УДК 004.056

А. І. Тарнавський

АНАЛІЗ МЕТОДІВ ШИФРУВАННЯ ДАНИХ

Вінницький Національний Технічний Університет

Анотація

Розглянуто популярні алгоритми шифрування для забезпечення інформаційної безпеки в корпоративних середовищах. Висвітлено їх переваги, недоліки та можливості застосування.

Ключові слова: шифрований обмін даними, шифрування файлів, методи шифрування даних.

Abstract

Analyzed popular encryption algorithms for ensuring information security in corporate environments. Their advantages, disadvantages, and application possibilities are highlighted.

Keywords: encrypted data exchange, file encryption, authentication, encrypting methods.

Вступ

Сьогодні питання забезпечення інформаційної безпеки в корпоративних середовищах стає надзвичайно актуальним, оскільки обсяг даних, які обробляються, передаються та зберігаються в таких середовищах, постійно зростає. З розвитком технологій збільшується кількість кіберзагроз, що створюють ризики витоку конфіденційної інформації, фінансових втрат і пошкодження репутації компаній. Забезпечення захищеного обміну файлами та даними є необхідною умовою для ефективної роботи сучасних підприємств.

Результати дослідження

Для забезпечення інформаційної безпеки в корпоративних середовищах надзвичайно важливим є використання ефективних методів шифрування, які гарантують конфіденційність, цілісність та автентичність даних. Різні алгоритми шифрування забезпечують різні рівні безпеки і мають свої переваги та обмеження.

У сучасних системах застосовується комбінація симетричних, асиметричних алгоритмів шифрування та хешування, що дозволяє забезпечити як високу швидкість роботи, так і надійний захист інформації. Нижче розглянуто найпоширеніші алгоритми, їх особливості та області застосування:

1. AES[1] (Advanced Encryption Standard) AES є одним із найпопулярніших симетричних алгоритмів шифрування. Він використовується у багатьох корпоративних середовищах завдяки високій швидкості, стійкості до атак та широкій підтримці. AES підтримує ключі довжиною 128, 192 та 256 біт, що дозволяє налаштовувати рівень безпеки залежно від потреб системи. Однак AES вимагає безпечного обміну ключами, що може бути складним у розподілених середовищах.
2. RSA[2] (Rivest–Shamir–Adleman) RSA є стандартом асиметричного шифрування, який використовується для безпечного обміну ключами, цифрового підпису та автентифікації. Його основною перевагою є можливість забезпечення безпеки навіть у публічних мережах. Недоліком RSA є низька швидкість роботи, через що його зазвичай використовують у поєднанні з симетричними алгоритмами.
3. MD5[3] — це криптографічний геш-алгоритм, який перетворює вхідні дані довільної довжини у фіксований 128-бітний (16-байтний) геш. Він був широко використаний для перевірки цілісності даних і створення цифрових підписів. Однак через виявлення вразливостей у вигляді колізій (можливості для різних вхідних даних створювати однаковий геш) його безпека вважається недостатньою для криптографічних цілей.

4. ECC[4] (Elliptic Curve Cryptography) ECC є сучасним методом асиметричного шифрування, який забезпечує еквівалентний рівень безпеки з меншою довжиною ключа порівняно з RSA. Це дозволяє зменшити обчислювальні витрати, що є важливим для пристроїв із обмеженими ресурсами. Однак ECC поки що має обмежену підтримку у деяких системах.

Висновки

У результаті аналізу сучасних алгоритмів шифрування можна зробити наступні висновки:

1. AES є одним із найефективніших симетричних алгоритмів для шифрування великих обсягів даних. Він забезпечує високий рівень захисту, але потребує безпечного обміну ключами, що є критичним завданням для його використання.

2. RSA чудово підходить для захисту ключів у публічних мережах і підтвердження автентичності, однак його швидкість роботи обмежує його застосування для великих обсягів даних.

3. MD5, незважаючи на свою популярність у минулому, більше не підходить для криптографічних задач через вразливість до атак. Він може бути використаний лише для перевірки цілісності даних у некритичних середовищах.

4. ECC є перспективним методом шифрування, який поєднує високу безпеку та низькі обчислювальні витрати, однак його впровадження ускладнюється через недостатню підтримку у деяких системах.

Технології шифрування продовжують розвиватися, адаптуючись до нових викликів і загроз. Використання сучасних алгоритмів, зокрема AES, RSA та ECC, у правильних комбінаціях дає змогу забезпечити оптимальний рівень безпеки даних у корпоративних середовищах. У свою чергу, відмова від застарілих алгоритмів, таких як MD5, дозволяє уникнути ризиків, пов’язаних із вразливостями старих технологій.

Інтеграція сучасних рішень шифрування у корпоративну інфраструктуру підвищує безпеку, знижує ризики витоку конфіденційної інформації та сприяє побудові довіри до систем управління даними.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. AES encryption: how does it safeguard your data? [Електронний ресурс] Режим доступу до ресурсу: https://nordlayer.com/blog/aes-encryption/ (date of access: 01.12.2024.)
2. RSA Algorithm in Cryptography [Електронний ресурс] Режим доступу до ресурсу: https://www.splunk.com/en_us/blog/learn/rsa-algorithm-cryptography.html (date of access: 01.12.2024.)
3. What is MD5? [Електронний ресурс] Режим доступу до ресурсу: https://www.okta.com/identity-101/md5/ (date of access: 01.12.2024.)
4. What is Elliptic Curve Cryptography (ECC)? [Електронний ресурс] Режим доступу до ресурсу: https://www.ssl.com/article/what-is-elliptic-curve-cryptography-ecc/ (date of access: 01.12.2024.)

Тарнавський Андрій Ігорович – студент групи 2ПІ-23м, кафедра програмного забезпечення, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, м. Вінниця, e-mail: and1tarnavskyi@gmail.com

Tarnavskyi Andrii Ihorovych - student of group 2PI-23m, Department of Software, Faculty of Information Technology and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: and1tarnavskyi@gmail.com