Одеський коледж комп’ютерних технології «Сервер»

Звіт з практичної роботи №4

З предмету «Технології захисту інформації»

Тема : «Опис сучасних нормативних систем шифрування та їх застосування в Україні»

Виконував :

Студент групи К21.1

Машков Володимир

Одеса 2024

ВСТУП

Сучасні нормативні системи шифрування відіграють ключову роль у забезпеченні безпеки даних в Україні, особливо в умовах посилення кіберзагроз і необхідності захисту державної та комерційної інформації. Складність завдань із захисту даних вимагає різноманітного та комбінованого використання криптографічних алгоритмів, враховуючи специфіку інформаційних загроз. Шифрування даних стало основою інформаційної безпеки, і важливо розуміти, які системи використовуються, як вони працюють і які їхні сильні та слабкі сторони.

СУЧАСНІ СИСТЕМИ ШИФРУВАННЯ ДАНИХ ТА ЇХ ЗАСТОСУВАННЯ

Для прикладу демонстрації та наведення прикладів, було обрано Україну, у якій використовуються різні типи шифрування, а саме :

* канальне шифрування,
* наскрізне шифрування,
* комбіноване шифрування,
* шифрування файлів.

Кожна з цих систем вирішує свої завдання, надаючи різні рівні захисту даних залежно від конкретних вимог до системи безпеки.

Далі у стислому форматі буде розглянуто те, які системи шифрування існують та використовуються :

1. Канальне шифрування

Цей тип шифрування використовується для захисту даних, що передаються через канали зв'язку. Шифрування застосовується на етапі передачі даних між відправником і одержувачем, що запобігає несанкціонованому доступу до інформації під час передачі. Прикладами можуть слугувати системи захисту телекомунікацій, як-от IPsec (Internet Protocol Security) і SSL/TLS (Secure Sockets Layer / Transport Layer Security).

1. Скрізне шифрування

Наскрізь шифрування забезпечує конфіденційність даних на всьому шляху від відправника до одержувача. Це означає, що дані шифруються на пристрої відправника і розшифровуються тільки на пристрої одержувача, що унеможливлює доступ третіх осіб, включно з постачальниками послуг зв'язку. Прикладом таких систем є широко використовувана в Україні та світі система месенджерів, таких як WhatsApp і Signal, де реалізовано наскрізь шифрування для захисту особистого листування.

1. Комбіноване шифрування

Цей метод поєднує різні типи шифрування, включно із симетричними та асиметричними алгоритмами, щоб забезпечити вищий ступінь захисту даних. Наприклад, у системах цифрового підпису використовують асиметричні алгоритми для підписання повідомлень і симетричні для прискорення процесу шифрування. Прикладом може слугувати використання гібридної схеми шифрування в протоколах передачі даних, таких як PGP (Pretty Good Privacy).

1. Шифрування файлів

Шифрування файлів застосовується для захисту даних, що знаходяться в сховищах або передаються через мережі. Цей метод шифрування робить інформацію недоступною для третіх осіб навіть у разі фізичного доступу до носія даних. Прикладами систем шифрування файлів є популярні в Україні рішення VeraCrypt і BitLocker.

Для забезпечення роботи вищеописаних криптографічних систем використовують різні алгоритми шифрування, кожен з яких має певні характеристики і використовується для вирішення специфічних завдань. Далі буде розглянуто схему шифрування AES (Advanced Encryption Standard) :

Advanced Encryption Standard – є Одним із найбільш широко використовуваних алгоритмів в Україні. Це симетричний алгоритм блочного шифрування, який застосовують для шифрування файлів і даних у різних системах безпеки. Він був прийнятий як стандарт шифрування урядом США в 2001 році і використовується для захисту конфіденційної інформації, включно з військовими та державними даними.

Схема роботи AES :

1. Генерація ключа: Генерується унікальний симетричний ключ, який буде використовуватися як для шифрування, так і для розшифрування даних. Ключ може мати довжину 128, 192 або 256 біт.
2. Розбиття даних на блоки: Дані розбиваються на блоки фіксованої довжини (128 біт).
3. Шифрування блоків: Кожен блок даних проходить через кілька циклів трансформації, що включають в себе підстановки, перестановки і лінійні перетворення. Кількість таких циклів залежить від довжини ключа (наприклад, 10 циклів для 128-бітного ключа).
4. Результат: Після завершення всіх циклів виходять зашифровані блоки даних, які потім об'єднуються в підсумковий зашифрований файл або повідомлення.

У цього методу шифрування є наступні доліки :

* Висока швидкість роботи, що робить його придатним для шифрування великих обсягів даних.
* Високий рівень безпеки, що робить його стійким до більшості відомих атак, включно з атаками грубої сили.
* Гнучкість використання, завдяки можливості вибору довжини ключа.

Але, незважаючи на свою широку популярність і визнання як безпечного алгоритму, AES не позбавлений певних недоліків, особливо в контексті специфічних загроз і вимог до захисту даних, а саме :

* Уразливість до атак по побічних каналах: AES як симетричний алгоритм шифрування вразливий до атак по побічних каналах, які використовують фізичні характеристики пристрою для отримання даних, як-от електромагнітні випромінювання, споживання енергії або час виконання операцій. Наприклад, якщо пристрій із шифруванням AES не захищений, зловмисник може проаналізувати електромагнітне випромінювання і на основі цих даних відновити шифрувальний ключ.
* Загроза злому під час використання слабких або повторюваних ключів: Хоча алгоритм AES сам по собі безпечний, його безпека безпосередньо залежить від довжини та якості ключа. Використання слабких, коротких або повторюваних ключів може істотно знизити рівень захисту і зробити систему вразливою до атак грубої сили. У разі використання 128-бітних ключів існує ймовірність, що в майбутньому з появою квантових комп'ютерів такі ключі можуть бути зламані відносно швидко.
* Неефективність для захисту невеликих обсягів даних: AES розроблявся для шифрування великих обсягів даних, що робить його неефективним для захисту малих файлів або коротких повідомлень. У таких випадках він може бути надлишковим за ресурсами і сповільнювати продуктивність системи.
* Неможливість захисту від деяких типів атак: AES не захищений від атак із використанням квантових обчислень. Квантові комп'ютери можуть у майбутньому реалізовувати атаки, як-от метод Гровера, який потенційно може скоротити час злому симетричних ключів наполовину, роблячи 128-бітові ключі вразливими.
* Відсутність вбудованої підтримки для управління ключами: AES не надає вбудованих механізмів управління ключами, що може стати проблемою під час реалізації криптосистеми на практиці. Без належного управління ключами, наприклад, ротації ключів або забезпечення їхньої конфіденційності, навіть безпечний алгоритм стає вразливим.

АКТУАЛЬНІСТЬ І ПОПУЛЯРИЗАЦІЯ КРИПТОГРАФІЧНИХ СИСТЕМ

Актуальність застосування криптографічних систем в Україні зумовлена необхідністю захисту даних в умовах зростаючих кіберзагроз і політичної нестабільності. Державні установи, фінансові організації та бізнес-сектор дедалі активніше використовують сучасні технології для захисту інформації. Серед усіх перерахованих типів шифрування найбільшого поширення набули системи наскрізь шифрування і шифрування файлів. Це пов'язано з масовим переходом на віддалену роботу, використанням хмарних технологій і зростанням кількості кібератак, спрямованих на крадіжку особистих даних і промислового шпигунства.

Використання гібридних систем шифрування, що поєднують симетричні та асиметричні алгоритми, також стало популярнішим, оскільки такі системи забезпечують баланс між безпекою і швидкістю обробки даних.

ВИСНОВОК

Сучасні криптографічні системи в Україні відіграють ключову роль у забезпеченні безпеки як державної, так і приватної інформації. Широке застосування знаходять такі методи, як наскрізь шифрування та шифрування файлів, що зумовлено потребою в захисті даних на різних рівнях. Алгоритм AES є одним із найпопулярніших рішень, завдяки своїй надійності та високій продуктивності. З огляду на складність і різноманітність загроз, комбіноване використання шифрувальних алгоритмів залишається найбільш ефективною стратегією захисту даних в умовах сучасної інформаційної безпеки.