ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до бакалаврської роботи
на тему:

«ДОСЛІДЖЕННЯ ШЛЯХІВ ТА РОЗРОБЛЕННЯ РЕКОМЕНДАЦІЙ ЩОДО ЗАСТОСУВАННЯ КРИПТОГРАФІЧНИХ АЛГОРИТМІВ З ВІДКРИТИМ ТА ЗАКРИТИМ КЛЮЧЕМ В ІНФОРМАЦІЙНІЙ СИСТЕМІ ОРГАНІЗАЦІЇ»

Виконав студент 4 курсу, групи БСД-41
спеціальності 125 Кібербезпека
освітньо-професійної програми «Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)
Бишук Д.В.
(прізвище та ініціали)
Керівник Дмітрієв В.Є.
(прізвище та ініціали)
Рецензент
(прізвище та ініціали)
Нормоконтролер
(прізвище та ініціали)

КИЇВ – 2023

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, інформаційна безпека є важливою ланкою у цілісній системі безпеки будь-чого: це стосується як людини, як організації, так і держави. Для повноцінного і ефективного захисту інформаційних ресурсів, була винайдена така наука як криптографія, що дозволяє зберігати інформацію у захищенному варіанті від усіх охочих. Саме тому, криптографія і її алгоритми все частіше і частіше використовуються спеціалістами для забезпечення максимального захисту від усіх можливих витоків інформації.

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. Дані – це життєво важлива інформація у вигляді персональних даних клієнтів, співробітників, інтелектуальної власності, бізнес-планів та будь-якої іншої конфіденційної інформації. Таким чином, криптографія є критичною інфраструктурою, оскільки безпека конфіденційних даних все більше залежить від криптографічних рішень.

Актуальність теми полягає в тому, що невиконання умов криптографії може піддати критично важливу інфраструктуру будь-якої організації вразливості. Громадська увага до розкритих даних приводить до ерозії бренду. Це сучасне середовище вимагає, щоб організації звертали увагу на те, як криптографія впроваджується та керується на підприємстві.

Тому, дослідження шляхів та розробка рекомендацій щодо захисту інформації з використанням криптографічних алгоритмів є важливою задачею для будь-якої організації.

Об'єкт дослідження – аналіз процесів застосування криптографічних алгоритмів в інформаційній структурі організації.

Предмет дослідження – методи та засоби створення криптографічних алгоритмів з відкритим та закртим ключем в інформаційній системі організації.

Мета дослідження – дослідити шляхи та розробити рекомендації щодо захисту інформації з використанням криптографічних алгоритмів з відкритим та закритим ключем та розробити рекомендації щодо їх застосування.

Завдання дослідження:

1. Провести аналіз використання криптографічних алгоритмів в інформаційній системі організації
2. Проаналізувати вразливості криптографічних алгоритмів дослідити методи та засоби захисту інформаційної системи організації з використанням криптографічних алгоритмів.
3. Розробити рекомендації щодо захисту інформаційної системи організації з використанням криптографічних алгоритмів.
4. Провести експериментальне дослідження ефективності запропонованих рекомендацій.

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

Практичне значення одержаних результатів: рекомендації щодо застосування криптографічних алгоритмів в можуть бути використані у сфері забезпечення кібербезпеки у корпоративних інформаційних системах.

1 АНАЛІЗ АКТУАЛЬНОСТІ ЗАСТОСУВАННЯ КРИПТОГРАФІЧНИХ АЛГОРИТМІВ В ІНФОРМАЦІЙНІЙ СИСТЕМІ ОРГАНІЗАЦІЇ

Застосування криптографічних алгоритмів в інформаційній системі організації є вкрай актуальним, оскільки захист конфіденційної інформації є важливим для будь-якого бізнесу. Криптографія використовується для забезпечення конфіденційності, цілісності та доступності інформації, що дозволяє запобігти несанкціонованому доступу до даних, а також захистити інформацію від крадіжки та пошкодження.

Використання криптографічних алгоритмів також є важливим за дотримання різних законодавчих вимог, пов'язаних із захистом персональних даних та іншої конфіденційної інформації. Наприклад, у Європейському Союзі діє Загальний регламент захисту даних (General Data Protection Regulation - GDPR), який вимагає від організацій захисту персональних даних за допомогою адекватних технічних та організаційних заходів, включаючи застосування криптографії.

Крім того, наразі все більше організацій переходить на хмарні рішення та зберігання даних у хмарі. Використання криптографічних алгоритмів є важливим механізмом захисту даних у хмарному середовищі, де захист даних має бути надійним та безпечним.

Таким чином, застосування криптографічних алгоритмів в інформаційній системі організації залишається актуальним та необхідним для забезпечення безпеки даних та захисту конфіденційної інформації. З розвитком технологій та появою нових загроз криптографічні алгоритми постійно вдосконалюються та доповнюються новими методами захисту даних.

Сьогодні криптографічні алгоритми використовуються у багатьох галузях, включаючи фінанси, охорону здоров'я, урядові служби, наукові дослідження та багато інших. У сучасних інформаційних системах застосовуються різні алгоритми з відкритим та закритим ключем, такі як RSA, AES, DES, Blowfish та багато інших.

Криптографічні алгоритми дозволяють забезпечити конфіденційність, цілісність та автентичність даних. Крім того, вони дозволяють захистити інформацію від несанкціонованого доступу та перешкоджають підробці даних. Важливо відзначити, що безпека інформаційної системи є одним із ключових факторів, що впливають на імідж організації та її довіру у клієнтів.

У зв'язку з цим використання криптографічних алгоритмів стає все більш актуальним і необхідним для захисту конфіденційних даних в інформаційній системі організації.

1.1 Теоретичний аналіз криптографічних алгоритмів

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, включаючи електронну комерцію, банківську справу, хмарні обчислення та зв'язок.

Основні цілі криптографії:

- 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.

Криптографічний алгоритм, або шифр - це математична формула, що описує процеси шифрування і розшифрування. Щоб зашифрувати відкритий текст, криптоалгоритм працює в сполученні з ключем - словом, числом або фразою.

Криптографічних алгоритмів існує безліч. Їх призначення в загальних рисах зрозуміло: захист інформації. Захищати ж інформацію потрібно від різних загроз і різними способами. Щоб правильно задіяти криптоалгоритм (КА), тобто забезпечити надійний і адекватний захист, потрібно розуміти, які бувають КА і який тип алгоритму краще пристосований для вирішення конкретного завдання.

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.

1.2 Область застосування криптографічних алгоритмів

До існуючих галузей застосування крипптографічних алгоритмів належать:

- Шифрування даних: Обидва типи алгоритмів використовуються для шифрування даних. Симетричні алгоритми часто використовуються для шифрування великих обсягів даних, оскільки вони працюють швидше. Асиметричні алгоритми широко використовуються для обміну ключами та встановлення безпечного каналу зв'язку.

- Аутентифікація: Асиметричні алгоритми використовуються для автентифікації користувачів чи систем. Наприклад, вони можуть бути використані для створення цифрових підписів, які підтверджують справжність документа чи повідомлення.
- Забезпечення цифрового підпису: Асиметричні алгоритми використовуються для створення та перевірки електронних цифрових підписів. Цифровий підпис гарантує, що документ або повідомлення не було змінено після підписання, а також підтверджує ідентифікацію відправника.
- Управління ключами: Асиметричні алгоритми зазвичай використовуються для управління ключами в криптографічних системах. Наприклад, вони можуть використовуватися для шифрування та передачі симетричних ключів між двома сторонами.
- Електронна комерція: Криптографічні алгоритми застосовуються для забезпечення безпеки електронних платежів, захисту персональних даних покупців та забезпечення конфіденційності в електронній комерції. Завдяки криптографічним алгоритмам, усі транзакції будуть зашифровані не можуть бути змінені третіми сторонами. Крім того, паролі, які ми встановлюємо для таких сайтів, також захищені ключами, щоб гарантувати, що жоден хакер не отримає доступ до деталей нашої електронної комерції для шкідливих цілей.
- Цифрова валюта: Широко відомим застосуванням криптографії є цифрова валюта, у якій криптовалюти торгуються через Інтернет. Найкращі криптовалюти, такі як Bitcoin, Ethereum і Ripple, були розроблені та продані з часом. З появою безготівкової економіки цифрові валюти привернули увагу світу. Криптовалюти, які не регулюються жодним урядом чи банками, — це наше майбутнє. Технологія блокчейн має багато спільного з цією програмою. Кілька вузлів у блокчейні забезпечені криптографією, яка забезпечує безпечну торгівлю криптовалютою в системі цифрової книги. Ці бухгалтерські книги захищені, збережені та не можуть бути доступні жодній іншій особі чи організації.
- Безпека мереж та зв'язку: Криптографія відіграє важливу роль у забезпеченні

безпеки мереж та зв'язку. Вона використовується для захисту даних, що передаються по мережі, автентифікації учасників мережі та запобігання несанкціонованому доступу до інформації.

Всі ці галузі застосування вимагають міцного та надійного захисту даних та інформації, що робить криптографічні алгоритми з відкритим та закритим ключем невід'ємною частиною сучасних систем безпеки та захисту інформації.

Необхідно сказати, що криптографія має застосування в реальному світі, які неминучі. Оскільки віртуальний світ розвивається, він стає важливим для операцій із підтримкою криптографії в багатьох сферах.Процес передачі повідомлень без доступа до будь-якої сторонньої криптографії став незамінним. Тим не менш, криптоалгоритми також використовуються для зловмисних цілей, які поступилися місцем етичним хакерським операціям. Можливо, час покаже, чи правильне використання криптографії переважить її шкідливі цілі.

1.3 Аналіз загроз інформаційній безпеці в інформаціній 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.

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.

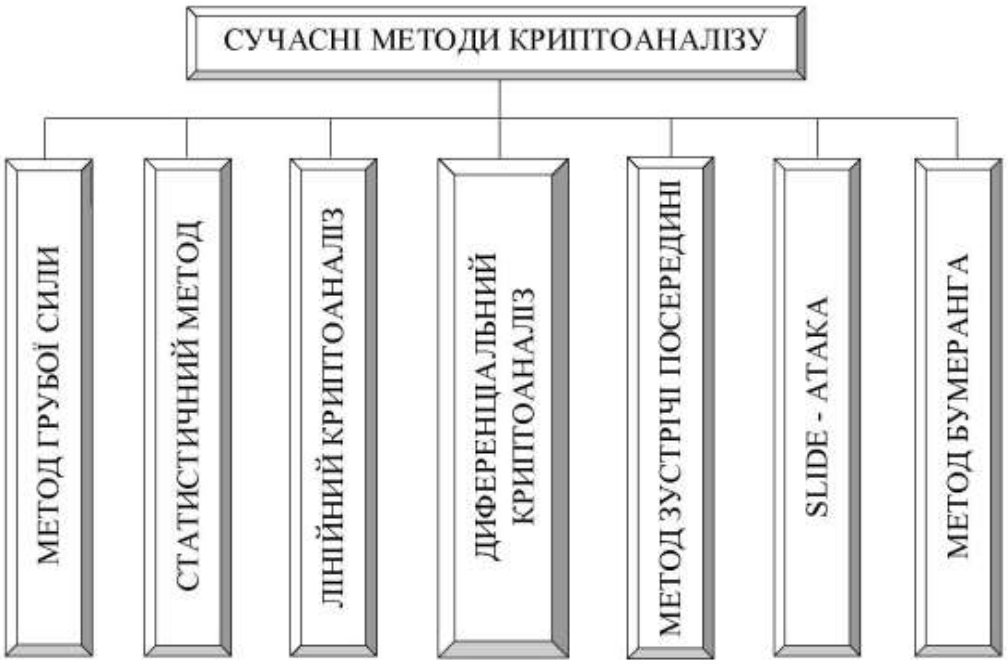

Рис. 1 — Класифікація сучаних методів криптоаналізу

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.

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.

1.4 Огляд існуючих методів захисту інформації з використанням криптографічних алгоритмів

Деякі з найпоширеніших методів захисту інформації з використанням криптографічних алгоритмів включає різноманітні підходи та технології, що

застосовуються для забезпечення конфіденційності, цілісності та доступності даних, а саме:

Шифрування даних: шифрування є одним з основних методів захисту інформації. Використовуючи криптографічні алгоритми, дані перетворюються у шифротекст, що забезпечує їх конфіденційність. Шифрування може бути симетричним (де використовується один ключ для шифрування та розшифрування) або асиметричним (де використовується пара ключів: публічний для шифрування і приватний для розшифрування). Ці методи захисту інформації з використанням криптографічних алгоритмів використовуються в різних сферах, включаючи фінансові установи, електронну комерцію, комунікаційні системи та інші сектори, де конфіденційність та безпека даних є важливими. Методи шифрування з використанням криптографічних алгоритмів дозволяють забезпечити конфіденційність даних, запобігаючи несанкціонованому доступу до них. Застосування симетричних і асиметричних алгоритмів шифрування залежить від конкретного сценарію та потреб безпеки інформації.

Електронний цифровий підпис: Цифровий підпис використовується для забезпечення цілісності та автентичності даних. Він заснований на криптографічних алгоритмах, де повідомлення підписується приватним ключем, а перевірка підпису здійснюється за допомогою відповідного публічного ключа. Електронний цифровий підпис дозволяє перевірити, чи були дані змінені після підпису та встановити авторство повідомлення.

Аутентифікація користувачів: Криптографічні алгоритми використовуються для забезпечення аутентифікації користувачів та контролю доступу до системи. Такі методи, як використання паролів, сертифікатів або біометричних даних, використовують криптографічні алгоритми для забезпечення безпеки інформаційних систем.

Обмін ключами: Криптографічні алгоритми також використовуються для безпечного обміну ключами між комунікуючими сторонами. Алгоритми, такі як алгоритм Діффі-Гелмана, дозволяють сторонам обмінюватися ключами без ризику розкриття їх від інших сторін. За допомогою цього алгоритму дві сторони можуть

узгодити спільний секретний ключ, який потім може бути використаний для симетричного шифрування. Обмін ключами забезпечує безпеку передачі секретного ключа, що робить його важливим методом для захисту інформації.

Хеш-функції є методом захисту інформації, який використовується для перетворення довільного великого блоку даних в коротку, фіксованої довжини хеш-значення. Хеш-значення слугує унікальною "відбиткою" даних і використовується для перевірки цілісності даних та виявлення неправильностей або змін у повідомленні. Хеш-функції є важливим елементом криптографічних протоколів, таких як TLS (Transport Layer Security) та інші, де вони використовуються для забезпечення цілісності та автентичності даних.

Віртуальні приватні мережі (VPN): Криптографічні алгоритми використовуються для створення зашифрованих каналів зв'язку між вузлами в мережі. Це дозволяє забезпечити конфіденційність даних, переданих через мережу, і захистити їх від несанкціонованого доступу.

Криптографічні протоколи є набором правил та процедур, які визначають спосіб обміну даними та ключами між комунікуючими сторонами з використанням криптографічних алгоритмів. Ці протоколи забезпечують безпеку комунікації шляхом застосування шифрування, аутентифікації та інших криптографічних механізмів. Найвідоміші криптографічні протоколи включають SSL/TLS, IPSec, SSH і багато інших.

Ці методи захисту інформації з використанням криптографічних алгоритмів допомагають забезпечити конфіденційність, цілісність та доступність даних, а також забезпечують автентифікацію та невідмовність у передачі інформації. Вони використовуються в різних сферах, таких як фінансові установи, електронна комунікація, електронна торгівля, мережева безпека та багато інших, для захисту конфіденційної та важливої інформації від несанкціонованого доступу та зловживання.

2 ДОСЛІДЖЕННЯ КРИПТОГРАФІЧНИХ АЛГОРИТМІВ З ВІДКРИТИМ ТА ЗАКРИТИМ КЛЮЧЕМ: ПРИНЦИП ЇХ РОБОТИ ТА ЗАСТОСУВАННЯ

Криптографічні алгоритми з відкритим та закритим ключем є основою сучасної криптографії та використовуються для різних цілей, включаючи шифрування даних, автентифікацію та забезпечення цифрового підпису. У цьому розділі розглянемо принцип роботи та сфери застосування цих алгоритмів.

Принцип роботи:

Криптографічні алгоритми із закритим ключем (симетричні алгоритми) використовують один і той же ключ для шифрування та розшифрування даних. Це означає, що відправник та одержувач повинні мати спільний секретний ключ. Прикладами симетричних алгоритмів є AES (Advanced Encryption Standard), DES (Data Encryption Standard) та Blowfish.

Криптографічні алгоритми з відкритим ключем (асиметричні алгоритми) використовують кілька ключів: відкритий і закритий. Відкритий ключ використовується для шифрування даних, а закритий ключ - для їхнього розшифрування. Пара ключів пов'язана таким чином, що інформацію, зашифровану одним ключем, можна розшифрувати лише іншим ключем із пари. Прикладами асиметричних алгоритмів RSA, ElGamal, ECC (еліптичні криві).

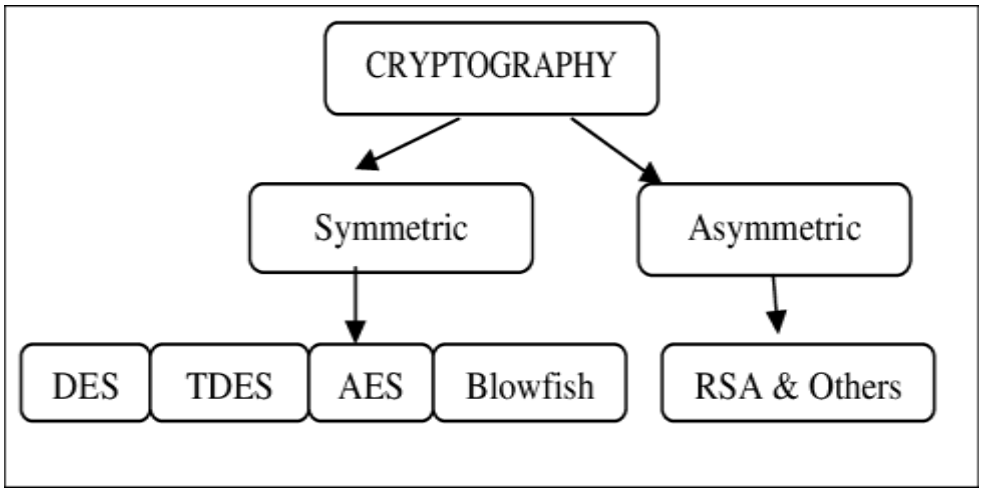

Рис.2 — Класифікація крипптографічних алгоритмів

У криптографії відкритий та закритий ключі є основними компонентами асиметричного шифрування. Вони утворюють пару ключів, яка використовується

для шифрування та розшифрування даних.

Відкритий ключ є загальнодоступним та може бути поширений усім бажаючим. Він використовується для шифрування даних та перевірки цифрового підпису. Закритий ключ, з іншого боку, має залишатися в таємниці та відомий лише його власнику. Закритий ключ використовується для розшифрування даних та створення цифрового підпису.

Процес використання відкритого та закритого ключів включає такі кроки:

1. Відправник отримує відкритий ключ одержувача та використовує його для шифрування даних перед їх надсиланням. Після шифрування дані стають незрозумілими для третіх осіб, і лише одержувач, який має відповідний закритий ключ, зможе їх розшифрувати.
2. Під час створення цифрового підпису відправник використовує свій закритий ключ для створення унікального цифрового підпису, який прикріплюється до даних. Отримувач може використовувати відкритий ключ відправника для перевірки автентичності підпису і переконатися, що дані не були змінені після їх підпису.

Відкритий та закритий ключі тісно пов'язані між собою математичними алгоритмами. Хоча відкритий ключ може бути використаний для шифрування, його використання для розшифровки без знання відповідного закритого ключа є обчислювально неможливим, забезпечуючи цим безпеку даних під час передачі.

2.1 Симетричні та асиметричні типи алгоритмів шфирування

В даний час використовуються дві основні форми шифрування даних: симетричне шифрування та асиметричне шифрування. Щодня, коли ви використовуєте свій веб-браузер, відповідаєте на електронні листи, надсилаєте форми веб-сайту та виконуєте інші дії, відбуваються процеси симетричного та асиметричного шифрування, іноді без вашого відома. Ви також можете бути знайомі з симетричним та асиметричним шифруванням, тому що у вас є досвід роботи з OpenSSL, службами керування ключами або, можливо, ви вже надсилали

зашифрований електронний лист або зашифровували файл Microsoft Word або Adobe PDF за допомогою пароля.

Важливо розуміти різницю між симетричним та асиметричним шифруванням та те, як ці технології безпеки працюють у повсякденній безпечній передачі повідомлень.

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.

Рис.3 — 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.

Популярні приклади симетричного шифрування включають:

- Стандарт шифрування даних (DES)
- Потрійний стандарт шифрування даних (Triple DES)
- Розширений стандарт шифрування (AES)
- Міжнародний алгоритм шифрування даних (IDEA)
- Протокол TLS/SSL

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.

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.

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, також відоме як криптографія з відкритим ключем, ґрунтується на використанні пари ключів: відкритого ключа та закритого ключа. Принцип асиметричного шифрування полягає в тому, що інформація, яка зашифрована з використанням відкритого ключа, може бути розшифрована тільки за допомогою відповідного закритого ключа.

Рис.4 — 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.

Електронний цифровий підпис

Для передачі інформації по незахищеному каналі без внесення змін, наприклад, різні розпорядження, довідки, і тому подібна документація, яка не представляє секрету, використовують елекронний цифровий підпис. Тут користувач обчислює контрольну суму повідомлення, шифрує її таємним ключем та приклеює шифрограму до повідомлення.

Електронний цифровий підпис (ЕЦП) – це криптографічний механізм, який використовується для аутентифікації та забезпечення цілісності електронних документів або повідомлень. Вона дозволяє підтвердити, що повідомлення або документ не було змінено після створення підпису, а також ідентифікувати відправника.

Принцип роботи електронного цифрового підпису ґрунтується на використанні асиметричної криптографії, де використовуються пари ключів: закритий та відкритий ключ. Ці ключі пов'язані математично таким чином, що інформацію, зашифровану одним ключем, можна розшифрувати лише іншим ключем з пари.

Процес створення та перевірки електронного цифрового підпису складається з наступних кроків:

- Генерація ключової пари Першим кроком є генерація ключової пари, що

складається із закритого та відкритого ключів. Закритий ключ зберігається в секреті та використовується для створення підпису, а відкритий ключ поширюється для перевірки підпису.

- Хешування повідомлення: Повідомлення або документ, який потрібно підписати, піддається хешуванню. Хеш-функція перетворює вихідне повідомлення на фіксований розмір хеш-значення.
- Створення підпису: Закритий ключ використовується для створення підпису. Він застосовує до хеш значення повідомлення криптографічну операцію, створюючи цифровий підпис.
- Перевірка підпису: Отримувач повідомлення отримує саме повідомлення, цифровий підпис та відкритий ключ відправника. Він застосовує відкритий ключ до цифрового підпису та перевіряє, чи отримане хеш-значення повідомлення хеш-значенню, отриманому при розшифровці підпису.

Електронний цифровий підпис має низку переваг, серед яких:

- Аутентифікація: Підпис дозволяє перевірити автентифікацію відправника та підтвердити, що повідомлення не було змінено після створення підпису.
- Цілісність: Використовуючи хешування, можна виявити навіть незначні зміни у повідомленні.
- Неможливість відмови: Оскільки підпис є унікальним для кожного повідомлення, відправник не може відмовитися від відповідальності за його вміст.
- Захист від підробки: Підпис створюється за допомогою закритого ключа, який повинен бути відомий лише відправнику. Це ускладнює можливість створення підробленого підпису.

Деякі недоліки електронного цифрового підпису включають:

- Залежність від секретності ключа: Безпека ЕЦП залежить від збереження закритого ключа. Якщо закритий ключ потрапляє в чужі руки, це може призвести до підробки підпису.
- Обчислювальна складність: Створення та перевірка електронного цифрового підпису потребують обчислювальних ресурсів. Складність алгоритмів може

уповільнити процес підписування та перевірки, особливо під час роботи з великими обсягами даних.

Загалом, електронний цифровий підпис є важливим інструментом криптографії, що забезпечує безпеку та довіру в електронних комунікаціях. Вона широко застосовується у сфері електронної комерції, електронного уряду, банківської системи та інших галузях, де потрібна справжність та цілісність інформації.

2.2 Аналіз криптографічних алгоритмів із закритим ключем (симетричні)

AES. AES — це алгоритм симетричного ключа, який працює з двовимірними масивами байтів, відомими як стан, і стан складається з чотирьох рядків кожного байта. AES має розмір ключа 128 192 АБО 256 біт, який захищає від певних поточних і майбутніх атак. Як апаратне, так і програмне забезпечення є швидшими та можуть бути реалізовані на різних платформах.

Ось основні принципи роботи AES:

- Розмір блоку: AES працює із блоками даних розміром 128 біт (16 байт). Якщо дані не вирівняні по межі 128 біт, вони доповнюються до необхідного розміру.
- Ключовий розклад: AES потребує ключа фіксованої довжини, який може бути 128 біт, 192 біт або 256 біт. Ключовий розклад генерує раундові з'єднання на основі вихідного ключа.
- Раунди: AES виконує серію раундових перетворень над блоками даних за допомогою різних раундових ключів. 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.
- SubBytes: Це нелінійне перетворення, в якому кожен байт блоку замінюється на відповідний байт із заздалегідь визначеної таблиці замін (S-блок).
- ShiftRows: Байти у кожному рядку блоку зсуваються циклічно вліво на певну кількість позицій. Це забезпечує дифузію даних усередині блоку.

- MixColumns: Кожен стовпець блоку перемішується шляхом множення на певну матрицю. Це забезпечує лінійну дифузію у блоці.
- AddRoundKey: Кожен байт блоку комбінується з відповідним байтом раундового ключа за допомогою операції XOR.
- Повторення раундових перетворень: Процес SubBytes, ShiftRows, MixColumns та AddRoundKey повторюється задану кількість разів залежно від довжини ключа.
- Фінальний раунд: В останньому раунді перетворення MixColumns опускається, і виконується лише SubBytes, ShiftRows та AddRoundKey.

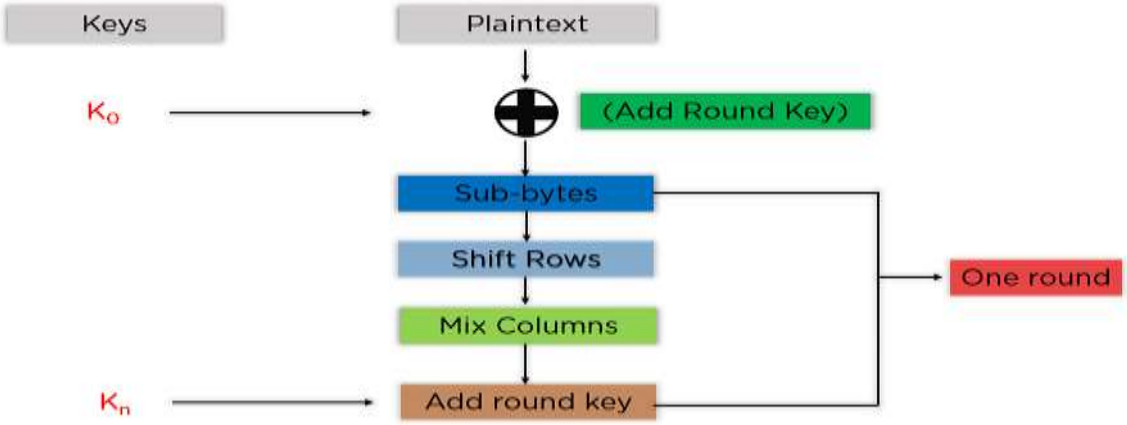

Рис.5 – Принцип роботи AES

Принципи роботи AES ґрунтуються на математичних перетвореннях та заміні байтів. Ці кроки забезпечують хорошу стійкість до атак і забезпечують конфіденційність даних під час шифрування.

DES. DES — це симетричний блоковий шифр, який має 64-бітний вхідний ключ, але використовує лише 56-бітний ключ. Розшифровка виконується за тим самим паролем, що й шифрування, лише етапи виконуються у зворотному порядку. DES має 16 раундів, для створення шифрованого тексту основний алгоритм повторюється 16 разів. Des більш вразливий до атаки грубою силою, оскільки як кількість раундів збільшується, алгоритм безпеки експоненціально зростає.DES був першим стандартом шифрування, опублікованим NIST. Він був розроблений IBM на основі їх Lucifer Cipher. Спочатку 56 бітів ключа вибираються з початкових 64 за допомогою переставленого вибору. Решта вісім бітів або відкидаються, або

використовуються як біти перевірки парності. Потім 56 біт діляться на дві 28-бітні половини; потім кожна половина обробляється окремо. У послідовних раундах обидві половини повертаються вліво на один або два біти, а потім 48 бітів підключу вибираються шляхом перестановки, 24 біти з лівої половини та 24 з правої. Розклад ключів для дешифрування аналогічний, підключі розташовані у зворотному порядку порівняно з шифруванням.

Рис.6 — Принцип роботи DES

Ось основні принципи роботи DES:

- Розмір блоку та ключа: DES працює з блоками даних розміром 64 біти (8 байт). Ключ має довжину 56 біт, проте насправді використовується 64-бітний ключ, з якого 8 біт відведено для перевірки парності.
- Раунди: DES виконує серію раундових перетворень над блоками даних із використанням раундових ключів. Усього в DES використовується 16 раундів.
- Substitution: DES використовує заміну байтів з використанням таблиці замін, відомої як S-блоки. S-блоки перетворюють кожні 6 біт на 4-бітове значення на основі заданої таблиці.
- Permutation: DES виконує перестановку бітів у блоці даних із використанням заданої таблиці перестановок. Це забезпечує поширення даних усередині блоку та вносить дифузію.
- XOR: DES використовує операцію XOR для комбінування раундових ключів із блоком даних на кожному раунді. Це дозволяє внести зміни до блока даних та забезпечити конфіденційність.
- Розширення ключа: Початковий 64-розрядний ключ перетворюється на 56-

розрядний ключ шляхом видалення бітів перевірки парності і виконується розширення ключа для створення 16 раундових ключів.

Принципи роботи DES засновані на комбінації замін та перестановок бітів. Шифрування DES забезпечує конфіденційність даних, проте згодом стало відомо, що він схильний до деяких атак, особливо при використанні малої довжини ключа.

У зв'язку з цим DES в даний час рекомендується використовувати в поєднанні з додатковими механізмами захисту, такими як режими шифрування та додаткові раунди.

TRIPLE DES. У криптографії TRIPLE DES — це загальна назва блокового шифру алгоритму потрійного шифрування даних, який застосовує стандартний алгоритм шифрування даних тричі до кожного блока даних. Алгоритм потрійного DES (3DES) був необхідний як заміна DES через прогрес у пошуку ключів. TDES використовує три цикли повідомлення. Це забезпечує TDES як найнадійніший алгоритм шифрування, оскільки надзвичайно важко зламати 2^168 можливих комбінацій. Іншим варіантом є використання двох різних ключів для алгоритма шифрування. Це зменшує вимоги до пам’яті ключів у TDES. Недоліком цього алгоритму є його надто трудомісткість. Розмір ключа оригінального шифру DES у 56 біт був загалом достатнім, коли розроблявся цей алгоритм, але доступність зростаючої обчислювальної потужності зробила атаки грубою силою можливими. Потрійний DES забезпечує відносно простий метод збільшення розміру ключа DES для захисту від таких атак. Потрібні три 64-бітні ключі для загальної довжини ключа 192 біти. У Triple DES дані шифруються першим ключем, розшифровуються другим ключем і, нарешті, шифруються третім ключем. Потрійний DES працює втричі повільніше, ніж DES, але набагато безпечніший. Процедура дешифрування така ж, як і процедура шифрування, за винятком того, що вона виконується у зворотному порядку.

Blowfish — це симетричний блоковий шифр, який можна ефективно використовувати для шифрування та захисту даних. Він використовує ключ змінної довжини, від 32 біт до 448 біт, що робить його ідеальним для захисту даних. Blowfish був розроблений у 1993 році Брюсом Шнайдером як швидка безкоштовна

альтернатива існуючим алгоритмам шифрування. Алгоритм Blowfish — це мережа Фейстеля, яка повторює просту функцію шифрування 16 разів. Розмір блоку становить 64 біти, а ключ може мати будь-яку довжину до 448 бітів. Він значно швидший, ніж більшість алгоритмів шифрування, коли він реалізований на 32-розрядних мікропроцесорах із великими кешами даних. Алгоритм складається з двох частин: частини розширення ключа та частини шифрування даних. Розширення ключа перетворює ключ довжиною щонайбільше 448 біт у кілька масивів підключів загальною довжиною 4168 байт. Зараз Blowfish вважається небезпечним для багатьох програм. Тому стає дуже важливим розширити цей алгоритм, додавши нові рівні безпеки, щоб зробити його застосовним і залежним від будь-якого загального каналу зв'язку.

2.3 Аналіз криптографічних алгоритмів із відкритим ключем (асиметричні)

RSA. RSA є найпоширенішим алгоритмом з відкритим ключем. Він забезпечує секретність і цифровий підпис. Сформувати публіку і закритий ключ, він використовує просте число та множить великі числа. Для цього він використовує два різні ключі шифрування та дешифрування. З метою безпеки розмір його ключа має бути більше 1024 біт.

RSA є найбільш широко використовуваною криптосистемою з відкритим ключем. Він забезпечує конфіденційність даних, обмін ключами та цифровий підпис. Сильна сторона RSA полягає в розкладанні великих чисел. Це блоковий шифр. У RSA відкритий і зашифрований текст є цілими числами від 0 до n-1 для деякого n. Опис алгоритму RSA виглядає наступним чином. Відкритий текст шифрується блоками, причому кожен блок має двійкове значення, менше деякого числа n.

Компоненти відкритого ключа:

n = добуток двох великих простих чисел p і q

e = випадкове число відносно просте та менше (p-1)(q-1)

Компоненти первинного ключа:

D = e-1 mod ((p-1)(q-1)), мультиплікативне обернення mod((p-1)(q-1))

Шифрування: C = Me mod n

Дешифрування: M = Cd mod n

Цифровий підпис: S = Mdmod n

M = Se mod n = Med mod n (для перевірки підпису)

Щоб RSA був задовільним, необхідно виконати наступні вимоги.

1. p і q два великих простих числа повинні залишатися таємними.

2. Можна знайти значення n, e, d таке, що Med mod n для всіх M<n.

3. Неможливо визначити d за e і n.

4. Легко обчислити середнє і C для всіх значень M<n.

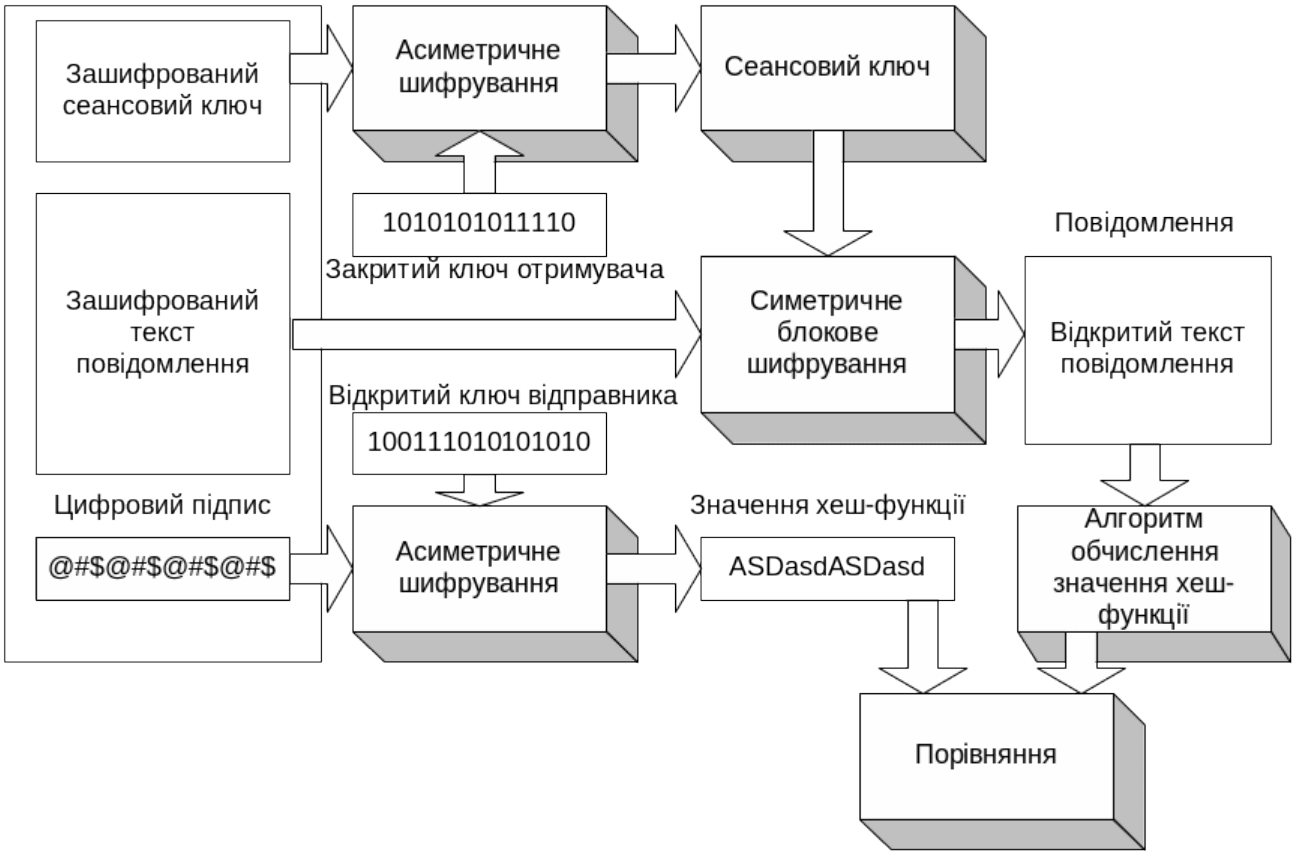

Рис.7 — Алгоритм шифрування/дешифоування RSA

DH. Алгоритм Діффі-Хеллмана (Diffie-Hellman) - це протокол обміну ключами, який дозволяє двом сторонам, що у відкритому каналі зв'язку, згенерувати спільний секретний ключ без попередньої угоди. Це алгоритм відкритого ключа, який використовує дискретні логарифми в кінцевому полі. Він також відомий як

алгоритм обміну ключами. У цьому випадку протокол дозволяє двом користувачам обмінюватися секретним ключем через незахищене середовище без будь-яких попередніх секретів. Таким чином, цей алгоритм вразливий до атаки «людина посередині».

Ось основні принципи роботи алгоритму Діффі-Хеллмана:

- Генерація параметрів: Обидві сторони узгоджуються на виборі великого простого числа "p" та генератора "g", який є примітивним елементом поля відрахувань за модулем "p". Ці параметри загальнодоступні і можуть бути передані по відкритому каналу зв'язку.
- Генерація закритого ключа: Кожна сторона генерує свій закритий ключ. Для цього вибирається випадкове число "a" (для однієї сторони) та випадкове число "b" (для іншої сторони). Ці закриті ключі є секретними та не розкриваються іншим сторонам.
- Обчислення відкритого ключа: Кожна сторона обчислює свій відкритий ключ, використовуючи параметри "p", "g" та свій закритий ключ. Відкритий ключ однієї сторони обчислюється як "A = g^a mod p", а з іншого боку - "B = g^b mod p". Отримані відкриті ключі передаються один одному на відкритому каналі зв'язку.
- Обчислення загального секретного ключа: Кожна сторона використовує отримані відкриті ключі та свій закритий ключ для обчислення загального секретного ключа. Для цього одна сторона обчислює "s=B^a mod p", а інша сторона обчислює "s=A^b mod p". Обидва обчислення призводять до одного й того самого загального секретного ключа "s".
- Використання загального секретного ключа: Отриманий загальний секретний ключ "s" може бути використаний для шифрування та розшифрування повідомлень або для створення ключа для симетричного шифрування.

Алгоритм Діффі-Хеллмана забезпечує безпечне узгодження загального секретного ключа, навіть якщо відкритий канал зв'язку не є безпечним. Він широко використовується в протоколах забезпечення конфіденційності, таких як TLS/SSL, VPN та інших системах, де потрібний обмін секретними ключами.

3 РОЗРОБКА РЕКОМЕНДАЦІЙ ІЗ ЗАСТОСУВАННЯ КРИПТОГРАФІЧНИХ АЛГОРИТМІВ З ВІДКРИТИМ ТА ЗАКРИТИМ КЛЮЧЕМ В ІНФОРМАЦІЙНІЙ СИСТЕМІ

3.1 Дослідження стійкості криптографічних алгоритмів в інформаційній системі організації

Дослідження стійкості криптографічних алгоритмів в інформаційній системі організації є важливою складовою безпеки інформації. Ці дослідження спрямовані на оцінку силки і надійності криптографічних алгоритмів та виявлення можливих вразливостей, які можуть бути використані для атак на систему.

Основні етапи дослідження стійкості криптографічних алгоритмів включають наступні кроки:

1. Аналіз алгоритму: Перший крок полягає в докладному аналізі самого криптографічного алгоритму. Вивчення математичних принципів, на яких базується алгоритм, його структури, особливостей та механізмів шифрування та розшифрування. Цей аналіз допомагає зрозуміти, як сам алгоритм працює та які можливі вразливості можуть бути пов'язані з його конструкцією.
2. Криптоаналіз: Наступний крок полягає в застосуванні криптоаналітичних методів для спроби зламати криптографічний алгоритм. Це може включати атаки на ключ, атаки на шифротекст, аналіз властивостей алгоритму та пошук слабких місць. Цей процес дозволяє виявити можливі вразливості алгоритму та перевірити його стійкість до різних атак.
3. Тестування на реалістичних сценаріях: Після криптоаналізу проводяться тестування на реалістичних сценаріях, де алгоритм використовується в реальній інформаційній системі. Це включає перевірку відповідності алгоритму стандартам безпеки, його працездатності, продуктивності та інтеграції з іншими компонентами системи. Тестування на реальних сценаріях дозволяє оцінити ефективність та надійність алгоритму у реальному середовищі.
4. Оновлення і вдосконалення: Дослідження стійкості криптографічних алгоритмів

також передбачає постійне оновлення і вдосконалення алгоритмів. З'являються нові методи атак та вразливості, тому важливо виявляти та виправляти їх шляхом оновлення алгоритмів та застосування нових підходів до захисту інформації.

Дослідження стійкості криптографічних алгоритмів в інформаційній системі організації допомагає забезпечити надійний захист конфіденційної інформації та запобігти можливим атакам та порушенням безпеки. Вони допомагають виявляти вразливості, покращувати алгоритми та забезпечувати стійкість криптографічного захисту в інформаційних системах.

Криптостійкість RSA

Передбачається, що криптостійкість RSA пов'язана з вирішенням задачі розкладання на множники великих чисел. Однак не було суворо доведено,що потрібно розкласти n на множники, щоб відновити m c і e. Ймовірно, що може бути відкритий зовсім інший спосіб криптоаналізу RSA.

Однак, якщо цей новий спосіб дозволить криптоаналітику отримати d, він також може бути використаний для розкладання на множники великих чисел. Також можна атакувати RSA, визначивши значення (p-1)(q-1). Однак цей метод не простіше розкладання n на множники. Доведено, що при використанні RSA розкриття навіть кількох бітів інформації щодо шифротексту не легше, ніж дешифрування всього повідомлення.

Найбільш очевидною атакою на RSA є розкладання n на множники. Будь-який противник зможе отримати відкритий ключ e та модуль n. Щоб знайти ключ дешифрування d, противник повинен розкласти n на множники. Криптоаналітик може перебирати всеможливі d, доки не підбере правильне значення. Але подібна силова атака навіть менш ефективна, ніж спроба розкладання n на множники.

У 1993 р. Було запропоновано метод церптоаналізу, заснований на малій теоремі Ферма. На жаль, цей метод виявився повільнішим за розкладання на множники. Існує ще одна проблема. Більшість загальноприйнятих тестів встановлює простоту числа з певною ймовірністю.

Що станеться, якщо p чи q виявиться складовим? Тоді модуль n матиме три

або більше дільників. Відповідно деякі дільники будуть меншими за рекомендовану величину, що, у свою чергу, відкриває можливості для атаки шляхом факторизації модуля. Інша небезпека полягає в генерації псевдопростих чисел (чисел Кармайкла), що задовольняють тестам на простоту, але при це не є простими. Однак ймовірність генерації таких чисел зневажливо мала. Насправді, послідовно застосовуючи набір різних тестів на простоту, можна звести можливість генерації складового числа до необхідного мінімуму.

Підсумки безпеки RSA

На підставі відомих атак можна сформулювати такі обмеження при використанні RSA:

- знання однієї пари показників шифрування/дешифрування для даного модуля дозволяє зловмиснику розкласти модуль на множники;
- знання однієї пари показників шифрування/дешифрування для даного модуля дозволяє зловмисникові обчислити інші пари показників, не розладнаючи модуль на множники;
- у криптографічних протоколах з використанням RSA загальний модуль використовуватися не повинен. (Це є очевидним наслідком попередніх двох пунктів.);
- для запобігання розкриттю малого показника шифрування повідомлення повинні бути доповнені («набиті») випадковими значеннями;
- показник дешифрування повинен бути великим.

Зауважимо, що недостатньо використовувати криптостійкий алгоритм; безпечною має бути вся криптосистема, включаючи криптографічний протокол. Слабке місце будь-якого з трьох компонентів зробить небезпечним всю систему.

3.2 Безпечна передача даних за допомогою шифрування SSL

SSL означає Secure Sockets Layer. Це галузевий стандарт безпеки, який шифрує персональні дані на одному кінці за допомогою відкритого ключа

шифрування, і лише цільовий сервер призначення, який перевіряє відкритий ключ на відповідність закритому ключу на вихідному сервері, може декодувати інформацію, щойно вона надходить. Щоб зберегти цю віртуальну безпечну доставку, SSL вимагає кількох кроків і введення додаткових служб.

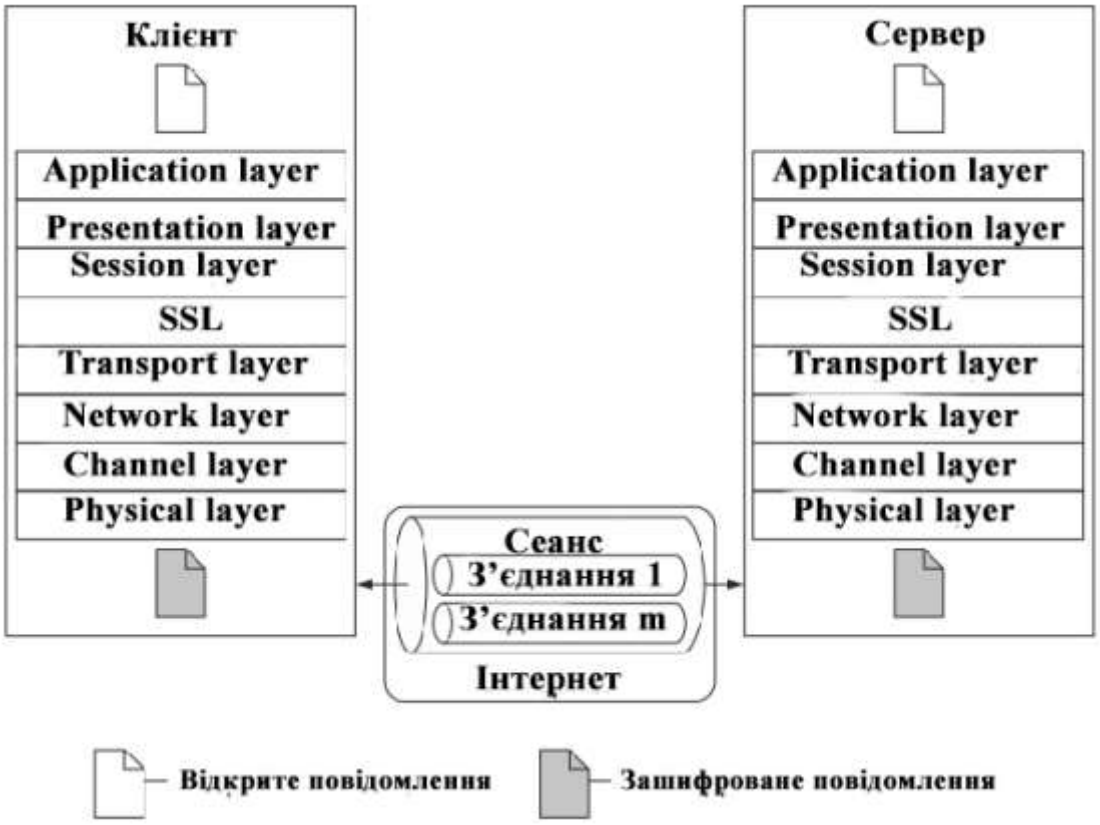

Рис. 8 — Взаємодія клієнта та сервера за допомогою SSL

Handshake SSL:

Коли користувач, якого в PKI називають «довіряючою стороною», відвідує сайт, захищений протоколом SSL, він або вона побачить, що в адресному рядку оголошення протоколу читає HTTPS. HTTPS, SSL і TLS описують комбінацію надійного рівня, який дозволяє застосовувати шифрування через HTTPS. Крім того, у самому браузері може бути вказівка: Chrome показує зелений замок, а Firefox показує сірий замок перед URL-адресою. При натисканні на ці замки буде надано більше інформації про сертифікат.

Після того як ви застосували сертифікат до свого сайту, браузер перевіряючої сторони повинен перевірити сертифікат. Це називається «SSL Handshake». Ключ

обмінюється, тобто повіряюча сторона надає відкритий ключ, а ваш сервер зіставляє його з закритим ключем. Якщо він збігається, встановлюється безпечне з'єднання, і зашифровані дані можуть бути передані.

Центри сертифікації SSL (CA):

Ці кроки та послуги разом називаються інфраструктурою відкритих ключів (PKI). PKI складається з органу видачі, який також називається центром сертифікації (CA), органу реєстрації (RA), бази даних сертифікатів і сховища сертифікатів.

Ви повинні вибрати підписаний сертифікат від надійних центрів сертифікації, таких як Comodo, Symantec, GlobalSign та інших відомих ЦС. Щоб отримати сертифікат, ви повинні підтвердити свою особу в постачальника, а коли він буде виданий, ви повинні встановити його в сховищі сертифікатів на вашому надійному сервері. Сертифікати не є безкоштовними, і, крім того, це вимагає суворих вимог до перевірки, тому третім особам важко отримати підроблений сертифікат. ЦС повинен прийняти вашу заявку в реєструючий орган (RA). RA може бути органом сертифікації, або RA може бути в змозі перевірити, що особа, яка запитує сертифікацію, заслуговує довіри. Деякі організації видають власні сертифікати рівня домену (самопідписані сертифікати) для внутрішнього використання на власних пристроях і серверах.

Аудит SSL:

Високий рівень безпеки залежить від надійності центру сертифікації, що видав, і цілісності сервера. Коли вам видається сертифікат SSL, також видаються інші сертифікати, як-от кореневий і проміжний сертифікати. Це забезпечує додатковий рівень довіри, який браузер використовує для перевірки того, що сертифікат і його постачальник найбільш сумісні з SSL.

Через шахрайську видачу сертифікатів нелегальними особами або хакерами центри сертифікації зобов'язані вести інвентаризацію сертифікатів, що видаються, під назвою бази даних сертифікатів. Він відстежує запитані, видані та відкликані сертифікати. Також важливо, щоб ЦС мав план зв'язку для інформування власників сертифікатів про будь-які порушення або компрометацію безпеки.

Організація, яка надсилає запит, може зробити ряд речей, щоб зменшити загрозу порушення сертифіката, перевіряючи власні системи, відстежуючи, які з них вимагають власні сертифікати та/або сертифікати відкритих ключів, і відстежуючи інформацію про безпеку для кожної системи, включаючи списки контролю доступу. , якорі довіри та терміни дії сертифікатів.

Додатковий захист можна додати за допомогою HSTS (HTTP Strict Transport Security). HSTS — це стандарт, до якого додається додатковий заголовок. Цей заголовок ігнорується, якщо протоколом є HTTP, але якщо викликається HTTPS, сервер читає заголовок, перш ніж надати доступ перевіряючій стороні. Якщо безпеку підключення неможливо перевірити, підключення не буде встановлено. Для HSTS потрібне з'єднання HTTPS, тому додавання HSTS означає також запобігання атак видалення, які перетворюють HTTPS на HTTP.

Різні типи перевірки:

Існують різні типи сертифікатів, які забезпечують різні рівні безпеки.

- Сертифікати SSL із підтвердженням домену генеруються за кілька хвилин, оскільки ЦС лише підтверджує право власності на домен.
- Підтверджений організацією сертифікат SSL, це може зайняти від кількох годин до кількох днів, оскільки ЦС потрібно перевірити зв'язок між заявником і правом власності на домен, а також перевірити існування бізнесу.
- Сертифікат EV (розширена перевірка) SSL є надзвичайно безпечним, тому перед тим, як центр сертифікації видасть його, потрібно кілька типів автентифікації. Ви повинні підтвердити, що ваша організація юридично зареєстрована та діє. Ви повинні вказати дійсну адресу та номер телефону. Ви повинні довести, що ваша організація має виключні права на домен, про який йде мова, і що особа, яка замовляє сертифікат, має на це повноваження. Нарешті, центр сертифікації перевірить, чи ваша організація не внесена до жодного державного чорного списку. Браузер, який завантажує сторінку, сертифіковану сертифікатом EV SSL, відображатиме додаткові візуальні підказки, як-от змінення тексту в адресному рядку на зелений (Firefox) або додавання зеленого блоку в адресний

рядок (Chrome). Сертифікати електромобілів можуть тривати до кількох тижнів. Різні сертифікати мають різну вартість, і постачальники можуть стягувати від 8 доларів США до 1200 доларів США за річний сертифікат. Час, необхідний для отримання сертифіката, також різниться залежно від необхідного рівня перевірки.

Переваги сертифікатів SSL:

- Сертифікат SSL шифрує поточну інформацію, щоб уникнути перерв третьої сторони та зберігає ваші дані від сторонніх очей.
- Використання SSL має переваги для SEO. Google оголосив, що вони збираються розглядати наявність SSL як сигнал ранжирування.
- Якщо ви приймаєте платежі онлайн, вам потрібен сертифікат SSL, щоб відповідати стандартам, визначеним індустрією платіжних карток для онлайн-транзакцій.
- CA автентифікує ваш бізнес, дотримуючись розширеного процесу перевірки, і ввімкне зелений адресний рядок у більшості браузерів, щоб користувачі могли легко ідентифікувати фішингові сайти.
- Окрім 256-бітного шифрування, належний сертифікат SSL також забезпечує автентифікацію. Це означає, що ви можете бути впевнені, що надсилаєте інформацію на правильний сервер із надійним шифруванням.

Імлементація SSL на сервері.

Якщо ви встановили SSL, процес його ввімкнення виглядає приблизно так:

- Під час налаштування сервера або перед подачею заявки на отримання сертифіката ви повинні переконатися, що ваш запис WHOIS актуальний і містить правильний список. Цей сервер буде вашим надійним сервером. (WHOIS — це серверний протокол, який дозволяє за допомогою запиту ідентифікувати право власності на домен і доступ до нього.)
- Програма SSL запропонує вам інформацію про ваш веб-сайт і вашу компанію, а потім створить відкритий ключ і закритий ключ.
- Далі ви створюєте запит на підписання сертифіката (CSR) на своєму сервері, який окрім відкритого ключа включатиме підтверджувальну інформацію, таку як назва та місцезнаходження вашої компанії та домен веб-сайту. Потім ви

надсилаєте CSR до органу, який видав сертифікат. ЦС використовуватиме CSR і запит WHOIS для перевірки вашої компанії та домену.

- Після підтвердження буде видано сертифікат. Коли ви отримаєте сертифікат SSL, ви встановите його на своєму надійному сервері в сховищі сертифікатів.

Якщо сертифікат недійсний, термін його дії минув або є підозри з іншого боку, перевіряюча сторона побачить сповіщення з браузера про те, що сертифікат не можна перевірити. Це вказує на неперевірений сертифікат або на використання будь-якого самопідписаного сертифіката взагалі.

Багато сайтів, звичайно, подають незашифрований вміст, а також зашифрований вміст. Якщо у вас є якісь дані, які все ще доставляються через HTTP, а не через HTTPS, користувач отримає попередження (помилка змішаного вмісту), що може викликати тривогу. Найкраща практика під час впровадження SSL – переконатися, що всі ваші дані доставляються через HTTPS, незалежно від того, чи є вони конфіденційними.

3.3 Розробка рекомендацій щодо імплементації симетричних і асиметричних криптографічних алгоритмів

1. Використовуйте надійні алгоритми: При виборі криптографічних алгоритмів з відкритим і закритим ключем, переконайтеся, що вони відповідають вимогам безпеки та є відомими, добре дослідженими алгоритмами. Оберіть алгоритми, які вважаються стандартами безпеки та мають відповідні сертифікати (RSA).

2. Використовуйте достатню довжину ключа: Довжина ключа має велике значення для безпеки криптографічного алгоритму. Використовуйте рекомендовані довжини ключів для конкретного алгоритму, які забезпечать високий рівень стійкості.

3. Забезпечте безпеку ключів: Ключі мають бути добре захищеними від несанкціонованого доступу. Використовуйте надійні методи зберігання ключів, такі як використання захищених сховищ, шифрування ключів паролем або використання апаратних модулів безпеки.

4. Регулярно оновлюйте ключі: Ключі мають бути періодично оновлюваними для забезпечення безпеки системи. Встановіть процедури для регулярної зміни ключів та виконуйте їх відповідно до вимог безпеки.

5. Забезпечте аутентифікацію та авторизацію: Криптографічні алгоритми з відкритим та закритим ключем можуть бути використані для забезпечення аутентифікації користувачів та авторизації їх доступу до ресурсів системи. Використовуйте механізми цифрових підписів або інші методи аутентифікації для перевірки ідентичності користувачів та контролю доступу до конфіденційної інформації.

6. Застосуйте комплексний підхід до захисту інформації: Криптографічні алгоритми є однією з складових частин системи захисту інформації. Використовуйте їх у поєднанні з іншими заходами безпеки, такими як мережеві заходи безпеки, фізичний доступ та політики безпеки, для створення комплексної системи захисту інформації.

7. Проводьте аудит безпеки: Регулярно проводьте аудит безпеки, щоб переконатися, що криптографічні алгоритми правильно застосовуються та виконують свої функції безпеки. Виявляйте можливі вразливості та проблеми та вживайте заходів для їх виправлення.

8. Забезпечте навчання та освіту персоналу: Персонал, що працює з інформаційною системою, має мати достатні знання та розуміння щодо застосування криптографічних алгоритмів. Забезпечте навчання та освіту персоналу з питань безпеки і застосування криптографічних методів для забезпечення правильного використання та захисту інформаційної системи.

Застосування цих рекомендацій допоможе забезпечити ефективне та безпечне застосування криптографічних алгоритмів з відкритим та закритим ключем в інформаційній системі організації та зменшить ризик несанкціонованого доступу до конфіденційної інформації.

ВИСНОВОК

У сучасному цифровому середовищі, де інформація є цінним активом, забезпечення безпеки та конфіденційності стає надзвичайно важливим завданням для організацій. Використання криптографічних алгоритмів з відкритим та закритим ключем є ефективним способом захисту інформації від несанкціонованого доступу та зловживання.

Криптографія в інформаційній безпеці є кращим рішенням багатьох складних завдань. Криптографічна технологія – це спосіб вирішення проблем безпеки. Безпека даних – це спосіб вивчення, за допомогою якого ми можемо захистити нашу інформацію. Ця техніка є найважливішою, оскільки кілька галузей державного управління хочуть убезпечити своїх громадян. З кожним днем відбувається стрімке зростання електронного зв'язку та обміну ним між людьми без будь-якої безпеки в кібернетичному циклі. Найважливіша мета криптографічних методів у життєвому циклі інформаційної безпеки полягає в тому, що повинні бути найнадійніші алгоритми секретності. Метою цих алгоритмів буде забезпечення конфіденційності та інших методів інформаційної безпеки.

В процесі дослідження було виявлено різні криптографічні алгоритми з відкритим та закритим ключем, такі як RSA, AES, DES, ЕЦП та інші. Кожен з них має свої переваги та особливості, і вибір конкретного алгоритму залежить від потреб та вимог організації.

Дослідження показало, що успішне впровадження криптографічних алгоритмів в інформаційній системі організації вимагає врахування кількох основних рекомендацій: проведення аналізу вимог безпеки, використання надійних алгоритмів, менеджмент ключів,регулярне оновлення алгоритмів,тощо

Таким чином, дослідження шляхів та розроблення рекомендацій щодо застосування криптографічних алгоритмів з відкритим та закритим ключем в інформаційній системі організації дозволило виявити важливі аспекти безпеки, вибрати відповідні алгоритми та сформулювати рекомендації для успішного впровадження та застосування криптографічного захисту.

ПЕРЕЛІК ПОСИЛАНЬ

1. М. В. Захарченко, О. В. Онацький, Л. Г. Йона, Т. М. Шинкарчук. «Асиметричні методи шифруванняв телекомунікаціях: навчальний посібник. Модуль 2. Криптографічні методи захисту інформації в телекомунікаційних системах та мережах.». - 2011. 46 с.
2. В.А. Колосов. Аналіз криптосистем із відкритим ключем. НТУ «ХПИ» (м. Харків). 108-115с.
3. Paar, C., & Pelzl, J. (2010). Understanding cryptography: A textbook for students and practitioners. Springer. 55-87 с.
4. Stinson, D. R. (2018). Cryptography: Theory and practice. CRC Press. Boneh, D., & Shoup, V. (2017). A graduate course in applied cryptography. 137 с.
5. Клименко С. В., Малайчук В. П., Селіванов Ю. М., Петренко О. М., Астахов Д. С. СИСТЕМА ПЕРЕДАЧІ ІНФОРМАЦІЇ ІЗ ЗАСТОСУВАННЯМ ІНТЕРАКТИВНОГО БЛОКОВОГО КРИПТОГРАФІЧНОГО АЛГОРИТМУ TWOFISH.— 2021. 65-69 с.
6. 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 с.
7. European Payments Council (EPC) AISBL. Guidelines on cryptographic algorithms usage and key management. – 2022. 33-38 с.
8. 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
9. P. Nagesh and N. Ramaraju "A comparative study of symmetric and asymmetric encryption algorithms for data security",The International Journal of Advanced Research in Computer Science, vol. 8, no. 5, 2017.
10. Методи шифрування. [Електронний ресурс] – Режим доступу:

11. https://studfile.net/preview/6012701/page:44/
12. Characteristics, Types and Applications of Cryptography. [Електронний ресурс]– Режим доступу: https://www.analyticssteps.com/blogs/characteristics-types-and-applications-cryptography
13. Symmetric vs. Asymmetric Encryption: What's the Difference? [Електронний ресурс] — Режим доступу: https://www.trentonsystems.com/blog/symmetric-vs-asymmetric-encryption
14. Transmit Data Securely with SSL Encryption. [Електронний ресурс] — Режим доступу: https://www.ssl2buy.com/wiki/transmit-data-securely-with-ssl-encryption