системах, визначає чотири рівня безпеки для криптографічних модулів, які покривають широкий спектр чутливих даних (наприклад, малоцінні адміністративні дані, грошові перекази на мільйон доларів, тривалий захист даних, особиста ідентифікаційна інформація й конфіденційна інформація, використовувана урядом) та визначають рівні захисту в області різноманітних прикладних середовищ (наприклад, охоронний об'єкт, офіс, знімні носії чи повністю незахищені місця). Стандарт забезпечує визначення критеріїв, за якими сертифікуються криптографічні засоби, що використовуються в урядових і приватних секторах для захисту чутливих даних.

Цей стандарт встановлює вимоги безпеки, призначені для підтримання безпеки, представленої в криптографічному модулі. Дотримання цього стандарту не достатньо для того, щоб конкретний модуль був безпечним, або безпека, яку забезпечує модуль, достатня і прийнятна для власника інформації, яку він захищає.

NIST SP 800-53 пропонує технічні рекомендації для федеральних агентств США щодо безпеки інформаційних систем, включаючи криптографію. Цей стандарт має особливе значення для федеральних установ, оскільки він допомагає формувати політики щодо використання криптографії в сертифікованих системах. NIST 800-53 надає детальні рекомендації щодо безпеки інформаційних систем і включає критерії для використання криптографії як одного з основних засобів захисту. Він визначає вимоги до криптографічного захисту даних, зокрема для шифрування та автентифікації, а також дає рекомендації щодо управління криптографічними ключами, забезпечення цілісності даних та гарантування конфіденційності. У контексті стандарту основною метою є розробка заходів для

захисту інформаційних систем від несанкціонованого доступу, витоків даних і змін в інформації.

Стандарт зокрема включає такі важливі аспекти:

1. Криптографічні алгоритми: NIST рекомендує використовувати надійні криптографічні алгоритми, такі як AES для симетричного шифрування та RSA для асиметричного. Це важливо для забезпечення високого рівня безпеки при передачі та зберіганні інформації.
2. Управління ключами: однією з основних складових є чітке визначення політики управління ключами. Важливо забезпечити належне генерування, зберігання та знищення криптографічних ключів, а також контроль їх доступності.
3. Контроль доступу: стандарт визначає необхідність використання криптографії для авторизації та автентифікації користувачів і систем, що забезпечує належний рівень доступу до інформаційних ресурсів.

У зв'язку з цим, NIST 800-53 забезпечує цілісність системи управління безпекою шляхом впровадження криптографії у різні етапи обробки інформації, що дозволяє ефективно боротися з численними кіберзагрозам. [6]

Захист інформації та конфіденційності особистих даних є одними з пріоритетів Європейського Союзу. Основним законодавчим актом, що регулює використання криптографії на території ЄС, є *Загальний регламент захисту даних (GDPR),* який був прийнятий у 2016 році. Сучасні правові норми, такі як Загальний регламент захисту даних (GDPR) в ЄС, визначають чіткі вимоги до обробки персональних даних, включаючи використання криптографічних методів для їх захисту. Згідно з GDPR, підприємства повинні застосовувати шифрування для захисту персональних даних, що забезпечує конфіденційність, цілісність та доступність інформації.

Задача такої правової регуляції полягає в тому, щоб забезпечити баланс між використанням криптографії для захисту даних і контролем з боку державних органів. Оскільки криптографія є важливим інструментом захисту приватних даних, правові норми повинні враховувати можливості для безпечного та етичного використання цих технологій. Використання повного шифрування, за допомогою якого дані стають недоступними навіть для постачальників послуг, є прикладом такого етичного застосування криптографії.

Регламент накладає обов'язки на організації щодо захисту персональних даних, що вимагає використання криптографічних технологій для захисту передавання та зберігання таких даних. GDPR передбачає використання шифрування як одного з основних заходів для забезпечення безпеки особистої інформації.

NIS-директива (Директива щодо безпеки мереж і інформаційних систем), прийнята ЄС у 2016 році, також має велике значення для криптографії. Вона зобов'язує операторів критичних інфраструктур у країнах ЄС застосовувати надійні засоби захисту інформаційних систем, серед яких обов'язково застосування шифрування і криптографії для захисту даних.

У Сполучених Штатах Америки питання використання криптографії регулюється низкою законодавчих актів, найважливішим з яких є *Закон про контроль за експортом криптографії (Cryptography Export Control Act)* 1996 року. Цей закон має вирішальне значення для міжнародної торгівлі криптографічними технологіями, оскільки він встановлює обмеження на експорт сильних криптографічних технологій за межі США. Закон передбачає, що такі технології не можуть бути продані чи передані іншим державам без спеціального дозволу уряду.

Згідно з *Federal Information Security Modernization Act (FISMA)*, державні установи США зобов'язані використовувати надійні криптографічні алгоритми для захисту конфіденційної інформації. Крім того, NIST SP 800-53 містить вимоги до використання криптографії у системах, що зберігають або обробляють важливі дані федеральних агентств.

В Україні правова база щодо криптографії стала особливо актуальною після прийняття низки законів у сфері кібербезпеки та захисту інформації. Одним із основних нормативних актів є *Закон України «Про основні засади забезпечення кібербезпеки України»*, що визначає принципи використання криптографії для забезпечення національної безпеки. Закон зобов'язує державні органи використовувати сертифіковані криптографічні засоби для захисту інформаційних систем.

Цей закон також передбачає встановлення контролю за використанням криптографії в різних сферах, зокрема в комунікаціях, фінансах і обороні. Для цього визначено, що державні органи повинні застосовувати засоби криптографії, сертифіковані відповідними органами, такими як Державний центр сертифікації ключів, що функціонує під Міністерством цифрової трансформації України. Закон також містить вимоги щодо проведення атестацій та перевірок систем захисту інформації.

Для досягнення відповідності національним стандартам та міжнародним вимогам, цей закон встановлює обов'язковість сертифікації програмного забезпечення та технічних засобів, що використовуються для криптографічного захисту, а також затвердження стандартів і нормативів у сфері захисту інформації.

Таким чином, закон не тільки визначає принципи використання криптографії, але й регулює практичні аспекти її застосування, що є важливою складовою національної безпеки. [7]

Також важливим є *Закон України «Про електронну іденнтифікацію та електронні довірчі послуги»*, який регулює використання електронних підписів та шифрування в електронних транзакціях. Це дозволяє забезпечити автентичність і цілісність електронних документів, що особливо важливо для сфери електронного урядування та бізнесу. Додатково документ визначає правові норми щодо електронного підпису, де гарантує юридичну силу електронних підписів у транзакціях, у яких використовуються криптографічні методи для забезпечення їх

автентичності. Це створює безпечні канали для здійснення фінансових операцій, укладання договорів, а також обміну чутливою інформацією між державними та комерційними структурами. [8]

Закон України «Про електронні документи та електронний документообіг» визначає правовий статус електронних документів, їх юридичну силу та порядок використання в офіційному документообігу. Документ регулює створення, зберігання та передачу електронних документів із застосуванням електронного цифрового підпису, що забезпечує їх автентичність і юридичну значимість. Закон є основою для впровадження електронного документообігу у державному управлінні та бізнесі, стимулюючи розвиток електронних послуг і підвищуючи ефективність діловодства. [9]

Також, важливим аспектом правової регуляції криптографії є використання електронних підписів та криптографічних сертифікатів, які набули значення в міжнародних правових системах, зокрема в Європейському Союзі та США. Вони регулюються через відповідні нормативно-правові акти, такі як *Закон про електронні підписи та документи США і Регламент ЄС 910/2014 (eIDAS).*

Згідно з законодавством ЄС, електронні підписи повинні відповідати певним вимогам, зокрема бути кваліфікованими підписами для надання юридичної сили документам, що використовують криптографічні алгоритми для забезпечення їх цілісності і автентичності. Це сприяє розвитку електронної комерції та зменшенню ризиків шахрайства в Інтернеті.

Криптографія є основою для захисту державної та комерційної інформації, що має стратегічне значення. У багатьох країнах розроблені спеціальні сертифікати для державних криптографічних засобів, що відповідають певним вимогам безпеки, і які використовуються для захисту конфіденційних даних у різних державних відомствах та органах. В Україні для цього застосовуються ДСТУ-4175 та інші стандарти, що встановлюють вимоги до криптографічних засобів для захисту інформації, яка знаходиться під юрисдикцією держави.

Національний стандарт України ДСТУ-4175 регулює вимоги до криптографічних засобів для захисту інформації в органах державної влади, організаціях та інших системах, що обробляють конфіденційну інформацію. Він включає технічні вимоги до використання криптографії для забезпечення надійності захисту даних, визначає параметри, за якими проводиться сертифікація криптографічних засобів, та описує методи оцінки ефективності їх застосування. Стандарт також надає правила для впровадження криптографічних методів у національну систему безпеки, включаючи вимоги до алгоритмів і їх реалізацій.

У світі фінансів криптографічні методи використовуються для забезпечення безпеки фінансових транзакцій, захисту електронних платіжних систем, а також у блокчейн-технологіях. За останні роки в Україні та світі активно використовуються блокчейн-технології, що застосовують криптографічні методи для створення незмінних записів у розподілених базах даних. У цьому контексті багато підприємств переходять до використання криптовалют та токенів для фінансових операцій, що ще більше підкреслює важливість криптографії для безпеки в фінансових секторах. Оскільки банки і фінансові інститути активно переходять на цифрові платформи, захист від шахрайства, несанкціонованих доступів і кібератак є критично важливим. Інтернет-банкінг та платіжні системи активно використовують протоколи, засновані на криптографії, для аутентифікації користувачів і забезпечення цілісності транзакцій. [10]

Окрім того, з появою криптовалют, таких як Bitcoin і Ethereum, які засновані на блокчейн-технології, криптографія стала основою для створення довірчих відносин в умовах відсутності централізованих фінансових інститутів. Законодавчі ініціативи щодо регулювання криптовалют, такі як *Закон про криптовалюти в ЄС* та інші національні закони, сприяють розвитку цифрової економіки, але одночасно створюють нові виклики для регуляторів.

В Україні та інших країнах діють національні стандарти для криптографічних систем, наприклад, ДСТУ 4145, які встановлюють вимоги до використання криптографічних методів для захисту державної та комерційної інформації. Крім

того, сертифікація криптографічних засобів є важливою складовою частиною правового поля для забезпечення їх ефективності та надійності. Важливими організаціями, які займаються сертифікацією криптографії, є Національний центр кібербезпеки в США та аналогічні органи в інших країнах.

1.3 Перспективи розвитку нормативно-правової бази криптографії

Із зростанням цифрової трансформації та інтеграцією нових технологій у всі сфери суспільного та економічного життя постає потреба у адаптації національних і міжнародних правових норм до нових реалій. Криптографія, будучи основною технологією для захисту даних, є в центрі уваги глобальних дебатів щодо приватності, безпеки та доступу до інформації. Зокрема, одним із ключових викликів є визначення меж між забезпеченням національної безпеки та правами громадян на приватність.

Проте, регулювання криптографії не може залишатися виключно в межах однієї країни. Враховуючи глобалізацію інформаційних технологій, виникає необхідність у міжнародних угодах та стандартах, що регулюють використання криптографії на глобальному рівні. Це включає ініціативи щодо створення єдиних стандартів для захисту даних, забезпечення відкритості і доступу до шифрування, а також необхідність врегулювання питань, пов'язаних з кібербезпекою і боротьбою з кіберзлочинністю.

У майбутньому нормативно-правова база в сфері криптографії, ймовірно, стане більш гнучкою і здатною адаптуватися до технологічних змін. Впровадження нових криптографічних стандартів, які відповідають вимогам нових технологій, таких як блокчейн та квантова криптографія, стане важливим напрямком для правової адаптації. Необхідність постійного оновлення нормативно-правових актів у сфері криптографії пояснюється швидким розвитком нових технологій, таких як квантові обчислення. Потенційна здатність квантових комп'ютерів розкривати

сучасні криптографічні алгоритми ставить під загрозу ефективність існуючих захисних систем. З огляду на це, науковці та правники пропонують перегляд існуючих стандартів і розвиток нових підходів до криптографії, що будуть стійкими до атак з боку квантових комп'ютерів.

Міжнародні організації відіграють важливу роль у формуванні загальних стандартів для використання криптографії. Основними з них є ISO, IEEE, IETF, а також національні органи, що займаються сертифікацією криптографічних засобів. Зокрема, IETF (Internet Engineering Task Force) розробляє протоколи та стандарти, що активно використовуються у криптографії для захисту передавання даних через Інтернет. Стандарти, зокрема, такі як TLS (Transport Layer Security) і IPsec, визначають найкращі практики для забезпечення конфіденційності та цілісності даних в мережах.

Важливе значення має також участь країн у Глобальній ініціативі з кібербезпеки, де країни співпрацюють для вироблення загальних правил для боротьби з кіберзагрозами. Це включає стандарти для використання криптографії в урядових і приватних системах, що повинні відповідати єдиним вимогам, визначеним міжнародними угодами.

На рівні міжнародних стандартів йде робота над створенням нових алгоритмів, здатних витримувати квантові атаки. Одним із таких напрямів є дослідження постквантових криптографічних алгоритмів, таких як алгоритми на основі решіток, що можуть забезпечити високий рівень безпеки навіть у майбутньому.

Одним із важливих напрямів розвитку нормативно-правової бази є адаптація до нових технологій, таких як квантова криптографія та блокчейн. Враховуючи, що квантові обчислення здатні порушити існуючі алгоритми, правова база повинна адаптуватися до цих змін і забезпечити застосування нових протоколів та методів, що залишаються стійкими до квантових атак. Це включає в себе впровадження

нових постквантових алгоритмів, а також нормативні акти, які зможуть регулювати такі технології.

Також слід зазначити, що правове регулювання криптографії не повинно бути обмежене лише національними межами. З глобалізацією Інтернету та цифрових технологій виникає потреба в міжнародних правових ініціативах, які дозволяють виробити єдині правила для захисту цифрової інформації. Проте, важливо знайти баланс між національними інтересами та міжнародними стандартами, оскільки деякі країни можуть мати специфічні вимоги до криптографії, що не відповідають загальносвітовим стандартам.

Сучасна правова база вимагає постійного удосконалення через нові загрози, зокрема, в контексті боротьби з кіберзлочинністю та тероризмом. Використання криптографії в боротьбі з цими загрозами є важливим, оскільки вона забезпечує конфіденційність передавання даних та перешкоджає витоку важливої інформації

1.4 Аналіз загроз інформаційної безпеки в інформаційній системі організації

У зв'язку з швидким розвитком комп'ютерної техніки та відкритих мереж, з'явилися нові загрози і вразливості, пов'язані з втратою, розкриттям та модифікацією даних, що належать різним користувачам. Забезпечення захисту інформації в комп'ютерних системах вимагає досліджень та удосконалення криптографічних алгоритмів, які забезпечують безпеку користувачів від таких загроз. Оцінка ефективності криптографічних алгоритмів є складним завданням і вимагає глибоких знань, що робить його більше науковою, ніж інженерною задачею. Це призводить до наявності багатьох засобів криптографічного захисту, ефективність яких не є однозначною та гарантованою, оскільки базові алгоритми можуть бути недостатньо дослідженими.

Криптоаналіз - це наука про вивчення та розкриття криптографічних систем і методів їх захисту. Його основною метою є зламання криптографічних алгоритмів шляхом знаходження слабкостей та вразливостей, що дозволяють отримати доступ до зашифрованої інформації без знання секретного ключа.

Криптоаналіз може використовувати різні підходи, такі як аналітичний підхід, статистичний аналіз, алгебраїчні методи, атаки з використанням комп'ютерної потужності та багато інших. Метою криптоаналізу є знаходження слабких місць в криптографічних системах та розробка нових методів атак для зламування шифрів. Класифікацію сучасних методів криптоаналізу наведено на рис. 1.3.

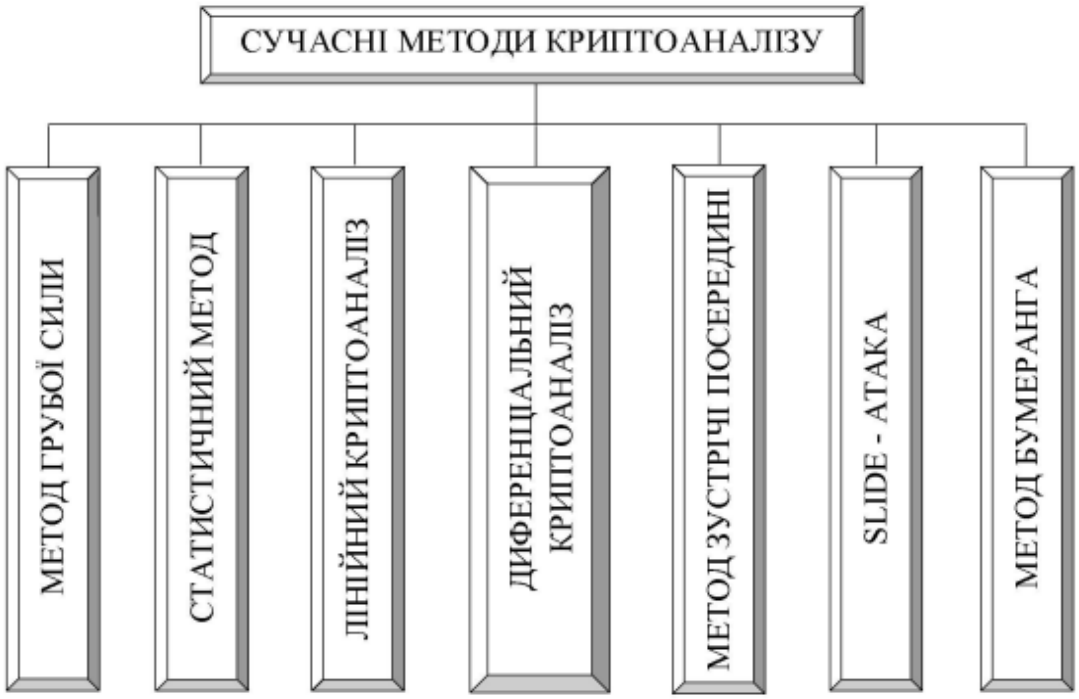


Рис. 1.3. Класифікація сучаних методів криптоаналізу

Призначення криптографії полягає у збереженні втаємниці відкритого тексту чи ключа (чи те й інше).Завданням криптоаналізу є відновлення відкритого тексту без доступу до ключа. Спроба криптоаналізу також називається атакою. А розкриття ключа без залучення спеціальних методів називають компрометацією ключа.Надійність чи криптостійкість симетричних та асиметричних алгоритмів залежить від ключів, а не від самих алгоритмів.

Атаки на криптографічні алгоритми мають на меті знайти відкритий текст на основі відомого шифротексту та невідомого ключа шифрування, або безпосередньо знайти ключ шифрування для можливості розшифрування зашифрованих повідомлень. Тому важливо проводити дослідження методів криптоаналізу для оцінки стійкості існуючих криптографічних алгоритмів.

Голландський криптограф Август Керкгоффс вперше сформулював постулати оцінки стійкості шифру (або криптостійкості) перед його зломом (розкриттям), відповідно до яких:

1) весь механізм перетворення вважається відомим зловмиснику ;

2) криптостійкість (надійність) алгоритмів перетворення визначається лише невідомим значенням ключа.

У сучасному криптоаналізі розглядаються атаки на засекречувальні системи на основі таких відомих даних:

1) шифртексту;

2) відкритого тексту та відповідного йому шифртексту;

3) обраного відкритого тексту;

4) обраного шифртексту;

5) на основі підібраного ключа.

У разі *атаки на основі шифртексту* криптоаналітик має у своєму розпорядженні шифртексти декількох повідомлень, зашифрованих одним алгоритмом. Його завдання полягає у розшифруванні повідомлень чи визначенні ключа (переважно).

При *атаках на основі відкритого тексту* криптоаналітик має в своєму розпорядженні шифртексти декількох повідомлень і відкриті текстами цих повідомлень. Його завдання – визначити ключ.

Атака на основі вибраного відкритого тексту передбачає не тільки можливість доступу криптоаналітика до шифртекстами кількох повідомлень та відкритих текстів цих повідомлень, але й можливість вибирати відкритий текст для зашифрування. Завдання – визначити ключ.

Атака на основі вибраного шифртексту дозволяє криптоаналітику вибирати різні шифртексти для розшифрування. Він також має доступ до розшифрованих текстів. Атака застосовується головним чином асиметричні алгоритми. Завдання – визначити ключ.

У разі *атаки на основі підібраного ключа* криптоаналітик дещо знає про зв'язки між ключами.

Складність тієї чи іншої атаки можна оцінити за наступними критеріям:

- за складністю даних – оцінюється обсяг даних, необхідні реалізації атаки;
- за складністю обробки – оцінюється час, необхіднийна реалізацію атаки (фактор трудовитрат);
- за вимогами до пам'яті комп'ютера – оцінюється мінімально необхідний обсяг пам'яті комп'ютера для виконання всіх розрахунково-аналітичних операцій.

Ларс Кнудсен класифікував складність злому алгоритмів за кількома критеріями:

- повний розтин - криптоаналітик знаходить ключ, такий що DK(C) = M
- глобальна дедукція – криптоаналітик знаходить альтернативний алгоритм, еквівалентний формулі без знання K;
- випадкова (або часткова) дедукція – криптоаналітик знаходить (чи краде) відкритий текст для перехопленого зашифрованого варіанта;
- інформаційна дедукція – криптоаналітик добуває деяку інформацію про ключ або про відкритий текст (кілька біт ключа або фрагменти відкритого тексту).

Криптографічний алгоритм вважається безумовно стійким, якщо відновлення відкритого тексту неможливе за будь-якого обсяг шифтексту.

Такий алгоритм реалізований у шифрі Вернама, або шифрі на основі одноразових блокнотів. Цей шифр запропонували у 1917 році Гілберт Вернам та Мейджор Моборн. Класичний одноразовий блокнот – це неповторний випадковий набір ключів. Кожен ключ використовується лише один раз і лише в одному повідомленні. Друга важлива особливість - довжина ключа повинна бути не менше довжини повідомлення, що шифрується.

Всі інші криптосистеми можна відкрити з використанням тільки шифртексту простим перебором можливих ключів та перевіркою свідомості отриманого відкритого тексту. Такий метод називається *лобовою атакою* (від англ. Brute-force). При використанні методу грубої сили відбувається перебір всіх можливих варіантів ключа шифрування, в результаті чого ключ шифрування буде обов’язково знайдено. Наприклад, якщо потрібно знайти ключ довжиною k біт, то такий пошук вимагатиме 2k-1 тестових операцій шифрування. Захистом від атак методом грубої сили є збільшення величини ключа, оскільки при збільшенні величини ключа на один біт кількість комбінацій ключа шифрування збільшується в два рази.

Час, необхідний для будь-якого розкриття системи, залежить від двох параметрів: числа ключів, що тестуються, і часу тестування окремої ключової комбінації. Зрозуміло, що навіть при сучасному розвитку обчислювальної техніки, метод грубої сили не є ефективним, проте його можна покращити при використанні спеціальних пристроїв перебору або розпаралелюванні процесу пошуку ключів.

При використанні *статистичного аналізу* потрібно визначити ключ шифрування або його частину, маючи деяку кількість пар "відкритий текст – шифротекст". Основою статистичного аналізу є процедура статистичної класифікації, яка для великої кількості статистичних даних, що вибираються випадковим чином, визначає закон розподілу цих даних і шуканий параметр – ключ шифрування.

Лінійний криптоаналіз поєднує пошук лінійних статистичних аналогів для рівнянь шифрування, статистичний аналіз відкритого та шифротексту, а також методи узгодження та перебору. Даний метод досліджує статистичні лінійні залежності між окремими бітами масивів відкритого, шифротексту та ключа і використовує ці залежності для визначення статистичними методами окремих біт ключа.

У методі лінійного криптоаналізу формуються залежності між відкритим текстом, шифротекстом та ключем. Ці залежності повинні мати високу ймовірність і разом з відомими парами "відкритий текст – шифротекст" використовуються для отримання бітів ключа. Для захисту від атак з використанням лінійного криптоаналізу необхідно досягти того, щоб при будьякій зміні відкритого тексту або ключа кожен з бітів шифротексту змінювався з різною ймовірністю.

У *диференціальному криптоаналізі* використовуються пари шифротексту, що мають деяку відмінність. У процесі аналізу досліджуються властивості даної відмінності при шифруванні відкритих текстів одним ключем. Зокрема, вибираються два відкритих тексти з фіксованою відмінністю і після процесу шифрування аналізується відмінність в отриманих шифротекстах. Потім різним ключам присвоюються різні ймовірності. В процесі подальшого аналізу наступних пар один з ключів стане більш ймовірним, тому він і є ключем шифрування.

Існує також посилений варіант диференціального криптоаналізу, який використовує не два, а чотири відкритих тексти та відповідних їм шифротексти, що пов’язані певною структурою, і називається методом бумеранга. Цей метод важко застосувати на практиці.

Метод зустрічі посередині використовує ідею парадоксу днів народження, яка полягає в тому, що для x√y ключів, вибраних з множини y, ймовірність їх збігу дорівнює (1 – exp(x 2 /2)). Пошук ключа шифрування зводиться до пошуку еквівалентної йому пари. Алгоритм працює так. На першому етапі для відкритого тексту фіксують ключ шифрування і одержаний шифротекст. На другому етапі

випадковим чином вибирають ключ розшифрування довільного шифротексту. У випадку збігу шифротекстів і відкритих текстів з першого і другого етапів ключі шифрування з цих етапів будуть шуканим ключем, інакше етапи пошуку повторюють. [11]

Розглянуті методи криптоаналізу дають змогу виявити недоліки і слабі місця різних криптографічних алгоритмів, врахувавши які можна підвищити стійкість сучасних криптосистем.

Однак, важливо враховувати, що успішний криптоаналіз не завжди гарантується. Застосування міцних криптографічних алгоритмів та виконання сучасних стандартів безпеки може значно ускладнити завдання криптоаналізу та зробити його практично неможливим. Тому постійне дослідження та вдосконалення криптографічних методів є важливим для забезпечення надійного захисту інформації.

Висновки до першого розділу

У першому розділі було розглянуто теоретичні основи використання криптографічних алгоритмів у інформаційних системах, що включають поняття криптографії, класифікацію основних типів алгоритмів, а також нормативно-правову базу, яка регулює їх застосування в Україні та в світі. Визначено ключові документи та стандарти, які регламентують використання криптографії для захисту інформації, виокрмелено значення криптографічних засобів для забезпечення безпеки в організаціях та державних установах.

2 АНАЛІЗ ПРАКТИЧНОГО ЗАСТОСУВАННЯ КРИПТОГРАФІЧНИХ АЛГОРИТМІВ З ВІДКРИТИМ ТА ЗАКРИТИМ КЛЮЧЕМ У ІНФОРМАЦІЙНИХ СИСТЕМАХ

Сучасні інформаційні системи є основою функціонування державних установ, комерційних організацій і приватних осіб, забезпечуючи зберігання та обробку великого обсягу даних. У зв’язку з цим питання захисту інформації є одним із найактуальніших у сфері кібербезпеки. Основним інструментом забезпечення конфіденційності, цілісності та доступності даних у цифровому просторі є криптографічні алгоритми, які використовуються для шифрування інформації, цифрового підпису та автентифікації.

В умовах постійного вдосконалення методів атак з боку зловмисників організації змушені адаптуватися, використовуючи найсучасніші криптографічні рішення. Цей процес включає як теоретичний аналіз сильних і слабких сторін алгоритмів, так і їхнє практичне впровадження у реальних інформаційних системах. Увага до практичного застосування криптографічних алгоритмів дозволяє забезпечити їх відповідність конкретним завданням і викликам.

Одним із найважливіших аспектів використання криптографії в практиці є баланс між ефективністю захисту і витратами на його впровадження. Підвищення рівня захисту не повинно призводити до значного зниження продуктивності системи або до надмірних витрат на її обслуговування. Тому на практиці обираються алгоритми, які відповідають вимогам безпеки, одночасно враховуючи їхню ефективність та ресурсозатратність.

У цьому розділі особлива увага буде приділена аналізу практичного застосування криптографічних алгоритмів в інформаційних системах, а також оцінці їх ефективності в реальних умовах. Розглянемо різні типи криптографічних методів, таких як симетричні та асиметричні алгоритми, їхні переваги та

обмеження, а також можливі варіанти реалізації в різних програмних і апаратних середовищах.

2.1 Особливості симетричних і асиметричних алгоритмів шифрування

Симетричні та асиметричні алгоритми є основними методами захисту даних у криптографії. Їхні відмінності, переваги та недоліки визначають області застосування кожного з підходів. Розуміння їхньої роботи, переваг і обмежень є ключовим для забезпечення інформаційної безпеки.

Симетричне шифрування

Симетричне шифрування — це широко використовуваний метод шифрування даних, за допомогою якого дані шифруються та розшифровуються за допомогою єдиного секретного криптографічного ключа. Зокрема, ключ використовується для шифрування відкритого тексту – стану даних перед шифруванням або після розшифрування – і розшифровки зашифрованого тексту – стану даних після шифрування чи попереднього розшифрування.

Симетричне шифрування є одним із найпоширеніших методів шифрування, а також одним із найстаріших, починаючи з часів Римської імперії. Шифр Цезаря, названий не на честь Юлія Цезаря, який використовував його для шифрування свого військового листування, є відомим історичним прикладом симетричного шифрування в дії.

Метою симетричного шифрування є захист конфіденційної інформації. Він щодня використовується в багатьох основних галузях промисловості, зокрема в оборонній, аерокосмічній, банківській, охороні здоров’я та інших галузях, у яких безпека конфіденційних даних людини, бізнесу чи організації є надзвичайно важливою.

Принцип роботи симетричного шифрування — симетричне шифрування використовує один і той же секретний ключ для шифрування та розшифрування даних. Ключ має бути відомий і відправнику, і одержувачу. Прикладами симетричних алгоритмів є AES, DES та 3DES. Вони забезпечують високу швидкість шифрування, але потребують безпечної передачі секретного ключа між сторонами. Схема використання методу симетричного шифрування зображено на рис. 2.1.

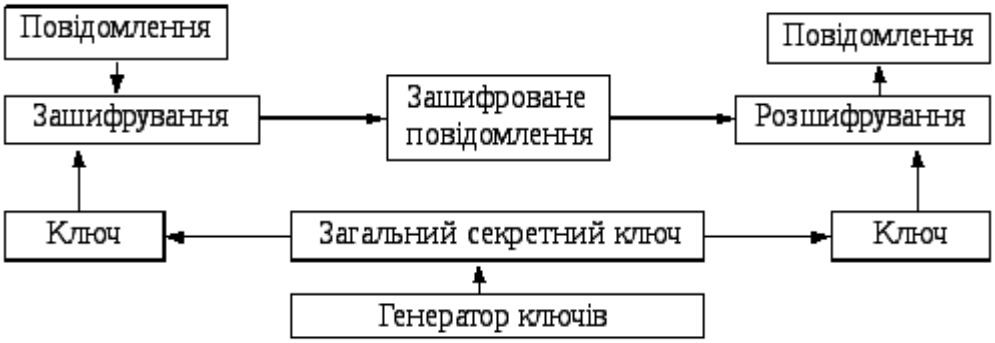


Рис. 2.1. Схема використання методу симетричного шифрування

Симетричне шифрування працює за допомогою потокового шифру або блочного шифру для шифрування та дешифрування даних. Поточний шифр перетворює відкритий текст у зашифрований текст по одному байту, а блоковий шифр перетворює цілі одиниці або блоки відкритого тексту, використовуючи попередньо визначену довжину ключа, наприклад 128, 192 або 256 біт.

Відправники та одержувачі, які використовують симетричне шифрування для передачі даних один одному, повинні знати секретний ключ, щоб, у випадку відправників, зашифрувати дані, якими вони мають намір поділитися з одержувачами, а у випадку одержувачів, розшифрувати та прочитати зашифровані дані відправниками поділитися з ними, а також зашифрувати будь-які необхідні відповіді. Однак симетричне шифрування не обмежується спільним використанням даних між одним відправником і одним одержувачем.

Шифрування AES, яке використовує блокові шифри 128, 192 або 256 бітів для шифрування та дешифрування даних, є одним із найвідоміших і

найефективніших методів симетричного шифрування, які використовуються сьогодні. На його злам знадобляться мільярди років, і тому його використовують для захисту конфіденційної інформації в уряді, охороні здоров'я, банківській справі та інших галузях. Він більш безпечний, ніж DES, Triple DES і IDEA.

Зараз Національний інститут стандартів і технологій (NIST) вважає шифрування DES застарілим алгоритмом симетричного шифрування, оскільки він довгий час був неефективним для захисту конфіденційної інформації від атак грубої сили. Насправді NIST повністю скасував стандарт, і його більш безпечний старший брат, шифрування Triple DES, чекає така ж доля. Незважаючи на те, що шифрування Triple DES все ще використовується, NIST у 2023 році скасовує та забороняє його через зростаючі проблеми безпеки.

Шифрування IDEA було розроблено як заміну DES у 1990-х роках, але зрештою AES було визнано більш безпечним. Зараз IDEA є відкритим і безкоштовним алгоритмом блокового шифрування, тож ним може користуватися будь-хто, але сьогодні він зазвичай вважається застарілим і неефективним для захисту конфіденційної інформації. Шифрування AES є золотим стандартом для обох цілей.

Захист транспортного рівня (TLS), як і його попередник, рівень захищених сокетів (SSL), використовує симетричне шифрування. По суті, коли клієнт отримує доступ до сервера, генеруються унікальні симетричні ключі, які називаються ключами сеансу. Ці ключі сеансу використовуються для шифрування та дешифрування даних, які спільно використовуються між клієнтом і сервером у конкретному сеансі клієнт-сервер у певний момент часу. Новий сеанс клієнт-сервер створить нові унікальні ключі сеансу.

TLS/SSL використовує не лише симетричне шифрування, а й симетричне й асиметричне шифрування, щоб забезпечити безпеку сеансів клієнт-сервер та інформації, якою обмінюються в них. [12]

Переваги симетричного шифрування.

Сьогодні використовується симетричне шифрування, оскільки воно може швидко шифрувати та дешифрувати великі обсяги даних і його легко реалізувати. Він простий у використанні, а його ітерація AES є однією з найбезпечніших доступних форм шифрування даних. Тепер симетричне шифрування має кілька переваг перед асиметричним аналогом, але ми поговоримо про асиметричне шифрування в цій публікації блогу трохи пізніше.

Деякі переваги симетричного шифрування включають:

- Безпека: симетричні алгоритми шифрування, такі як AES, потребують мільярди років, щоб зламати за допомогою атак грубої сили.
- Швидкість: симетричне шифрування, завдяки меншій довжині ключа та відносній простоті порівняно з асиметричним шифруванням, виконується набагато швидше.
- Затвердження галуззю: симетричні алгоритми шифрування, як-от AES, стали золотим стандартом шифрування даних завдяки їхнім перевагам у безпеці та швидкості, і як такі десятиліттями користуються впровадженням і визнанням у галузі.

Недоліки симетричного шифрування.

Безумовно, найбільшим недоліком симетричного шифрування є використання єдиного секретного криптографічного ключа для шифрування та дешифрування інформації.

Якщо секретний ключ зберігається в незахищеному місці на комп’ютері, то хакери можуть отримати до нього доступ за допомогою програмних атак, що дозволить їм розшифрувати зашифровані дані і тим самим порушити всю мету симетричного шифрування. Крім того, якщо одна сторона або організація шифрує в одному місці, а окрема сторона або організація розшифровує в другому, тоді ключ

потрібно буде передати, залишаючи його вразливим для перехоплення, якщо канал передачі зламано.

Ось чому вкрай важливо забезпечити безпеку ключа шифрування під час зберігання та передачі. Інакше ви просто попросите низку незалежних і спонсорованих державою кібератакувальників отримати доступ до ваших критично важливих даних, критично важливих для безпеки чи захищених законом даних.

Єдиним іншим недоліком використання симетричного шифрування є його ефективність безпеки порівняно з асиметричним шифруванням, яке зазвичай вважається більш безпечним, але також повільнішим у виконанні, ніж симетричне шифрування.

Симетрична криптосистема – це система, яка здійснює процес шифрування і дешифрування повідомлення, відкритого тексту, маючи в основі використання одного ключа. Отже, будь-хто, хто має доступ до ключа шифрування, може отримати доступ до зашифрованої інформації. Саме тому, використовуючи симетричні криптосистеми, ключ має залишатися у таємниці. Симетричні шифрування характеризуються найбільш високою швидкістю шифрування. За допомогою таких систем забезпечуються конфіденційність, цілісність і достовірність інформації. Конфіденційність передачі інформації у симетричній криптосистемі залежить від надійності шифру і забезпечення конфіденційності ключа шифру.

Достовірність забезпечується тому, що без дешифрування неможливо провести змістову модифікацію або зміну інформації. Та фальшиве повідомлення не може бути правильно зашифровано без знання секретного ключа.

Цілісність забезпечується за рахунок додавання до зашифрованого повідомлення спеціального коду, який твориться із секретного ключа. Перевірка виконується одержувачем повідомлення за рахунок порівняння спеціального коду із ключа та із повідомлення.

Симетричне шифрування є ідеальним для шифрування інформації одним користувачем, для запобігання несанкціонованому доступу до неї. Проблемою симетричних криптографічних систем шифрування є розподіл секретних ключів при великій кількості користувачів. На N користувачів потрібно $N(N-1)/2$ секретних ключів. [13]

Асиметричне шифрування

На відміну від симетричного шифрування, яке використовує той самий секретний ключ для шифрування та дешифрування конфіденційної інформації, асиметричне шифрування, також відоме як криптографія з відкритим ключем або шифрування з відкритим ключем, використовує математично пов'язані пари відкритого та закритого ключів для шифрування та дешифрування відправників і конфіденційні дані одержувачів.

Як і у випадку з симетричним шифруванням, відкритий текст усе ще перетворюється на зашифрований текст і навпаки під час шифрування та дешифрування відповідно. Основна відмінність полягає в тому, що дві унікальні пари ключів використовуються для асиметричного шифрування даних.

Асиметричне шифрування, ґрунтується на використанні пари ключів: відкритого ключа та закритого. Принцип асиметричного шифрування полягає в тому, що інформація, яка зашифрована з використанням відкритого ключа, може бути розшифрована тільки за допомогою відповідного закритого ключа. [14] Схема використання методу асиметричного шифрування проілюстровано на рис. 2.2.

Рис. 2.2. Схема використання методу асиметричного шифрування

Ось основні принципи асиметричного шифрування:

1. Пара ключів: в асиметричному шифруванні генерується пара ключів: відкритий ключ та закритий ключ. Відкритий ключ призначений для шифрування даних, а закритий ключ - для їхнього розшифрування.
2. Шифрування: у разі використання асиметричного шифрування відправник зашифровує дані з використанням відкритого ключа одержувача. Це означає, що криптографічний перетворення даних виконується за допомогою відкритого ключа.
3. Розшифровка: для розшифровування зашифрованих даних одержувач використовує свій закритий ключ, який є єдиним власником цього ключа. Закритий ключ дозволяє розшифрувати дані, отримані за допомогою відповідного відкритого ключа.
4. Безпека: однією з основних переваг асиметричного шифрування є безпека. Оскільки закритий ключ не відкривається іншим сторонам, тільки власник закритого ключа може успішно розшифрувати дані, зашифровані за допомогою відповідного відкритого ключа.
5. Цифрові підписи: асиметричне шифрування також дозволяє створювати та перевіряти цифрові підписи. Це спосіб гарантувати справжність відправника та цілісність даних. Підпис створюється з використанням закритого ключа відправника та може бути перевірений з використанням відповідного відкритого ключа.

Принцип асиметричного шифрування забезпечує ефективний спосіб обміну зашифрованими даними з використанням відкритих ключів, не вимагаючи попереднього обміну секретними ключами. Це робить його особливо корисним для забезпечення безпеки в мережевих комунікаціях та інших додатках, де потрібна конфіденційність та цілісність даних

Одна з причин, чому асиметричне шифрування часто вважається більш безпечним, ніж симетричне шифрування, полягає в тому, що асиметричне шифрування, на відміну від його аналога, не вимагає обміну одним і тим же ключем шифрування-дешифрування між двома або більше сторонами. Так, обмін відкритими ключами відбувається, але користувачі, які обмінюються даними в асиметричній криптосистемі, мають унікальні пари відкритих і приватних ключів, і їхні публічні ключі, оскільки вони використовуються лише для шифрування, не становлять ризику неавторизованого дешифрування хакерами, якщо вони стануть відомі, тому що хакери, припускаючи, що приватні ключі зберігаються приватними, не знають приватних ключів користувачів і тому не можуть розшифрувати зашифровані дані.

Асиметричне шифрування також дозволяє автентифікувати цифровий підпис, на відміну від симетричного шифрування. По суті, це передбачає використання приватних ключів для цифрового підпису повідомлень або файлів, а їхні відповідні відкриті ключі використовуються для підтвердження того, що ці повідомлення надійшли від правильного перевіреного відправника.

Концепція асиметричних криптографічних систем з відритим ключем заснована на застосуванні односпрямованої функції. Це така функція $F(x)$, де знаходження $Y = F(x)$ є простим завданням, а знаходження зворотної $F-1(y) = X$ є дуже складною задачею, яку не можна виконати за розумний час.

Переваги асиметричних криптосистем:

- кожен користувач вільно може створити свою пару ключів, а відкриті ключі можуть вільно передаватися;

- в асиметричних криптосистемах залежність числа ключів від числа користувачів лінійна – для N користувачів $2N$ ключів;

- дозволяють реалізувати протоколи взаємодії сторін, між якими немає довіри один до одного.

Недоліки асиметричних криптосистем:

- відсутність математичного доказу, що односпрямована функція незворотна;
- асиметричне шифрування істотно повільніше симетричного через те, що використовує досить ресурсоємні операції;
- необхідність захисту відритих ключів від підміни.

Недоліки асиметричного шифрування:

- Обчислювальна складність: асиметричне шифрування є більш складним, ніж симетричне шифрування. Він вимагає більшого обсягу обчислювальних ресурсів та часу для виконання операцій шифрування та розшифрування. Це може впливати на продуктивність системи при обробці великих обсягів даних.
- Обмежена швидкість: через обчислювальну складність асиметричного шифрування, швидкість передачі даних може бути обмежена. Це особливо помітно під час обміну великими обсягами даних або під час використання асиметричного шифрування у часі.
- Розмір ключів: довжина ключів, що використовуються в асиметричному шифруванні, зазвичай більша, ніж у симетричному шифруванні. Більш довгі ключі вимагають більшого обсягу пам'яті для зберігання та можуть впливати на продуктивність системи.
- Необхідність довірених сторін: асиметричне шифрування вимагає довіри до відкритих ключів, які використовуються для шифрування даних. Для цього необхідний механізм перевірки та підтвердження справжності відкритих ключів, що може вимагати використання довірених сторін або інфраструктури відкритих ключів (PKI).
- Незважаючи на деякі обмеження, асиметричне шифрування є важливим інструментом у криптографії, забезпечуючи безпеку та конфіденційність даних. Ефективне використання асиметричного шифрування вимагає балансу між

безпекою та продуктивністю, а також правильного управління ключами та довірчих відносин між учасниками комунікації. [15]

Загальне порівняння криптографічних алгоритмів з відкритим та закритим ключем показано у таблиці 1.1

Таблиця 1.1

Порівняння симетричних і асиметричних криптографічних алгоритмів

Параметр	**Симетричні алгоритми**	**Асиметричні алгоритми**
Швидкість	Висока, оскільки використовуються простіші математичні операції	Низька, через складні математичні обчислення
Безпека	Залежить від безпеки передачі ключа, уразливість при крадіжці ключа	Високий рівень безпеки, ключі не передаються, приватний ключ залишається захищеним
Використання ключів	Ключ потрібно передавати між учасниками	Відкритий ключ можна публічно передавати, приватний ключ зберігається в таємниці
Управління ключами	Складне: кожна пара учасників повинна мати унікальний ключ	Легке: лише відкритий ключ передається, приватний зберігається в таємниці
Широке застосування	Шифрування великих обсягів даних, наприклад, у зберіганні даних	Цифрові підписи, безпечний обмін даними, протоколи SSL/TLS
Переваги	Швидкість, ефективність для великих обсягів даних	Вища безпека, використання для автентифікації і підписів
Недоліки	Проблеми з безпекою при передачі ключа, управління великою кількістю ключів	Повільність, більші вимоги до обчислювальних ресурсів

2.2 Реалізація криптографічних алгоритмів у програмному забезпеченні

Реалізація криптографічних алгоритмів у програмному забезпеченні є ключовим етапом захисту інформаційних систем, особливо з огляду на вимоги до конфіденційності, цілісності та автентичності даних. Криптографія використовується в широкому спектрі застосувань, від шифрування переданих даних до забезпечення захисту від несанкціонованого доступу до конфіденційної інформації. Оскільки криптографічні алгоритми є основою безпеки сучасних інформаційних систем, важливо правильно інтегрувати їх у програмне забезпечення, щоб забезпечити надійний захист даних.

Етапи реалізації криптографічних алгоритмів

Реалізація криптографії у програмному забезпеченні включає кілька ключових етапів, кожен з яких має важливе значення для забезпечення високої якості та безпеки. Процес реалізації криптографічних алгоритмів можна описати такими етапами:

1) Вибір алгоритму

На цьому етапі розробники повинні вибрати відповідний криптографічний алгоритм в залежності від цілей і вимог системи. Наприклад, для захисту даних при зберіганні зазвичай використовують симетричні алгоритми, такі як AES, оскільки вони забезпечують високу швидкість і ефективність при обробці великих обсягів даних. Для шифрування і захисту ключів або для забезпечення захищеного обміну даними через мережу використовують асиметричні алгоритми, такі як RSA або ECDSA. Також необхідно враховувати такі фактори, як розмір ключа, швидкість шифрування та рівень безпеки.

Вибір криптографічного алгоритму базується на принципах стійкості до різних атак. Для сучасних систем важливо використовувати лише ті алгоритми, що пройшли перевірку часом та мають високу стійкість до сучасних методів криптоаналізу. Наприклад, вибір між AES і DES для шифрування даних буде

визначатися не тільки швидкісними вимогами, а й необхідністю забезпечення стійкості до атак на основі перебору.

2) Інтеграція бібліотеки

Після вибору алгоритму наступним кроком є інтеграція криптографічної бібліотеки у програму. Це включає підключення необхідних бібліотек до коду, налаштування середовища для їх використання та тестування на сумісність із програмним середовищем. Інтеграція повинна забезпечити не тільки коректність роботи криптографічних операцій, але й ефективність їх виконання. Для цього можуть бути використані специфічні бібліотеки або фреймворки, що підтримують необхідні алгоритми та стандарти, наприклад, OpenSSL, PyCryptodome або Bouncy Castle.

Важливою частиною цього етапу є оцінка продуктивності і швидкості роботи бібліотеки в умовах реального навантаження. Це дозволяє перевірити, чи не виникають збої чи затримки у процесах шифрування/розшифрування при великих обсягах даних або в умовах обмежених обчислювальних ресурсів.

3) Генерація ключів

Ключі є основою криптографічного захисту, тому процес їх генерації повинен бути максимально безпечним. На цьому етапі потрібно обрати метод генерації ключів, який відповідатиме вимогам безпеки, зокрема, щодо випадковості та складності. Наприклад, при використанні алгоритму AES для симетричного шифрування генеруються ключі довжиною 128, 192 або 256 біт, а для RSA — пару ключів (відкритий та закритий ключ), які забезпечують аутентифікацію і шифрування даних.

Генерація ключів повинна базуватися на криптографічно стійких псевдовипадкових генераторах чисел. Це забезпечує неможливість передбачити ключі, що в свою чергу захищає від атак на основі перебору.

4) Шифрування даних

На цьому етапі застосовуються самі криптографічні алгоритми для перетворення відкритих даних у зашифровану форму, що може бути прочитана лише тими, хто має відповідний ключ. Вибір режиму шифрування (наприклад, CBC, GCM або ECB) важливий для забезпечення рівня безпеки. Кожен режим має свої переваги та обмеження: деякі режими, наприклад GCM, забезпечують як конфіденційність, так і цілісність даних (автентифікацію), що є важливим у сучасних безпекових системах.

5) Розшифрування

Розшифрування є зворотнім процесом шифрування, де зашифровані дані перетворюються назад у їх початковий вигляд за допомогою відповідного ключа. Для цього важливо правильно організувати обмін ключами та забезпечити доступ лише до тих даних, до яких мають право отримати авторизовані користувачі або системи. Всі процеси розшифрування повинні бути захищені від несанкціонованого доступу, щоб уникнути компрометації конфіденційної інформації.

6) Управління ключами

Управління ключами — критичний етап, який включає в себе не тільки створення та зберігання ключів, але й їх регулярне оновлення, відмову від використання старих або скомпрометованих ключів, а також захист від несанкціонованого доступу. Важливо забезпечити належний контроль за термінами дії ключів, а також впровадити ефективну політику для їх відкликання і заміни. Для забезпечення високого рівня безпеки необхідно використовувати систему управління ключами (KMS), яка дозволяє централізовано здійснювати ці операції.

Реалізація криптографії в програмному забезпеченні супроводжується певними проблемами і викликами, які можуть серйозно вплинути на ефективність і безпеку системи.

Основні проблеми реалізації криптоалгоритмів з відритим та закритим ключем:

- Продуктивність. Виконання криптографічних операцій може бути ресурсоємким, особливо коли мова йде про обробку великих обсягів даних або складні операції, такі як цифрові підписи або асиметричне шифрування. Використання криптографічних алгоритмів, таких як RSA або ECDSA, може сповільнити роботу системи, оскільки вони вимагають значних обчислювальних потужностей для виконання операцій. Щоб зберегти баланс між безпекою та продуктивністю, часто використовують гібридні системи, де асиметричні алгоритми застосовуються для обміну ключами, а симетричні — для власне шифрування даних.

- Вразливості через неправильну інтеграцію. Однією з головних причин порушень безпеки є неправильне використання криптографічних бібліотек. Наприклад, використання слабких або незахищених режимів шифрування, неправильне управління ключами чи невідповідність між протоколами можуть призвести до серйозних уразливостей. Багато з таких помилок стають результатом недотримання рекомендацій або неповного розуміння принципів роботи криптографічних алгоритмів. Саме тому важливо детально вивчати специфікації і протоколи перед їх інтеграцією в систему.

- Застарілі алгоритми. Використання застарілих алгоритмів, таких як MD5 або SHA-1, може призвести до серйозних проблем безпеки. Ці алгоритми вже не відповідають сучасним вимогам, оскільки вони вразливі до атак за допомогою методів на основі колізій (наприклад, атаки на хеш-функції), що робить їх непридатними для захисту даних у сучасних умовах. Тому вкрай важливо своєчасно оновлювати криптографічні рішення і застосовувати алгоритми, які пройшли ретельне тестування та відповідають актуальним стандартам безпеки.

- Складність в управлінні ключами. Незважаючи на розвиток технологій, управління ключами залишається складною задачею. Відсутність належної політики управління ключами може призвести до компрометації конфіденційності

даних. Також часто виникають проблеми з зберіганням ключів в безпечному середовищі або їх передачі через незахищені канали. Важливо, щоб рішення для управління ключами відповідали сучасним стандартам безпеки, таким як FIPS 140-2 (Federal Information Processing Standard) або вимогам GDPR, якщо це стосується обробки персональних даних. [16]

Розробники програмного забезпечення часто використовують криптографічні бібліотеки для інтеграції алгоритмів у свої програми. Серед найбільш популярних і перевірених варіантів:

1) OpenSSL є однією з найпоширеніших криптографічних бібліотек з відкритим кодом, яка активно використовується в багатьох галузях інформаційної безпеки. Її перевагами є надійна підтримка широкого спектру криптографічних алгоритмів, зокрема симетричних (AES, DES), асиметричних (RSA, DSA, ECDSA) і алгоритмів хешування (SHA-256, SHA-512). Це дозволяє використовувати OpenSSL для забезпечення шифрування даних, автентифікації та цифрових підписів у різних додатках, від веб-сервісів до корпоративних рішень. Крім того, бібліотека характеризується високою продуктивністю та кросплатформністю, оскільки підтримує різні операційні системи, зокрема Windows, Linux, macOS, що робить її універсальним інструментом для розробки та реалізації безпечних комунікацій. Важливою перевагою OpenSSL є активна спільнота розробників, яка постійно працює над удосконаленням бібліотеки, забезпечуючи регулярні оновлення та виправлення вразливостей.

Однак OpenSSL не позбавлений і недоліків. Одна з головних проблем — складність коду, що може призводити до помилок у реалізації криптографічних алгоритмів, а отже, створювати вразливості, як це сталося з відомою вразливістю Heartbleed. Крім того, для ефективного використання бібліотеки потрібні глибокі знання криптографії та внутрішніх механізмів, що може бути складно для новачків. Тому важливо дотримуватись найкращих практик при розробці з використанням OpenSSL, щоб мінімізувати ризики.

2) Bouncy Castle — бібліотека, що орієнтована на підтримку криптографії в середовищах Java та C#, що робить її популярною серед розробників цих мов. Бібліотека спеціалізується на цифрових підписах і автентифікації, забезпечуючи високий рівень безпеки для додатків, де необхідна перевірка автентичності даних або користувачів. Завдяки сумісності з численними криптографічними стандартами, такими як PKCS#1, PKCS#12, X.509, Bouncy Castle полегшує інтеграцію з іншими системами. Водночас, хоча бібліотека має багато переваг для розробників на Java і C#, її продуктивність може бути обмеженою порівняно з бібліотеками, написаними на низькорівневих мовах, таких як C++, і може бути менш гнучкою щодо деяких розширених можливостей, які надає OpenSSL.

3) Crypto++ є ще однією потужною бібліотекою, яка орієнтована на високу продуктивність і ефективне оброблення великих обсягів даних, що робить її ідеальним вибором для систем, де критично важлива швидкість. Вона підтримує сучасні криптографічні алгоритми, такі як ChaCha20 та ECDSA, і має відкриту ліцензію, що дозволяє її використання в комерційних та некомерційних проектах. Проте, бібліотека написана мовою C++, що може підвищувати ймовірність помилок у управлінні пам'яттю, що, в свою чергу, може призводити до вразливостей безпеки. Крім того, на відміну від OpenSSL, Crypto++ не включає готові рішення для реалізації таких протоколів безпеки, як TLS/SSL, що вимагає додаткової інтеграції з іншими бібліотеками. Однак, завдяки високій продуктивності, Crypto++ активно використовується у наукових, фінансових та інших високонавантажених системах, де швидкість обробки даних є ключовою вимогою.

4) PyCryptodome є бібліотекою, яка інтегрується з Python, і є ідеальним вибором для розробників, які хочуть швидко додати криптографічні функції до своїх додатків на Python. Вона надає простий і зрозумілий інтерфейс і підтримує сучасні алгоритми, такі як AES, RSA, DSA, HMAC. Завдяки своїй простоті використання PyCryptodome часто вибирають у випадках, коли важливо швидко реалізувати захист даних або забезпечити автентифікацію користувачів. Однак бібліотека має

обмежену продуктивність у порівнянні з більш оптимізованими рішеннями, написаними на низькорівневих мовах, таких як C або C++. Це може стати проблемою для високонавантажених систем, де потрібна висока швидкість обробки даних. Тим не менш, PyCryptodome є відмінним вибором для невеликих і середніх додатків, таких як веб-додатки або системи управління користувачами, де використання шифрування або цифрових підписів є необхідним для захисту конфіденційної інформації та забезпечення автентичності даних. [17]

Усі ці бібліотеки мають свої сильні та слабкі сторони, що робить їх релевантними для різних типів проектів і систем. OpenSSL залишається стандартом де-факто для багатьох типів комунікаційних і веб-додатків, в той час як Bouncy Castle є ідеальним вибором для Java та C# розробників, які працюють із цифровими підписами та автентифікацією. Crypto++ чудово підходить для систем, де продуктивність є критично важливою, а PyCryptodome — для невеликих додатків, що потребують швидкого впровадження криптографічних функцій у Python.

2.3. Дослідження прикладів застосування криптографічних алгоритмів в інформаційних системах

У сучасному цифровому світі криптографія є критично важливим елементом для забезпечення конфіденційності, цілісності та аутентифікації інформації. У цьому розділі розглянемо реальні кейси застосування криптографії в різних сферах з конкретними прикладами та детальним аналізом принципів використання.

1. Захист з'єднань через HTTPS у веб-сервісах

Принципи використання: HTTPS є поєднанням протоколу HTTP та криптографії на базі SSL/TLS (Secure Sockets Layer/Transport Layer Security), що забезпечує шифрування та аутентифікацію під час передачі даних між клієнтом і сервером

через Інтернет. Основною метою є запобігання перехопленню або зміни даних в процесі комунікації.

SSL/TLS використовує дві основні техніки шифрування:

- Асиметричне шифрування (RSA, ECDSA) для встановлення безпечного з'єднання (обмін ключами).
- Симетричне шифрування (AES) для швидкої передачі даних після встановлення з'єднання.

У банківських системах, таких як Приват24, протокол HTTPS захищає всі транзакції, забезпечуючи шифрування персональних даних клієнта, таких як номер карти та паролі, за допомогою алгоритмів RSA для аутентифікації сервера та AES для шифрування даних транзакцій. Завдяки цьому кожен запит, наприклад, під час проведення оплати, є захищеним від атак Man-in-the-Middle (MitM).

2. Шифрування даних у хмарних сервісах

Використання шифрування в хмарних сервісах є необхідним для захисту конфіденційності даних, що зберігаються в хмарі. Для цього часто використовуються симетричні алгоритми (наприклад, AES) для шифрування великих обсягів даних і асиметричні алгоритми (наприклад, RSA) для управління ключами.

AES шифрує дані на стороні сервера перед їх зберіганням, при цьому користувачі мають доступ лише до зашифрованих файлів. Ключі для шифрування даних генеруються за допомогою RSA або ECC для безпечного обміну і аутентифікації.

У хмарних сервісах, таких як Google Drive або Dropbox, дані користувачів автоматично шифруються перед завантаженням на сервери. AES-256 використовується для шифрування файлів на сервері, а RSA — для обміну ключами між користувачем і сервером.

3. Електронний підпис для автентифікації та захисту документів

Електронний підпис використовує криптографію для автентифікації особи та підтвердження цілісності документів. Ключова роль у процесі електронного підпису належить асиметричним алгоритмам, таким як RSA чи ECDSA, для створення підпису та перевірки його автентичності. Для забезпечення цілісності даних використовуються хеш-функції (наприклад, SHA-256).

В Україні, застосунок “Дія” використовує електронний підпис для підписання юридичних документів та подачі податкових декларацій. Під час підписання документу на порталі “Дія” створюється хеш документа, який шифрується приватним ключем користувача, а для перевірки використовується публічний ключ, виданий акредитованим центром сертифікації - це забезпечує юридичну силу підписаних документів.

У наукових роботах, опублікованих у Journal of Information Security and Applications (2023), зазначено, що для підвищення безпеки електронного підпису необхідно використовувати мультифакторну аутентифікацію (МФА), де криптографія доповнюється іншими методами перевірки, такими як біометрія або одноразові паролі (OTP).

4. Захист доступу до інформаційних систем через автентифікацію та авторизацію

Аутентифікація та авторизація користувачів здійснюються через криптографічні методи, такі як HMAC (Hashed Message Authentication Code) та OAuth, для забезпечення безпечного доступу до інформаційних систем.

HMAC використовується для перевірки цілісності і автентичності повідомлень, а OAuth дозволяє безпечно передавати облікові дані через токени, що використовують криптографічне підписання.

У системах авторизації, таких як Google та Facebook, використовується протокол OAuth 2.0, який дозволяє стороннім додаткам отримувати доступ до особистих даних користувачів, використовуючи токени доступу. Токени

передаються через зашифровані канали, щоб запобігти перехопленню даних. HMAC-SHA256 часто застосовується для генерації токенів та їх перевірки.

Детальніше розберемо принципи роботи наведених прикладів використання криптографічних алгоритмів у різних технологіях.

2.3.1 Застосунок "Дія"

Застосунок "Дія" розроблений Міністерством цифрової трансформації України, є важливим інструментом цифровізації в Україні. Його основна мета — забезпечити громадянам швидкий доступ до державних послуг і документів, водночас гарантуючи максимальний рівень безпеки персональних даних. Досягнення цього завдання стало можливим завдяки інтеграції сучасних криптографічних алгоритмів, які виконують критично важливі функції: шифрування, аутентифікація, управління ключами, цифровий підпис і захист передавання даних.

Основною функцією застосунку є обробка та зберігання персональних даних громадян, включно з паспортними даними, водійськими посвідченнями та іншими офіційними документами. Для цього впроваджено низку заходів, які базуються на найсучасніших принципах інформаційної безпеки:

- Шифрування даних на стороні клієнта

Дані користувача шифруються до їхньої передачі на сервер. Це зменшує ризики перехоплення, навіть якщо пристрій користувача зламаний або компрометований. Використовується алгоритм AES-256, який відповідає стандарту FIPS (Federal Information Processing Standards) і рекомендований NIST. Алгоритм шифрує блоки даних розміром 128 біт із використанням 256-бітного ключа. Коли користувач додає документ у застосунку, дані про документ (наприклад, паспорт чи водійські права) конвертуються у бінарну форму. Перед відправленням на сервер ці дані

шифруються на рівні пристрою користувача. Наприклад, інформація про номер документа, дату видачі та інші деталі шифрується єдиним ключем, створеним під час сесії. Сервер отримує лише зашифровану версію даних, а дешифрування можливе тільки після надання відповідного ключа.

Для захисту ключів AES-256, які генеруються на стороні клієнта, застосовується додаткове шифрування через PBKDF2 (Password-Based Key Derivation Function 2). Ця функція гарантує, що ключ неможливо підібрати через атаку перебору.

Наприклад, при оцифруванні водійського посвідчення, дані спочатку шифруються за AES-256, а потім передаються на сервери державних реєстрів. Такий підхід мінімізує можливість отримання доступу до даних навіть у випадку перехоплення.

- Передавання даних через захищені канали

Для передачі даних між пристроєм користувача та сервером використовується протокол HTTPS із підтримкою TLS 1.3. Цей протокол забезпечує аутентифікацію серверів і шифрування переданих даних, запобігаючи атакам типу "людина посередині" (MITM).

Під час авторизації через "Дію" (наприклад, BankID) TLS створює зашифрований тунель між пристроєм користувача та сервером банку. Використовується RSA для обміну ключами. Сервер генерує пару ключів (відкритий і закритий), відкритий ключ надсилається користувачеві, який ним шифрує сесійний ключ AES. Лише сервер може дешифрувати його закритим ключем. Сесійний ключ AES використовується для подальшого шифрування всього трафіку.

TLS 1.3 усуває застарілі криптографічні алгоритми, як-от MD5 чи SHA-1, які вже не вважаються безпечними. Протокол також підтримує функцію "перфектної пренеглядної таємності" (Perfect Forward Secrecy), яка гарантує, що компрометація одного ключа не призведе до розкриття попередніх сеансів.

- Цифровий підпис

Для аутентифікації документів і підтвердження їхньої цілісності застосовується електронний цифровий підпис (ЕЦП). Алгоритми DSA (Digital Signature Algorithm) та ECDSA (Elliptic Curve Digital Signature Algorithm) дозволяють забезпечити захист документів від підробки та гарантують достовірність їхнього походження.

При створенні цифрового документа генерується хеш (SHA-256) його змісту. Цей хеш шифрується закритим ключем ЦСК (Центру сертифікації ключів). Коли користувач або державний орган перевіряє документ, відкритий ключ ЦСК розшифровує хеш. Якщо результат відповідає оригіналу, документ підтверджується. Навіть QR-коди в "Дії" містять криптографічний підпис. Їхня верифікація виконується через сервери, які порівнюють отриманий підпис із закритим ключем системи.

Кожен цифровий документ у "Дії" підписується за допомогою ключа, що зберігається в захищеному модулі смарт-карти або у хмарному сховищі, контрольованому державою. Під час перевірки підпису застосунок використовує публічний ключ, виданий сертифікаційним центром.

- Управління ключами

Для управління ключами "Дія" інтегрується із Державним центром сертифікації ключів (ЦСК), який відповідає за генерацію, розповсюдження та оновлення криптографічних ключів. При реєстрації нового користувача "Дія" запитує доступ до ключів через інтеграцію з BankID або іншими сертифікаційними установами. Таким чином, користувачеві надається можливість підписувати цифрові документи без потреби зберігати ключі на власному пристрої.

Методи криптографічного захисту застосунку “Дія”

- Авторизація користувачів

Застосунок використовує двофакторну аутентифікацію (2FA) з використанням криптографічних методів. Наприклад, після введення PIN-коду користувача

перевіряється його автентичність через криптографічний хеш, збережений на сервері.

За понад три роки існування "Дія.Підпис" нею скористувалося більше ніж 10,4 мільйона користувачів [18], статистику наведено на рис. 2.3.

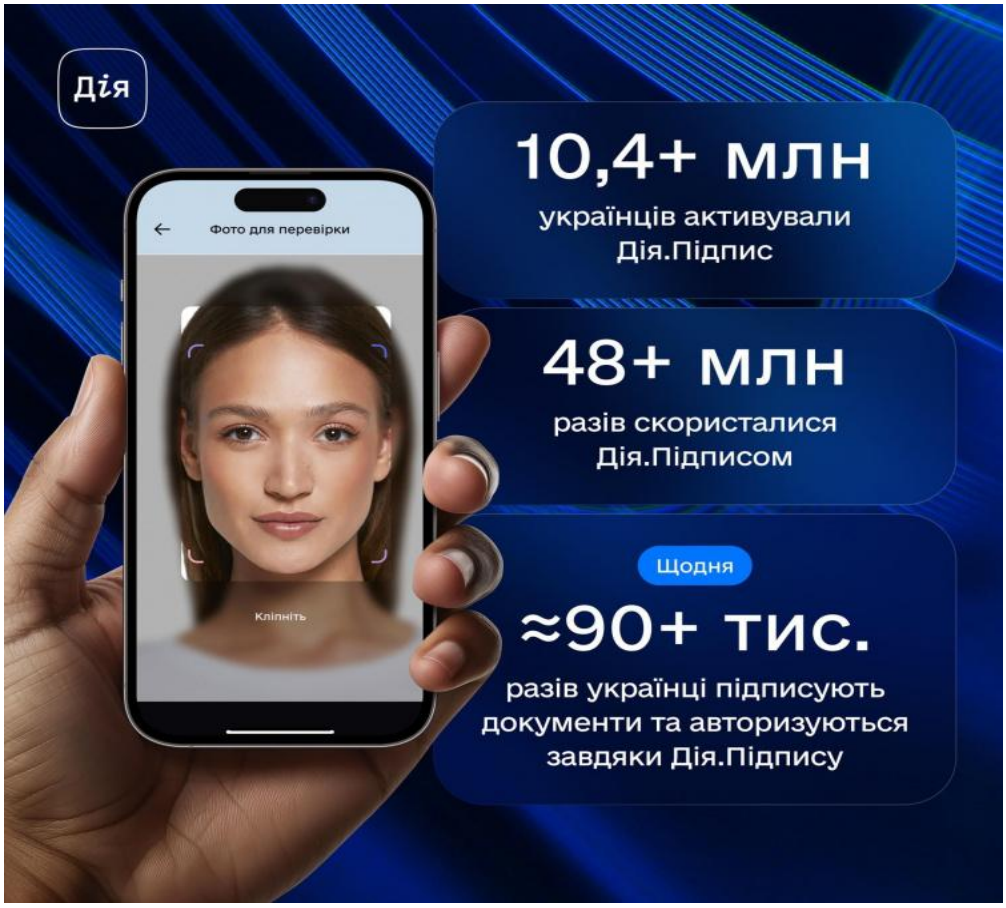


Рис. 2.3. Статистика використання Дія.Підпис

- Верифікація документів

Документи, доступні у "Дії", перевіряються за допомогою QR-коду, який містить криптографічно підписані метадані. Сканування цього коду дозволяє миттєво визначити достовірність документа через перевірку цифрового підпису.

- Захист проти атак

Застосунок реалізує механізми захисту проти атак повтору (replay attacks) через використання унікальних ідентифікаторів транзакцій, які генеруються під час кожної сесії.

- Шифрування резервних копій

У разі збереження резервної копії даних "Дія" застосовує алгоритми AES-256 із додатковим захистом ключів через алгоритм PBKDF2 (Password-Based Key Derivation Function 2), що робить ключі стійкими до атак на основі перебору.

Наукові праці, присвячені оцінці безпеки застосунку "Дія", відзначають високий рівень використаних технологій. Наприклад, дослідження, проведене у 2023 році Національним технічним університетом "КПІ", підтвердило ефективність застосування TLS 1.3 у "Дії", а також високу стійкість до атак типу MITM.

На думку Олександра Борнякова, заступника міністра цифрової трансформації, впровадження криптографічних стандартів міжнародного рівня стало одним із факторів успіху "Дії". Він також зазначив, що інтеграція з державними реєстрами через захищені канали забезпечує безперервність і безпеку роботи системи.

2.3.2 Система BankID

Система BankID є однією з основних технологій для безпечної ідентифікації та аутентифікації користувачів в Україні. Вона забезпечує взаємодію між громадянами, банками та державними органами за допомогою сучасних криптографічних методів.

Система BankID в Україні ґрунтується на *принципі довірчих посередників* — банках, які виступають посередниками між кінцевим користувачем і державними органами чи іншими сервісами. Основним завданням таких посередників є підтвердження особи користувача та надання їй доступу до державних послуг без необхідності створювати окремі акаунти для кожної з них.

Під час реєстрації в онлайн-банкінгу користувач надає свою особисту інформацію (ім’я, адресу, ідентифікаційний код, тощо), що перевіряється банком.

Після успішної ідентифікації користувач отримує можливість використовувати BankID для доступу до державних сервісів.

Звісно, дана система має переваги для державних установ, замість того, щоб кожен державний орган самостійно ідентифікував громадян, банківські установи вже виконують цю роль. Це спрощує процеси для всіх сторін і дозволяє зосередитись на безпеці та зручності взаємодії.

Для авторизації користувачів використовується стандарт OAuth 2.0, який є однією з найбільш поширених моделей аутентифікації для веб-додатків. OAuth дозволяє користувачам надавати доступ до своїх даних без необхідності передавати свої облікові дані (логін та пароль). Реалізація технології BankID в Україні спирається на кілька ключових принципів, які забезпечують її безпеку, ефективність та можливість інтеграції в різноманітні державні та фінансові сервіси. Ці принципи відображаються як на технологічному рівні, так і на рівні організаційних та юридичних механізмів, що підтримують систему.

Для підпису ідентифікаційних даних та електронних транзакцій використовуються цифрові сертифікати на основі стандарту X.509. Це дає змогу використовувати криптографічні ключі для підписання даних і забезпечує захист від їх підробки.

Формат PKCS#12 використовується для зберігання приватних ключів та сертифікатів, що використовуються в процесах шифрування та аутентифікації. Цей формат дозволяє безпечно зберігати та транспортувати цифрові сертифікати та ключі між різними системами, що є важливим для міжбанківських і міжсистемних інтеграцій.

Принцип "знання тільки необхідного" (Principle of Least Privilege) — цей принцип є основою для забезпечення конфіденційності даних користувачів. Згідно з цим принципом, кожен компонент системи має доступ лише до тієї інформації, яка необхідна для виконання конкретної задачі, і не більше.

Під час аутентифікації через BankID державні установи отримують лише мінімально необхідні дані для виконання запиту — це може бути, наприклад, підтвердження особи або інформація про статус конкретної заявки. Банки ж, в свою чергу, не передають державним установам доступ до фінансових або інших конфіденційних даних користувача.

Ідентифікація через BankID дозволяє зберегти конфіденційність фінансових даних, адже сам процес ідентифікації не передбачає передачу інформації про рахунки чи транзакції, а лише перевіряє, чи має особа доступ до банківських послуг.

Одним із важливих аспектів будь-якої національної системи аутентифікації є її надійність та стійкість до збоїв. У контексті BankID важливо забезпечити безперебійність доступу до послуг навіть у випадку технічних збоїв або атак.

У разі виникнення проблем з основним каналом зв'язку, система BankID забезпечує автоматичне перенаправлення трафіку через резервні канали, що дозволяє користувачам продовжувати користуватися сервісами.

Для виявлення потенційно небезпечних дій система передбачає активний моніторинг. Всі операції реєструються в аудитних журналах, що дозволяє відновити доступ до даних навіть у разі їх компрометації або скоєння злому.

Безпека приватних ключів також є одним з основних аспектів захисту даних. Для безпечної роботи з ключами та цифровими підписами застосовуються кілька рівнів захисту.

- Захист ключів

Приватні ключі, що використовуються для створення цифрових підписів в системі BankID, зберігаються в спеціальних захищених сховищах (наприклад, апаратних токенах або смарт-картах). Це дозволяє зменшити ризик їхнього викрадення або компрометації.

- Довірена інфраструктура сертифікації

Для генерації та перевірки цифрових сертифікатів, що використовуються в процесі аутентифікації, застосовується інфраструктура відкритих ключів (PKI). Це дає можливість керувати сертифікатами, надаючи користувачам високий рівень гарантій щодо автентичності їх підписів. Згідно з коментарями розробників і науковців, успішність BankID в Україні значною мірою залежить від технологічної реалізації і того, наскільки ефективно вона впроваджена в різні соціальні та державні сфери.

Система BankID в Україні продовжує розвиватися, і одним із важливих напрямків є інтеграція з новими електронними послугами, що пропонуються державою. Станом на перший квартал 2024 року, успішних електронних ідентифікацій, які були здійснені з використанням Системи BankID НБУ, становила 16,1 млн, що на 16% більше, ніж у IV кварталі 2023 року, це найбільша кількість успішних ідентифікацій за квартальний період з початку роботи системи.

Наразі система BankID НБУ налічує 142 учасники: 38 банків-ідентифікаторів та 104 абоненти – надавачі послуг. Детальну статистику [19] можемо побачити на рис. 2.4.

Рис. 2.4. Результати діяльності системи BankID

Технологія BankID є важливою складовою сучасної системи електронних послуг в Україні. Вона базується на надійних криптографічних методах, що забезпечують високий рівень безпеки та захисту даних користувачів. Для подальшого розвитку необхідно зосередити увагу на вдосконаленні інфраструктури, підвищенні доступності для всіх користувачів та постійному оновленні захисних механізмів.

2.3.3 Хмарний сервіс Google Drive

Процес залучення криптографічних алгоритмів у хмарному сервісі Google Drive здійснюється для забезпечення безпеки даних, які зберігаються та передаються через сервіс. Google використовує кілька рівнів захисту для запобігання несанкціонованому доступу до користувацьких файлів, у тому числі шифрування даних на стороні клієнта, при передачі та зберіганні файлів на серверах. [20]

1. Шифрування даних на стороні клієнта та при передачі.

Google використовує TLS (Transport Layer Security) для захисту даних, що передаються між клієнтом (користувачем) та сервером Google Drive. Коли користувач завантажує або отримує доступ до файлів, дані автоматично шифруються за допомогою протоколу TLS, що гарантує захищену передачу даних через мережу.

Коли користувач завантажує файл у Google Drive, спершу використовується механізм аутентифікації (як правило, через обліковий запис Google). Після цього дані передаються через захищене з’єднання, де вони шифруються за допомогою TLS 1.2 або 1.3. Цей протокол забезпечує, що дані будуть захищені від перехоплення або модифікацій під час їх передачі через Інтернет.

Процес шифрування при передачі даних між клієнтським пристроєм (користувачем) і серверами Google Drive включає використання протоколу TLS для забезпечення конфіденційності та цілісності даних. Цей криптографічний протокол, що забезпечує шифрування даних у реальному часі, що значно знижує ризик перехоплення та змін інформації під час її передачі. Оскільки TLS використовує механізм сертифікації за допомогою публічних ключів і цифрових сертифікатів, він також забезпечує захист від атак "man-in-the-middle", при яких зловмисник може намагатися підслухати або змінити передані дані. Метод шифрування даних та дешифрування даних зображено на рис. 2.5.

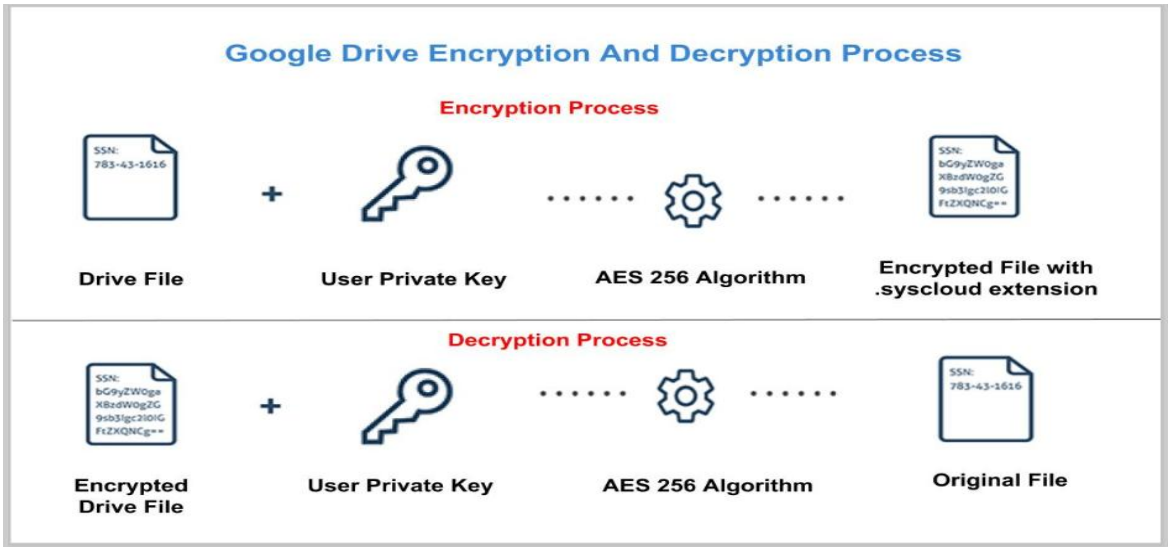


Рис. 2.5. Процес шифрування та дешифрування даних на Google Диску

2. Шифрування даних на сервері.

Після того, як дані завантажуються в Google Drive, вони потрапляють на сервери Google, де здійснюється їх шифрування для зберігання. Для шифрування даних на сервері Google використовує алгоритм AES (Advanced Encryption Standard) з ключем довжиною 256 біт. AES-256 вважається одним із найсильніших алгоритмів для симетричного шифрування і забезпечує високий рівень захисту даних. Це означає, що дані користувача шифруються на сервері і залишаються в захищеному вигляді до того часу, поки користувач не запросить доступ до них.

Шифрування файлів за допомогою AES-256 гарантує, що навіть якщо зловмисник отримає доступ до фізичних серверів, він не зможе дешифрувати дані без відповідного ключа. Важливо, що ключі для AES генеруються та зберігаються на серверах Google, що дозволяє контролювати доступ і зменшує ймовірність витоку ключів.

3. Управління ключами шифрування.

Google приділяє велику увагу безпеці управління ключами шифрування, щоб гарантувати надійність доступу до даних користувачів та уникнути несанкціонованого доступу.

Дана компанія використовує централізовану систему управління криптографічними ключами, де ключі для шифрування даних генеруються автоматично і зберігаються в ізольованому середовищі, що зменшує ризик їх витоку. Крім того, доступ до ключів суворо обмежений, і для їх використання потрібно пройти багатоетапну перевірку.

Кожен доступ до зашифрованих даних обмежується на основі ролей та дозволів, наданих користувачам і системам. Це забезпечує додатковий рівень захисту, оскільки навіть при можливому зламі одного облікового запису зловмисник не матиме доступу до всіх даних.

Google надає клієнтам можливість контролювати управління ключами через Google Cloud Key Management. Це рішення дозволяє організаціям створювати, зберігати, та обирати ключі для шифрування даних. Враховуючи важливість безпеки ключів, цей інструмент забезпечує гнучкість, а також відповідність вимогам безпеки різних секторів. Управління ключами здійснюється на кількох рівнях, що включає автоматичне створення та ротацію ключів, а також можливість інтеграції з системами зовнішнього управління ключами. [21]

Крім шифрування, Google Drive також застосовує технології резервного копіювання для забезпечення доступності даних користувачів у разі технічних збоїв або інших надзвичайних ситуацій. Доступ до резервних копій даних

здійснюється лише за допомогою відповідних ключів доступу, що забезпечує додатковий рівень безпеки.

Застосування криптографічних алгоритмів в Google Drive забезпечує високий рівень безпеки даних користувачів, дозволяють захистити інформацію від несанкціонованого доступу, навіть у разі зламу серверів або перехоплення переданих даних, а досконала системи управління ключами та багатофакторна аутентифікація додають додаткові рівні безпеки, що дозволяє Google Drive бути надійним рішенням для зберігання та обміну даними в хмарі.

Висновки до другого розділу

Було розглянуто теоретичні аспекти симетричних і асиметричних криптографічних алгоритмів, їх особливості та роль у захисті даних. Пояснено, як ці алгоритми використовуються для забезпечення конфіденційності та автентичності інформації в інформаційних системах. Виокремлено, як криптографічні бібліотеки та протоколи вбудовуються в інформаційні системи для надання захисту даних під час їх обробки та передачі даних.

Досліджено застосування криптографічних алгоритмів у різних інформаційних системах, наведено приклади використання шифрування для захисту даних користувачів у популярних платформах, таких як Google Drive та інших, а також розглянуто аспекти безпеки в системах електронної ідентифікації, зокрема BankID. Оцінено ефективність різних алгоритмів у реальних умовах та їх застосування для досягнення високих стандартів захисту

Дослідження показало, що криптографічні алгоритми є невід'ємною частиною сучасних інформаційних систем, забезпечуючи захист даних на різних етапах їх обробки та зберігання. Інтеграція криптографії в електронні сервіси та платформи дозволяє підвищити рівень довіри користувачів і забезпечити відповідність сучасним стандартам безпеки.

3 ТЕХНОЛОГІЇ ЗАСТОСУВАННЯ КРИПТОГРАФІЧНИХ АЛГОРИТМІВ В ІНФОРМАЦІЙНІЙ СИСТЕМІ ОРГАНІЗАЦІЇ

3.1 Методика вибору криптографічних алгоритмів для організацій

Вибір правильного алгоритму шифрування передбачає ретельну оцінку різних факторів, кожен із яких має власний вплив на безпеку, продуктивність і зручність використання. Розглянемо ці фактори докладніше:

1. Рівень безпеки.

Рівень безпеки алгоритму визначається його стійкістю до атак, які можна розділити на дві категорії:

- Атаки грубою силою

Ці атаки передбачають систематичне перепробування всіх можливих ключів, доки не буде знайдено правильний. Чим довша довжина ключа, тим більше комбінацій потрібно спробувати зловмиснику, щоб зробити шифрування надійнішим.

- Криптоаналітичні атаки

Ці атаки використовують слабкі місця в конструкції або реалізації алгоритму, щоб відновити відкритий текст або ключ, не випробовуючи всі можливі комбінації. Стійкість алгоритму до криптоаналітичних атак є критичним фактором його безпеки.

Вибираючи алгоритм шифрування, враховуйте конфіденційність ваших даних і потенційні загрози, з якими вони стикаються. Для дуже конфіденційних даних вибирайте алгоритми з більшою довжиною ключа та перевіреною стійкістю до криптоаналітичних атак. Наприклад, AES-256 (AES з 256-бітним ключем) широко вважається безпечним вибором для більшості програм.

2. Продуктивність

Шифрування та дешифрування – це інтенсивні обчислювальні процеси, які можуть вплинути на продуктивність вашої системи. Швидкість алгоритму залежить від різних факторів, включаючи його складність, довжину ключа та використовуване апаратне забезпечення.

Якщо ви маєте справу з великими обсягами даних або програмами в режимі реального часу, продуктивність стає критично важливою. У таких випадках симетричні алгоритми, такі як AES, як правило, швидше, ніж асиметричні алгоритми, такі як RSA. Однак прогрес у оптимізації апаратного та програмного забезпечення зробив асиметричні алгоритми більш практичними для багатьох випадків використання.

Оцінюючи продуктивність, враховуйте компроміс між безпекою та швидкістю. Сильніший алгоритм може бути повільнішим, але додаткова безпека може вартувати впливу на продуктивність, залежно від ваших конкретних потреб.

3. Управління ключами

Керування ключами — це процес створення, зберігання, розповсюдження та анулювання ключів шифрування. Це важливий аспект шифрування, оскільки безпека ваших даних зрештою залежить від секретності ключів.

Для симетричного шифрування потрібен безпечний механізм для обміну ключем між відправником і одержувачем. Це може бути складно, особливо у великих систем або під час спілкування із зовнішніми сторонами. Асиметричне шифрування спрощує розподіл ключів, оскільки відкритий ключ можна вільно ділитися. Однак для цього потрібна надійна інфраструктура для керування приватними ключами, які мають бути конфіденційними.

Вибираючи алгоритм шифрування, враховуйте складність керування ключами та доступні ресурси. Якщо розповсюдження ключів є основною проблемою, асиметричне шифрування може бути кращим вибором. Однак, якщо у вас є

безпечний механізм для обміну ключами, симетричне шифрування може запропонувати кращу продуктивність.

4. Стандартизація та впровадження алгоритму

Важливими факторами, які слід враховувати, є широке впровадження та стандартизація алгоритму шифрування. Стандартизовані алгоритми пройшли сувору перевірку експертів і, як правило, вважаються більш безпечними, ніж власні або незрозумілі алгоритми. Крім того, використання широко поширеного алгоритму забезпечує сумісність з різними системами та додатками.

AES, RSA та ECC є прикладами добре налагоджених і широко підтримуваних алгоритмів. Вибираючи алгоритм шифрування, віддавайте перевагу тим, які стандартизовані такими авторитетними організаціями, як NIST або ISO.

5. Орієнтованість на розвиток технологій

Сфера криптографії постійно розвивається, регулярно з’являються нові алгоритми та атаки. Вибираючи алгоритм шифрування, враховуйте його довговічність і потенціал надійності в майбутньому. Уникайте алгоритмів, про які відомо, що вони є вразливими або термін служби яких наближається до кінця. Вибирайте алгоритми, які активно обслуговуються та підтримуються криптографічною спільнотою. Це гарантує безпеку ваших даних навіть у разі появи нових загроз.

Проілюструємо процес вибору алгоритму на кількох прикладах:

Сценарій 1. Захист конфіденційних особистих даних: ви розробляєте програму, яка зберігає конфіденційну особисту інформацію, як-от записи про стан здоров’я чи фінансові дані. У цьому випадку безпека понад усе. Ви повинні вибрати сильний симетричний алгоритм, такий як AES-256, який пропонує високий рівень безпеки та розумну продуктивність.

Сценарій 2. Захист даних під час передавання: вам потрібно захистити дані, що передаються через мережу, наприклад онлайн-транзакції чи повідомлення

електронною поштою. Тут розподіл ключів є проблемою. Асиметричне шифрування, як-от RSA або ECC, є відповідним вибором, оскільки воно спрощує керування ключами.

Сценарій 3. Шифрування великих обсягів даних: ви маєте справу з масивними наборами даних, які потрібно зашифрувати для зберігання. У цьому випадку продуктивність має вирішальне значення. Кращим є швидкий симетричний алгоритм, такий як AES, оскільки він може ефективно обробляти великі обсяги даних.

Сценарій 4. Перевірка вашого шифрування на майбутнє: ви впроваджуєте шифрування в довгостроковий проект, де безпека даних має вирішальне значення на довгі роки. У цьому сценарії виберіть алгоритм, який активно обслуговується та підтримується, як-от AES або ECC, забезпечуючи безпеку ваших даних навіть у разі появи нових загроз. [22]

Вибір правильного алгоритму шифрування є критично важливим рішенням, яке може значно вплинути на безпеку ваших даних. Ретельно оцінюючи такі фактори, як рівень безпеки, продуктивність, керування ключами, стандартизація та перспективність, організація може вибрати алгоритм, який відповідає її конкретним потребам і захищає цінну інформацію від несанкціонованого доступу.

3.2 Створення політики управління ключами

1. Визначення політики управління ключами

Процес розробки політики управління криптографічними ключами включає встановлення основних принципів і правил для генерації, використання, зберігання та знищення ключів. Важливою частиною є також визначення типу криптографії, яка буде використовуватись — симетричні (AES) або асиметричні (RSA, ECC) алгоритми.

Політика має визначити, які криптографічні алгоритми будуть використовуватись для забезпечення конфіденційності та цілісності даних. Вибір залежить від специфікацій системи та вимог до безпеки. Наприклад, AES використовується для шифрування великих обсягів даних завдяки своїй швидкості та ефективності, а RSA застосовується для захисту ключів через свою здатність працювати з відкритими та приватними ключами.

2. Генерація та зберігання ключів

Генерація криптографічних ключів повинна бути здійснена за допомогою високоякісних генераторів випадкових чисел (HWRNG), щоб забезпечити достатню стійкість ключів до атак.

Створення криптографічних ключів має базуватись на математичних принципах та алгоритмах, що гарантують їх випадковість. Це може бути досягнуто через використання криптографічно стійких генераторів випадкових чисел. Наприклад, генератори випадкових чисел, що включають апаратні елементи (HWRNG), часто використовуються для створення ключів у фінансових системах.

Ключі для криптографії, що використовуються в банківських системах для захисту платіжних транзакцій, повинні мати високу ступінь випадковості, щоб уникнути прогнозованості під час атаки типу "brute-force".

Для безпечного зберігання ключів використовуються спеціалізовані пристрої, такі як апаратні модулі безпеки (HSM), які забезпечують захист від несанкціонованого доступу. Зберігання на таких пристроях дозволяє фізично ізолювати ключі від програмного середовища, що мінімізує ризики компрометації.

Наприклад, у хмарних сервісах, таких як Amazon Web Services (AWS) та Microsoft Azure, використовуються апаратні модулі безпеки (HSM), які гарантують, що ключі, що використовуються для шифрування даних, ніколи не залишають безпечний контейнер.

3. Ротація та заміна ключів

Процедури ротації ключів повинні бути автоматизованими для зменшення людського фактору. Заміна ключів має здійснюватися регулярно, зокрема після завершення певного циклу використання, для забезпечення довгострокової безпеки. Встановлення чітких правил для ротації ключів є важливим елементом управління безпекою. Це дозволяє знижувати ризик, що ключ може бути скомпрометований. Заміна ключів може бути реалізована через встановлені часові інтервали або після виконання певної кількості операцій.

У системах електронних платежів, таких як PayPal, кожен криптографічний ключ має обмежений термін служби, після чого автоматично генерується новий ключ для забезпечення додаткової безпеки.

Для зниження ризиків використовуються спеціалізовані інструменти для автоматичного оновлення криптографічних матеріалів (наприклад, використання технік, що дозволяють автоматично поновлювати сертифікати в інфраструктурах відкритих ключів).

4. Управління доступом до ключів

Правильне управління доступом до криптографічних ключів є основою для забезпечення безпеки систем. Для цього застосовуються чітко визначені моделі доступу, такі як принцип найменших привілеїв (Least Privilege), а також багатоетапні методи аутентифікації.

Система повинна включати багатоетапну аутентифікацію для доступу до критичних даних, зокрема для ключів, які використовуються для розшифрування або підписування інформації.

У корпоративних середовищах використовується багатофакторна аутентифікація для захисту доступу до криптографічних ключів. Наприклад, для доступу до сертифікатів для електронного підпису можуть використовуватись не тільки паролі, а й фізичні пристрої, такі як смарт-карти або токени.

5. Знищення ключів

Правильне знищення криптографічних ключів є важливим елементом безпеки, щоб попередити їх відновлення або несанкціоноване використання після завершення їх служби. Знищення ключів повинно бути нереверсованим, щоб виключити можливість їх відновлення. Для цього використовуються алгоритми стирання, які перезаписують ключі кілька разів, або ж фізичне знищення носіїв, на яких зберігаються ці ключі.

Після завершення терміну дії або використання ключів у хмарних сервісах (AWS, Azure), ключі підлягають повному знищенню через сертифіковані методи, що включають їх фізичне видалення із серверів або стирання з внутрішніх пам'ятей.

6. Відповідність стандартам та аудит

Забезпечення відповідності нормативним стандартам і проведення аудитів є невід'ємною частиною політики управління ключами. Політика повинна передбачати регулярні перевірки використання криптографічних ключів, щоб виявити порушення та уникнути їх несанкціонованого використання. [23]

У фінансових організаціях, таких як банки, часто проводяться аудити для перевірки правильності використання криптографічних ключів і їх відповідності стандартам ISO/IEC 27001.

3.3 Захист від втрати та компрометації ключів

Компрометація криптографічного ключа може призвести до серйозних наслідків, таких як несанкціонований доступ до даних, фінансові втрати та репутаційні ризики. Зловмисники постійно шукають нові способи зламу систем і отримання доступу до ключів. Необхідно вживати комплекс заходів та рекомендацій для захисту ключів від різноманітних загроз, які наведено у даному пункті.

1) Використання HSM (Hardware Security Modules)

Модулі апаратної безпеки (HSM) — це спеціалізовані апаратні пристрої, які забезпечують високий рівень безпеки для управління криптографічними ключами. Вони призначені для того, щоб бути стійкими до втручань і захищати приватні ключі в ізольованому середовищі, значно знижуючи ризик несанкціонованого доступу або пошкодження даних. Ці пристрої використовуються організаціями для захисту чутливої інформації, виконуючи криптографічні операції, такі як шифрування, підписання та аутентифікацію, без надання доступу до самих ключів.

Одна з ключових переваг HSM полягає в тому, що вони дозволяють уповноваженим користувачам виконувати криптографічні операції за допомогою збережених ключів, але без безпосереднього доступу до самих ключів. Це забезпечує захист ключів навіть у разі, якщо зловмисник отримає доступ до системи. Крім того, HSM дозволяють виконувати криптографічні операції без завантаження приватних ключів у пам'ять веб-сервера, що робить систему більш безпечною від кібератак, оскільки веб-сервери часто є більш вразливими до експлойтів.

Типи HSM:

- Апаратні модулі, вбудовані в сервер, забезпечують високу продуктивність та інтеграцію з іншими компонентами системи.
- Самостійні апаратні модулі, які можуть підключатися до мережі та використовуватися декількома серверами.
- Програмні HSM (pHSM), емулюють функціональність апаратних HSM в програмному забезпеченні.

Ось кілька основних функцій, які надають HSM:

- Генерація криптографічних ключів.

HSM використовуються для створення ключів, що генеруються всередині безпечного апарату, таким чином запобігаючи витоку або компрометації ключа під час його генерації.

- Шифрування та дешифрування.

Всі операції з шифруванням і дешифруванням виконуються всередині HSM, що дозволяє уникнути ризику витоку даних через відкриті канали.

- Підписання та перевірка підписів.

HSM можуть використовуватися для цифрового підпису документів і перевірки підписів, що дає гарантії автентичності і цілісності даних.

- Безпечне зберігання ключів.

Хоча ключі і використовуються для операцій, вони не залишають межі HSM, що значно знижує можливість їх компрометації в результаті злому або фізичного доступу до системи.

- Інтеграція HSM в інформаційну систему.

HSM можуть бути інтегровані у внутрішні системи для забезпечення більш гнучкого та автоматизованого управління криптографічними ключами. Інтеграція може відбуватися через:

- Інтеграція з хмарними платформами.

Багато великих хмарних провайдерів, таких як AWS, Microsoft Azure або Google Cloud, підтримують використання HSM через свої послуги для криптографії, надаючи розширену гнучкість в управлінні ключами.

- Інтеграція з KMS.

Інтеграція з системами управління ключами (KMS) дозволяє спростити використання ключів, оскільки KMS автоматично керує різними криптографічними операціями, включаючи їх обертання, створення та зберігання.

2) Двофакторна аутентифікація (2FA)

Двофакторна аутентифікація (2FA) є важливою складовою для забезпечення безпеки при використанні криптографічних ключів. Вона включає дві окремі форми аутентифікації для підтвердження ідентичності користувача.

- Щось, що ти знаєш (Knowledge Factor).

Це традиційні методи аутентифікації, такі як паролі, PIN-коди або секретні відповіді. Вони можуть бути уразливими до зламів, особливо якщо користувачі вибирають прості паролі або їх часто використовують у різних системах.

- Щось, що ти маєш (Possession Factor).

Цей фактор базується на чомусь фізичному, що користувач має, наприклад, смарт-карта, OTP-токен або мобільний телефон з генерацією одноразових паролів (OTP). Смарт-карти часто використовуються для підвищення рівня захисту в організаціях.

- Щось, що ти є (Biometric Factor):

Використання біометричних даних, таких як відбитки пальців, сітківка ока або розпізнавання обличчя, дає можливість додатково перевірити особу користувача за унікальними фізичними характеристиками.

- Комбінації факторів.

2FA забезпечує додатковий рівень безпеки, комбінуючи ці фактори. Одним із прикладів є комбінація пароля (що знаєш) і одноразового пароля з мобільного пристрою (що маєш). Це значно знижує ймовірність успішного злому навіть у разі компрометації одного з факторів аутентифікації.

3) Моніторинг активності

Моніторинг усіх операцій з криптографічними ключами є критично важливим для забезпечення їх безпеки. Кожна спроба доступу, обертання, підписання або дешифрування повинна бути записана в логах для подальшого аналізу. Записи повинні містити:

- Ідентифікацію користувача або процесу - хто саме здійснив операцію.
- Тип операції: шифрування, дешифрування, підписування, доступ до ключа тощо.
- Час та місце виконання операції та IP-адреса користувача.
- Результат операції: Чи була операція успішною, чи була зафіксована помилка.

Використання сучасних технологій для виявлення аномалій у поведінці користувачів, таких як машинне навчання для виявлення шаблонів поведінки, що є ненормальними. Наприклад, спроби доступу до ключів з незвичних місць або вночі, або якщо користувач здійснює надто багато операцій з ключами за короткий період часу. [24]

Системи виявлення вторгнень можуть допомогти виявити підозрілу активність, зокрема спроби несанкціонованого доступу до систем з криптографічними ключами. Вони моніторять мережеву активність і можуть інтегруватися з іншими інструментами для захисту ключів.

Висновки до третього розділу

Було розглянуто важливі аспекти впровадження криптографічних алгоритмів в організаціях, зокрема методику вибору алгоритмів, створення політики управління ключами та захисту від їх втрати чи компрометації.

Викоремлоно інформацію про політику управління ключами - важливий елемент, який охоплює всі етапи роботи з ключами: їх генерацію, зберігання, оновлення та знищення. Дослідження показало, що впровадження ефективних методів управління криптографічними ключами та заходів захисту дозволяє суттєво підвищити рівень безпеки в організаціях. Оперативне реагування на можливі загрози та інтеграція сучасних технологій, таких як HSM, гарантують не тільки захист даних, а й захист від внутрішніх і зовнішніх атак.

ВИСНОВКИ

У кваліфікаційній роботі отримано наступні наукові та науково-практичні результати:

1. Проаналізовано сучасний стан використання криптографічних алгоритмів в інформаційних системах для забезпечення конфіденційності та цілісності даних. Розглянуто основні типи алгоритмів, зокрема симетричні (AES, DES) та асиметричні (RSA), а також їх застосування для захисту інформації в цифровому середовищі.

2. Здійснено дослідження впливу криптографії на безпеку організацій, зокрема через інтеграцію криптографічних алгоритмів в системи захисту даних. Оцінено роль криптографії в захисті від несанкціонованого доступу, а також забезпеченні безпеки електронної ідентифікації в таких системах, як BankID.

3. Розглянуто аспекти управління криптографічними ключами в організаціях, включаючи методи вибору алгоритмів, управління доступом до ключів та розробку політик безпеки. Виокремлено важливість захисту ключів від компрометації як основного елементу системи безпеки.

4. Досліджено практичні рекомендації щодо впровадження криптографічних алгоритмів в інформаційні системи. У ході роботи було розроблено стратегії інтеграції криптографії в інформаційні процеси організацій, а також оцінено ефективність використання апаратних засобів, таких як HSM, для забезпечення високого рівня захисту даних.

5. Проаналізовано результати застосування криптографії в реальних умовах і проведено оцінку її ефективності на основі результатів використання криптографічних протоколів в сучасних інформаційних платформах.

6. Розроблено ряд рекомендацій щодо покращення практик безпеки для організацій, зокрема впровадження новітніх алгоритмів, оптимізацію процесів управління ключами та підвищення рівня захисту від зовнішніх загроз.

Таким чином, дослідження дозволило глибше зрозуміти роль криптографії в забезпеченні безпеки сучасних інформаційних систем і розробити практичні рекомендації для їх ефективного впровадження.

Результати дослідження можуть бути використані як основа для розробки ефективних методів впровадження криптографії в організаційні інформаційні системи. Практичні рекомендації стосуються як малих, так і великих організацій, що прагнуть покращити безпеку своїх систем і відповідати сучасним стандартам захисту даних.

ПЕРЕЛІК ПОСИЛАНЬ

1. PGP Corporation. An Introduction to Cryptography - 2002. 10-11 с.
2. R. Tripathi, S. Argawal, "Comparative Study of Symmetric and Asymmetric Cryptography Techniques", International Journal of Advanced Foundation and Research in Computer, vol. 1, issue 6, 2014. 5-6 с. [Електронний ресурс] — Режим доступу: https://ijafrc.org/Volumn1/Vol_issue6/9.pdf
3. M. Singh, S. Babbar, Y. Kumar, K. Malhotra "Hybrid Crypthograhic Algorithm", International Journal of Current Advanced Research, 2019.
4. Франчук В.М. Захист інформаційних ресурсів: криптографічні та стеганографічні методи захисту даних. Посібник для викладачів, вчителів та студентів інформатичних спеціальностей НПУ імені М.П.Драгоманова. Інститут інформатики. Київ — 2012. 98-100 с.
5. ISO/IEC 27001: Information technology — Security techniques — Information security management systems — Requirements, 2015.
6. NIST 800-53: Security and Privacy Controls for Federal Information Systems and Organizations, 2021.
7. Закон України «Про основні засади забезпечення кібербезпеки України». [Електронний ресурс] - Режим доступу: https://zakon.rada.gov.ua/laws/show/2163-19
8. Закон України «Про електронну ідентифікацію та електронні довірчі послуги». [Електронний ресурс] - Режим доступу: https://zakon.rada.gov.ua/laws/show/2155-19#Text
9. Закон України «Про електронні документи та електронний документообіг». [Електронний ресурс] - Режим доступу: https://zakon.rada.gov.ua/laws/show/851-15#Text
10. Нацональний стандарт України ДСТУ 4145-2002 [Електронний ресурс] - Режим доступу: https://ksv.do.am/GOST/DSTY_ALL/DSTU2/dstu_4145-2002.pdf
11. О. М. Гапак, І. М. Глепена.Криптоаналіз. Криптографічні протоколи Посібник для студентів інформатичних спеціальностей “УжНУ”. — 2021. 8-18
12. M. S. Aliyu, S. S. K. Yadav, and R. N. Uma, "A Survey of Cryptographic Algorithms

and their Application in Security," International Journal of Advanced Research in Computer Science and Software Engineering, vol. 7, no. 1, 2017

13. Paar, C., & Pelzl, J. (2010). Understanding cryptography: A textbook for students and practitioners. Springer. 55-87 с.
14. Клименко С. В., Малайчук В. П., Селіванов Ю. М., Петренко О. М., Астахов Д. С. Системи передачі інформації із застосуванням інтерактивного блокового криптографічного алгоритму TWOFISH. — 2021. 65-69 с.
15. В.А. Колосов. Аналіз криптосистем із відкритим ключем. НТУ «ХПІ» (м. Харків). 108-115с.
16. European Payments Council (EPC) AISBL. Guidelines on cryptographic algorithms usage and key management. – 2022. 42-47 с.
17. J. Blessing, M. Spencer, D. Weitzner “You Really Shouldn't Roll Your Own Crypto: An Empirical Study of Vulnerabilities in Cryptographic Libraries”, MIT, 2021. 3-12с. [Електронний ресурс] — Режим доступу: https://www.researchgate.net/publication/353210621_You_Really_Shouldn't_Roll_Your_Own_Crypto_An_Empirical_Study_of_Vulnerabilities_in_Cryptographic_Libraries
18. Статистика використання технології “Дія.Підпис”. [Електронний ресурс] — Режим доступу: https://bank.gov.ua/ua/news/all/sistema-bankid-nbu-pidsumki-roboti-v-i-kvartali-2024-roku
19. Підсумки роботи BankID. [Електронний ресурс] — Режим доступу: https://bank.gov.ua/ua/news/all/sistema-bankid-nbu-pidsumki-roboti-v-i-kvartali-2024-roku
20. 2024 Guide to Google’s Cloud Security & Privacy. [Електронний ресурс] — Режим доступу: https://www.cloudwards.net/is-google-drive-secure/#:~:text=Google's%20Security,enable%20is%20two%2Dfactor%20authentication
21. Data encryption options [Електронний ресурс] — Режим доступу: https://cloud.google.com/storage/docs/encryption
22. How to Choose the Right Encryption Algorithm for Your Data? [Електронний

ресурс] — Режим доступу: https://hogonext.com/how-to-choose-the-right-encryption-algorithm-for-your-data/

23. Key Management Best Practices: A Practical Guide. [Електронний ресурс] – Режим доступу: https://www.ssl.com/article/key-management-best-practices-a-practical-guide/
24. Riza G. The study ofthe HSM as a solution to file encryption and security. University of Tirana, 2024. 4-8 с.

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презетація)

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут кібербезпеки та захисту інформації
Кафедра систем та технологій кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА
НА ТЕМУ: «ТЕХНОЛОГІЇ ЗАСТОСУВАННЯ КРИПТОГРАФІЧНИХ АЛГОРИТМІВ З ВІДКРИТИМ ТА ЗАКРИТИМ КЛЮЧЕМ В ІНФОРМАЦІЙНІЙ СИСТЕМІ ОРГАНІЗАЦІЇ»

Керівник:
д.т.н., професор
Кожухівський Андрій Дмитрович

Виконав:
студент 6-го курсу
групи БСДМ-61
Бишук Данило Вікторович

Об'єкт дослідження – застосування криптографічних алгоритмів в інформаційних системах організацій.

Предмет дослідження – технології застосування криптографічних алгоритмів з відкритим та закритим ключем для захисту інформації.

Мета роботи – дослідити ефективність використання криптографічних алгоритмів з відкритим та закритими ключем та розробити рекомендації щодо їх застосування в інформаційних системах організацій.

Наукові завдання:

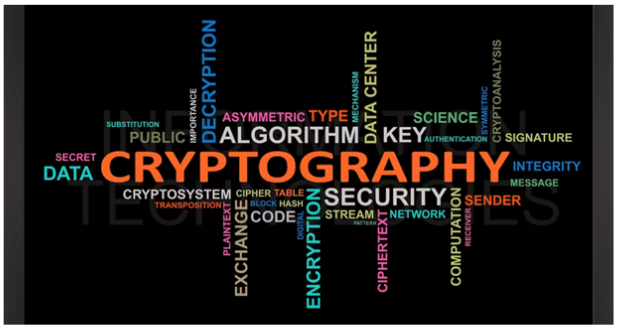
- провести аналіз сучасних проблем та загроз в області інформаційної безпеки.
- розглянути основи функціонування криптографічних алгоритмів з відкритими та закритими ключами.
- проаналізувати існуючі підходи до впровадження цих алгоритмів у практичній діяльності.
- дослідити ефективність сучасних криптографічних рішень у контексті захисту даних.
- розробити рекомендації для впровадження криптографічних алгоритмів в інформаційні системи організацій.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння.

Актуальність дослідження

Криптографія стала інтегрованим рівнем захисту у цифровому бізнесі. Як основа сучасних систем безпеки, криптографія використовується для захисту транзакцій та комунікацій, захисту особистої інформації та інших конфіденційних даних, автентифікації особистості, запобігання підробці документів та встановлення довіри між серверами. Криптографія є одним з найбільш важливих інструментів, що використовуються підприємствами, корпораціями, і навіть державами для захисту систем, в яких зберігаються їхні найважливіші активи – дані.

Невиконання умов криптографії може піддати критично важливу інфраструктуру будь-якої організації вразливості. Сучасне середовище вимагає, щоб організації звертали увагу на те, як криптографія впроваджується та керується на підприємстві.



Криптографія. Цілі криптографії

Криптографія - це наука про методи забезпечення конфіденційності, цілісності та автентичності інформації з використанням математичних та алгоритмічних перетворень. Вона займається розробкою та аналізом криптографічних алгоритмів, які забезпечують захист даних від несанкціонованого доступу та модифікації. Криптографія є основним інструментом у сфері інформаційної безпеки та широко застосовується у різних сферах бізнесу.

Основні цілі криптографії:

- Конфіденційність
- Цілісність
- Автентичність
- Неможливість відмови
- Стійкість до атак

Типи алгоритмів шифрування

Симетричне

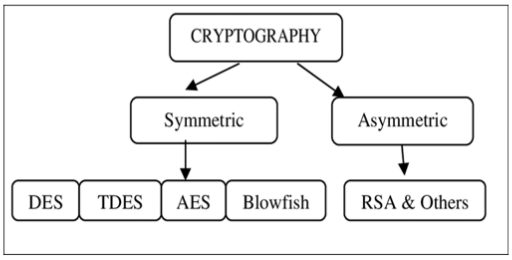
Симетричне шифрування використовує один і той же секретний ключ для шифрування та розшифрування даних.

Ключ має бути відомий і відправнику, і одержувачу. Прикладами симетричних алгоритмів є AES, DES та 3DES. Вони забезпечують високу швидкість шифрування, але потребують безпечної передачі секретного ключа між сторонами

Асиметричне

Асиметричне шифрування, ґрунтується на використанні пари ключів: відкритого ключа та закритого.

Принцип роботи асиметричного шифрування полягає в тому, що інформація, яка зашифрована з використанням відкритого ключа, може бути розшифрована тільки за допомогою відповідного закритого ключа



Реалізація криптографічних алгоритмів у програмному забезпеченні

Етапи:

1) Вибір алгоритму
2) Інтеграція бібліотеки
3) Генерація ключів
4) Шифрування даних
5) Розшифрування
6) Управління ключами

Основні проблеми реалізації:

1) Продуктивність
2) Вразливості через неправильну інтеграцію
3) Застарілі алгоритми
4) Складність в управлінні ключами

Приклади застосування криптоалгоритмів в інформаційних системах

1) Захист з'єднань через HTTPS у веб-сервісах

2) Шифрування даних у хмарних сервісах

3) Електронний підпис для автентифікації та захисту документів

4) Захист доступу до інформаційних систем через автентифікацію та авторизацію

Приклади застосування криптоалгоритмів в інформаційних системах

Застосунок "Дія"

Застосування криптоалгоритмів:

- Шифрування даних на стороні клієнта
- Передавання даних через захищені канали
- Цифровий підпис
- Управління ключами
- Авторизація користувачів
- Верифікація документів
- Захист проти атак
- Шифрування резервних копій

Приклади застосування криптоалгоритмів в інформаційних системах

Система BankID

Застосовуються такі криптоалгоритми:

- OAuth 2.0 - для авторизації користувачів
- X.509 -для підпису ідентифікаційних даних
- PKCS#12 – для зберігання приватних ключів та сертифікатів

Приклади застосування криптоалгоритмів в інформаційних системах

Хмарний сервіс “Google Drive”

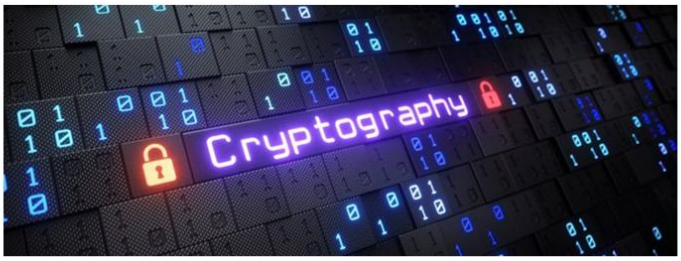
Застосування криптоалгоритмів:

- Шифрування даних на стороні клієнта та передача даних через захищені канали
- Шифрування даних на серверія
- Управління ключами

Методика вибору криптографічних алгоритмів для організацій

Вибір правильного алгоритму шифрування передбачає ретельну оцінку різних факторів, кожен із яких має власний вплив на безпеку, продуктивність і зручність використання.

1. Рівень безпеки.
2. Продуктивність
3. Управління ключами
4. Стандартизація та впровадження алгоритму
5. Орієнтованість на розвиток технологій



Створення політики управління ключами

1. Визначення політики управління ключами
2. Генерація та зберігання ключів
3. Ротація та заміна ключів
4. Управління доступом до ключів
5. Знищення ключів
6. Відповідність стандартам та аудит

Висновки

1. Проаналізовано сучасний стан використання криптографічних алгоритмів в інформаційних системах для забезпечення конфіденційності та цілісності даних. Розглянуто основні типи алгоритмів, зокрема симетричні (AES, DES) та асиметричні (RSA), а також їх застосування для захисту інформації в цифровому середовищі.

2. Здійснено дослідження впливу криптографії на безпеку організацій, зокрема через інтеграцію криптографічних алгоритмів в системи захисту даних. Оцінено роль криптографії в захисті від несанкціонованого доступу, а також забезпеченні безпеки електронної ідентифікації в таких системах, як BankID.

3. Розглянуто аспекти управління криптографічними ключами в організаціях, включаючи методи вибору алгоритмів, управління доступом до ключів та розробку політик безпеки. Виокремлено важливість захисту ключів від компрометації як основного елементу системи безпеки.

4. Досліджено практичні рекомендації щодо впровадження криптографічних алгоритмів в інформаційні системи. У ході роботи було розроблено стратегії інтеграції криптографії в інформаційні процеси організацій, а також оцінено ефективність використання апаратних засобів, таких як HSM, для забезпечення високого рівня захисту даних.

5. Проаналізовано результати застосування криптографії в реальних умовах і проведено оцінку її ефективності на основі результатів використання криптографічних протоколів в сучасних інформаційних платформах.

6. Розроблено ряд рекомендацій щодо покращення практик безпеки для організацій, зокрема впровадження новітніх алгоритмів, оптимізацію процесів управління ключами та підвищення рівня захисту від зовнішніх загроз.