УДК 004.01

Мельник М.М., студент 3 курс, 111-Математика
Нескородєва Т.В., д.т.н., завідувач кафедри інформаційних технологій

РОЗРОБКА ЕКСПЕРТНОЇ СИСТЕМИ ДЛЯ ДИНАМІЧНОЇ ОПТИМІЗАЦІЇ МЕТОДІВ ШИФРУВАННЯ

Донецький національний університет імені Василя Стуса, м. Вінниця

У сучасному світі більша частина обміну інформації відбувається через глобальну мережу Інтернет. Після десятиліть прогресу і розвитку нових можливосней, сучасному, середньо-статистичному громадянину важко уявити своє життя без використання усіг цифрових благ. Основна мета переходу на новітні технології це оптимізація шляхів та часу, за якими проходять процеси у різноманітних сферах бізнесів та індустрій, та мінімізація людського фактору, надаючи перевагу точним та стабільним машитам і технологіям. Не дивно, що після цього перевороту Інтернет став невід'ємною частиною нашого життя, адже це мережа в якій можна найшвидше передати данні, в будь-яку місце призначання з будь-якої точки планети. Але якщо розглянути іншу сторону монети, а протиріччя можливостям передавати дані, мережа має бігато вразливостей, які значно спрощують процес її перехоплення.

Актуальність. Повертаючись до теми криптогріфії, яка є особливо актуальною в епоху зростаня кількості електронних пристроїв та залежності суспільства від цифрових технологій, можна сказати, що вдало підібраний метод шифрування інформації, серед великої кількості варіантів підлаштованих під певні ситуації, може значно вплинути на продуктивність та ефективність деяких процесів, в особливості тих які майже повністю побудованих на передачі даних. Криптографія відіграє важливу роль у забезпеченні кібербезпеки у багатьох сферах життя, включаючи банківську систему, мережі зв'язку, електронну пошту, онлайн-магазини, соціальні мережі та інші. Кібер злочинці постійно шукають нові способи для викрадення та зламування конфіденційної інформації. Тому враховуючи певні фактори, такі як: розмір даних, формат, важливість та рівень захисту, одною з важливих задач компанії, яка обирає яким чином забезпечити цілісність і конфіденційність своїх даних – це вибір найбільш ефективного алгоритму шифрування, який за використання найменшої кількості ресурсів забезпечував би надійний захист. Цей процес також вимагає певного аналізу та присвячення часу. Але чи доречно використовувати один алгоритм під усі специфічні задачі?

Актуальні дослідження. У 2018 році, інформаційний ресурс Joe Project Store опублікував особисте дослідження на тему: «Експертні системи у комп'ютерній системі безпеки: шифрування даних, алгоритми кодування та хешування ключів». В якій було детально описано актуальність криптографії,

важливість свідомого підходу до визначення методу шифрування, та розробка потенційної платформи для доповнення комп'ютерної безпеки.

Також проект DARPA-Brandeis за участі Доктора Джоуша Барона веде розробку програми, яка спрямована створення технічних засобів для захисту приванох та конфіденційно інформації окремих осіб та підприємств, яке б забезпечувало автоматизований, динамічний підбір методів шифрування на основі змінних умов, таких як атаки на систему, чи зміни в обсязі даних.

Мета:

- Дослідити актуальність розробки у даній галузі.
- Дослідити найбільш популярні алгоритми шифрування, та де вони використовуються.
- Побудувати експертну систему.
- Дослідити галузі та можливості інтеграції даної системи у реальні процеси.

Популярні алгоритми шифрування:

1. Алгоритм Діффі-Геллмана: Цей алгоритм шифрування допомагає забезпечити безпеку при обміні ключами між двома сторонами, що хочуть спілкуватися зашифрованими повідомленнями.

2. RSA: Це один з найбільш популярних методів шифрування, який використовується для захисту відкритих даних у мережі. RSA використовує математичну теорію чисел, щоб створити ключі шифрування.

3. Шифрування Вернама: Цей метод шифрування є одним з найбільш безпечних методів, оскільки він використовує випадкові ключі для шифрування повідомлень. Шифрування Вернама застосовується у сучасних системах електронної комерції та урядових системах.

4. Шифрування AES: AES є одним з найбільш популярних симетричних методів шифрування, який використовується для захисту даних у багатьох сучасних застосунках та системах.

5. Blowfish: криптографічний алгоритм, який реалізує блочне симетричне шифрування. Розроблений Брюсом Шнайєром в 1993 році. Являє собою шифр на основі мережі Фейстеля. Виконано на простих і швидких операціях: XOR, підстановка, додавання. Не запатентований і вільно поширюваний.

Проаналізувавши вище наведені алгоритми шифрування можна визначити, під які конкретні задачі можна їх використовувати.

Побудова експертної системи:

Визначимо параметри даних, за якими буде вестись підбір відповідного методу шифрування:

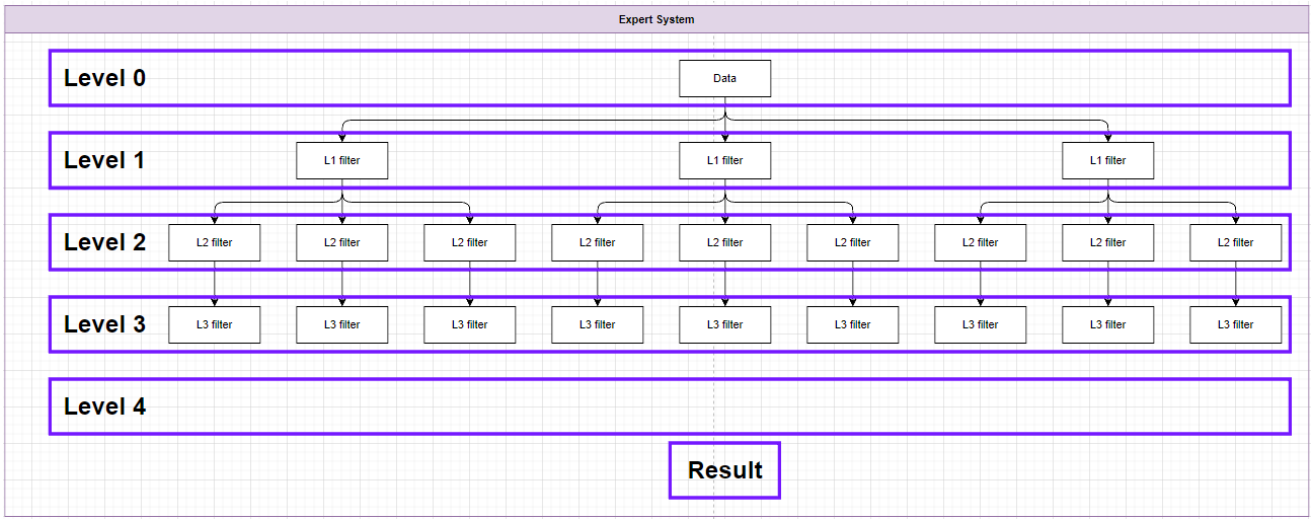
$$data: \begin{cases} [security\_level] \\ [size] \\ [format] \\ [hardware] \end{cases}$$

Також визначимо в якому вигляді буде подаватись результат аналізу експертної системи:

$$enqryption: \begin{cases} [name] \\ [key\_size] \\ [block\_size] \\ [compression] \end{cases}$$

Окрім звичайного вибору методу шифрування, експертна система буде здатна конфігурувати його більш детальними параметрами, такі як розмір ключа, який впливає на складність зашифрованого матеріалу. Розмір блоку який передається, що впливає на швидкість передачі інформації, та компресія зашифрованого об'єму даних, для зменьшення затрат ресурсів оперативної пам'яті на передачу інформації.

Алгоритм пошуку реалізується у вигляді звичайного дерева, зв'язок між гілками якого відображає певний інтервал конкретного параметру. Оскільки в системі тільки 4 параметри всього буде 5 рівнів гілок, де нульовий рівень – це ніяк не проаналізована інформація, а останній – містить коріння всіх можливих варіацій конфігурації методів шифрування. Зв'язок між рівнями відображає оцінку певного параметру даних, що приближає його до більш оптимального результату. На одному рівні гілки ніяк між собою не зв'язані.



Expert system plan

Перший рівень відповідає за фільтрацією $\{data.security_{level}\}$, Першочергово потрібно визначитись яким методом шифрування користуватись найвигідніше, та який оптимальний розмір ключа.

Другий рівень відповідає фільтрацію $\{data.hardware\}$, оцінка потужності роботи машин, допоможе визначити потрібний рівень компресії, та виставить певні ліміти на інші параметри конфігурації методу шифрування.

Третій рівень відповідає за фільтрацію $\{data.format\}$, формат визначить який розмір блоків буде найбільш вигідним, для передачі пакетів. Наприклад відео, не варто розбивати на дуже маленькі блоки, адже може виникнути втрана кадрів.

Четвертий рівень відповідає за фільтрацію $\{data.size\}$, розуміння обсягу даних які потрібно зашифрувати, надасть можливість точно підібрати оптимальний розмір блоків.

Висновок. Отже, розроблена експерта система може набути широкого використання у різних комунікаційних сервісах, в яких переважно йде обмін різними форматами даних. Або у закритих середовищах та системах, в яких відбувається внутрішній обмін конфіденціальної інформації. Вона може бути інтегрована як один із засобів розробки, або виступати у ролі самостійного хмарного сервісу, який би підключався до вже існуючого трафіку інформації. Також система відкрити до розширення у двух різних напрямках: кількість рівнів фільтрації та різноманітність параметрів методу шифрування, які б налаштовували його роботу більш точно.

Список літератури:

1 *Офіційний сайт проекту Darpa: https://www.darpa.mil/staff/dr-joshua-baron*
2 *Галузі застосування Darpa: https://www.darpa.mil/work-with-us/ai-forward*
3 *Наукове дослідження експертних систем по криптографії редакції Iproject: https://iproject.com.ng/project-material/expert-system-for-computer-security-data-encryption-decryption-and-key-hash-algorithms/index.html*
4 *Наукове дослідження експертних систем по криптографії редакції newprojecttopics: https://newprojecttopics.com.ng/expert-system-computer-security*
5 *Нескородєва Т., Федоров Є., Січко Т., Нескородєва А. Експертні та рекомендаційні системи: навч. посіб. для здобувачів вищої освіти спеціальностей 122 «Комп'ютерні науки», 125 «Кібербезпека», 113 «Прикладна математика» / Т. В. Нескородєва, Є. Є. Федоров, Т.В. Січко, Нескородєва А.Р. Вінниця: ДонНУ імені Василя Стуса, 2022. 208 с.*

УДК 004.056

Радзіховська А.О., студентка 3 курсу спеціальності 122 «Комп'ютерні науки»
Нескородєва Т. В., д.т.н., завідувачка кафедри інформаційних технологій

ВІЗУАЛІЗАЦІЯ ДАНИХ У МОВІ R

Донецький національний університет імені Василя Стуса, м. Вінниця

R — мова програмування і програмне середовище для статистичних обчислень, аналізу та зображення даних в графічному вигляді. Вона була