УДК 004.42

П.І.Савченко
О.В.Ромаюк

РОЗРОБКА ПРОГРАМНОЇ СИСТЕМИ ДЛЯ ПОРІВНЯЛЬНОГО АНАЛІЗУ СИМЕТРИЧНИХ АЛГОРИТМІВ ШИФРУВАННЯ ДАНИХ

Вінницький національний технічний університет

Анотація

У роботі розглянуто проблему забезпечення безпеки даних шляхом використання симетричних алгоритмів шифрування. Проведено аналіз сучасних алгоритмів шифрування, таких як AES, DES, 3DES та Blowfish, а також досліджено їх продуктивність, криптостійкість і ефективність використання. На основі отриманих результатів обґрунтовано доцільність створення програмної системи для порівняльного аналізу симетричних алгоритмів шифрування та визначено її основний функціонал.

Ключові слова: шифрування, симетричні алгоритми, AES, DES, криптографія, інформаційна безпека, аналіз.

Abstract

The paper considers the problem of ensuring data security using symmetric encryption algorithms. An analysis of modern encryption algorithms such as AES, DES, 3DES, and Blowfish was conducted, along with an evaluation of their performance, security, and efficiency. Based on the obtained results, the feasibility of developing a software system for comparative analysis of symmetric encryption algorithms is substantiated, and the main functionality of the proposed system is described.

Keywords: encryption, symmetric algorithms, AES, DES, cryptography, information security, analysis.

Вступ

У теперішньому електронному просторі проблема охорони відомостей стає надзвичайно важливою. З огляду на поступ інформаційних технік, наростає число небезпек, пов'язаних із несанкціонованим проникненням до відомостей, їх зміною чи привласненням. Одним із ключових способів гарантування таємності інформації виступає застосування криптографічних методів, зокрема алгоритмів симетричного шифрування.

Симетричні засоби вирізняються застосуванням єдиного ключа як для убезпечення (шифрування), так і для відновлення (дешифрування) даних. Це надає їм перевагу у швидкості роботи та результативності під час опрацювання значних масивів даних. Однак, різні методики володіють відмінними показниками швидкості дії, стійкості до зламу та труднощів впровадження, що ускладнює процес визначення найкращого варіанту.

Отже, створення програмного комплексу для зіставлення симетричних алгоритмів є своєчасним завданням, адже воно дає змогу з'ясувати їхню дієвість та вибрати найбільш обґрунтований спосіб з огляду на специфічні вимоги експлуатації.

Аналіз сучасних симетричних алгоритмів шифрування

Застарілі техніки, як от DES (Data Encryption Standard) [1], належать до категорії найпростіших методів шифрування. Хоча цей метод у свій час набув значного поширення, його ключ, що складається з 56 бітів, вже не відповідає нинішнім вимогам щодо захищеності, тому він піддається ризику атак шляхом підбору всіх можливих комбінацій.

Сучасна альтернатива — це застосування алгоритму AES (Advanced Encryption Standard) [2], який гарантує значний ступінь захисту та працює з різними розмірами ключів (128, 192 чи 256 бітів). Завдяки своїй швидкодії та стійкості до крипто аналітичних атак, AES набув широкого вжитку у сучасних системах, призначених для убезпечення даних.

3DES являє собою модифікацію DES, у якій для зміцнення безпеки застосовується потрійне шифрування [3]. Попри це, його швидкодія суттєво поступається AES, що обмежує сфери його практичного використання.

Blowfish [4] також є відомим алгоритмом, що вирізняється високою швидкістю обробки даних та можливістю гнучко обирати довжину ключа. Проте зараз його витісняють новіші розробки.

Для глибшого вивчення було зорганізовано порівняння перелічених алгоритмів з урахуванням ключових показників.

Таблиця 1 – Порівняльна характеристика алгоритмів

Критерій	DES	3DES	AES	Blowfish
Довжина ключа	56 біт	112/168 біт	128/192/256 біт	до 446 біт
Швидкодія	висока	низька	дуже висока	висока
Криптостійкість	низька	середня	висока	висока
Сучасне використання	-	±	+	±
Загальна оцінка	30%	60%	90%	80%

Здійснений розгляд демонструє, що актуальні методики, на кшталт AES, значно випереджають старі розробки у плані надійності та швидкості опрацювання. Однак, визначення відповідного алгоритму мусить базуватися на специфічних обставинах застосування, зокрема, величині інформації, потребах у швидкості реакції та необхідному ступені збереження даних.

Опис функціоналу програмної системи

Розроблена програмна система націлена на стандартизацію процесу порівняння симетричних криптографічних алгоритмів і водночас пропонує зручний інструментарій для аналізу їхньої ефективності. Структура системи базується на компонентному підході, що гарантує гнучкість, можливість нарощування потужностей та спрощує майбутнє доповнення можливостей. Центральні елементи системи складаються з блоку взаємодії з користувачем, блоку криптографічних операцій, блоку оцінки та зіставлення показників, а також блоку фіксації отриманих даних. Блок криптографічних обчислень втілює в собі процеси шифрування та розшифрування згідно з їхніми описами. Для кожного окремого методу передбачене власне втілення, що сприяє достовірності розрахунків та можливості окремої перевірки.

Отримані показники піддаються обробці та представленню у формі табличних даних або графічних діаграм, що дає змогу особі, яка користується системою, візуально зіставити

ефективність різних алгоритмів. Підсистема даних дбає про те, щоб результати тестування були занотовані або у спеціалізованому сховищі, або у вигляді звітних документів. Це відкриває шлях для подальших досліджень, зіставлення результатів різних випробувань та застосування їх у наукових працях. Підсистема спроможння до розширення, зокрема, відкривається можливість інтеграції новітніх криптографічних технік або збагачення переліку метрик для аналізу без необхідності суттєвого перероблення початкового архітектурного плану. Розробка програмного забезпечення очікується із застосуванням передових мов програмування та спеціалізованих криптографічних збірок, що забезпечить високу швидкість роботи, надійність та відповідність сучасним вимогам захисту інформації.

Внаслідок використання цього інструментарію, користувач отримує комплексний засіб для аналізу симетричних криптографічних розробок, що дозволяє обґрунтовано обирати найбільш оптимальні рішення залежно від поставлених завдань.

Висновок

Здійснивши розгляд симетричних методів шифрування, було з’ясовано, що нинішні стратегії захисту відомостей різняться значно щодо стійкості до зламу, швидкості роботи та того, наскільки ощадливо вони використовують наявні потужності. Як приклад, старіші методи, як-от DES, більше не задовольняють актуальним критеріям захищеності, натомість, криптографічні рішення останнього покоління, зокрема AES, гарантують вищий ступінь охорони відомостей, не поступаючись при цьому у швидкості виконання операцій. Це вивчення дало змогу окреслити сильні та слабкі сторони кожного з проаналізованих механізмів, що є ключовим для прийняття зваженого рішення щодо вибору криптографічних засобів залежно від конкретних обставин їхнього впровадження. Отримані дані слугують доказом того, що застосування новітніх криптографічних підходів є виправданим у системах, де пріоритетом є водночас надійність захисту та оперативність роботи з інформацією. Обґрунтовано потребу у створенні програмного комплексу для зіставлення симетричних алгоритмів. Такий інструмент дає змогу автоматизувати оцінку їхніх параметрів та надавати результати у наочній формі. Розроблений комплекс створює сприятливі умови для проведення експериментів і може бути задіяний як у навчальному процесі, так і при створенні програмних продуктів, де необхідно забезпечити високий рівень захисту даних.

Отже, ця програмна розробка сприяє зростанню якості аналізу криптографічних схем, дає змогу робити обґрунтований вибір між ними та закладає фундамент для майбутніх наукових пошуків у сфері захисту інформації.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Advanced Encryption Standard (AES) [Електронний ресурс] – Режим доступу: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf
2. Data Encryption Standard (DES) [Електронний ресурс] – Режим доступу: https://csrc.nist.gov/publications/detail/fips/46/3/final
3. Triple Data Encryption Algorithm (3DES) [Електронний ресурс] – Режим доступу: https://csrc.nist.gov/publications/detail/sp/800-67/rev-2/final
4. Schneier B. Blowfish Encryption Algorithm [Електронний ресурс] – Режим доступу: https://www.schneier.com/academic/blowfish/

Савченко Павло Ігорович – студент групи 6Пі-22б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: suslik.suslanskiy@gmail.com

Науковий керівник: Романюк Оксана Володимирівна – доцент кафедри програмного забезпечення, Вінницький національний технічний університет, Вінниця, e-mail: romaniukoksanav@gmail.com

Savchenko Pavlo Igorovich – student of group 6PI-22b, Faculty of Information Technology and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: suslik.suslanskiy@gmail.com

Supervisor: Romaniuk Oksana Volodymyrivna – Associate Professor of the Software Department, Vinnytsia National Technical University, Vinnytsia, e-mail: romaniukoksanav@gmail.com