УДК 004.056.55

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ КРИПТОГРАФІЧНОЇ СИСТЕМИ НА ОСНОВІ МЕРЕЖІ ФЕЙСТЕЛЯ В ЛЕГКІЙ ПРОМИСЛОВОСТІ

Студ. Сулима Д. О., гр. МгІТ-2-18,
Науковий керівник доц. Резанова В. Г.
Київський національний університет технологій та дизайну

Мета і завдання. Метою дослідження є створення криптографічної системи на основі мережі Фейстеля для забезпечення безпеки конфіденційних даних легкої промисловості. Завданням дослідження є спроектувати та реалізувати у вигляді додатку для ПК криптографічної системи на основі мережі Фейстеля.

Об'єкт та предмет дослідження Об'єктом дослідження є забезпечення безпеки важливої інформації легкої промисловості, наприклад, ескізів нового спецодягу. Предметом дослідження є структура та реалізація криптографічної системи.

Результати дослідження. Криптографічна система представляє собою сервіс, що надає користувачу можливість зашифровувати або розшифровувати інформацію, для подальшої передачі в комп'ютерних мережах або для безпечного зберігання на жорсткому диску. Вона повинна бути представлена у вигляді віконного застосування з інтуїтивно зрозумілим інтерфейсом, щоб системою могли користуватись звичайні користувачі. Криптографічна система представлена у вигляді декількох візуальних форм, які дозволяють виконувати спеціальні функції, зокрема: генерація паролю з заданою кількістю символів (до 32 символів); перегляд та вибір файлу на жорсткому диску користувача; перегляд інформації про файл; введення паролю користувачем; можливість сховати символи паролю; перегляд зашифрованих або розшифрованих файлів в визначених каталогах.

Для шифрування та розшифрування був обраний алгоритм на основі мережі Фейстеля, оскільки він є блоковий та з використанням симетричного ключа, тобто під час роботи дані, які необхідно зашифрувати розбиваються на блоки однакової довжини та шифруються або розшифруються одним й тим же ключем. Під мережою Фейстеля (Feistel network) мається на увазі розбиття опрацьовуваного блока даних на кілька субблоків (частіше всього-2), один з котрих опрацьовується деякою функцією f та накладається на 1 чи декілька інших субблоків) R разів (раундів), як зображено на рисунку 1. Ще однією перевагою при використанні цього методу шифрування є велика кількість досліджень як при розробці алгоритма, так і при його аналізі.

Накладання опрацьованого субблока на неопрацьований частіше за все виконується за допомогою логічної операції «виключне АБО» (Exclusive OR,XOR), як показано на рисунку 1. Достатньо часто замість XOR тут використовується додавання за модулем 2, де n-розмір субблока в бітах. Після накладання, субблоки міняються місцями, тобто в наступному раунді алгоритма опрацьовується вже інший субблок даних.

Така структура алгоритмів шифрування отримала свою назву в честь Хорста Фейстеля (Horst Feistel) - одного з розробників алгоритма шифрування Lucifer та розробленого на основі алгоритма DES (Data Encryption Standart) -колишнього (але до сих пір широко використовуваного) стандарту шифрування США.

Оскільки процес шифрування або розшифрування може займати багато часу, то необхідно обрати мову програмування, яка підтримує парадигму ООП та дозволяє проводити низькорівневу оптимізацію. Тому для реалізації було обрано мову програмування C++ та середовище розробки Borland C++ Builder.

Для реалізації графічного інтерфейсу зручно використовувати VCL - об'єктно-орієнтовану бібліотеку для розробки програмного забезпечення, яка розроблена компанією «Borland» для підтримки принципів візуального програмування.

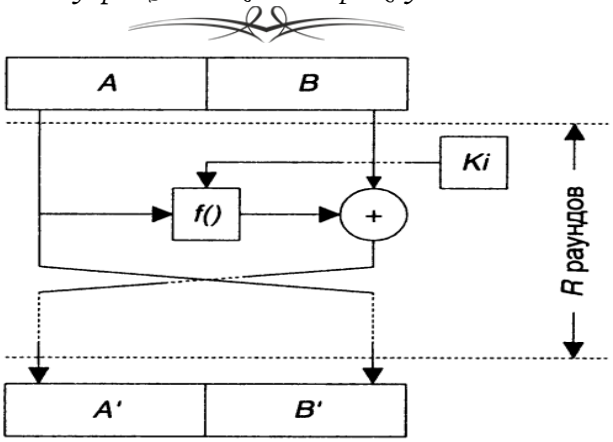

Рисунок 1 - Мережа Фейстеля

Також необхідно передбачити підсистему генерації пароля, в якій можна задавати довжину та набір символів пароля. Рекомендовано використовувати довжину в 16 символів, тому що в більшості комп'ютерних систем один символ займає 1 байт (8 біт), отже пароль в 16 символів = 8 * 16 = 128 біт, яких достатньо для забезпечення необхідного рівня криптостійкості (на поточному рівні обладнання).

Загальний алгоритм виконання програми полягає в тому, що на вхід програми подається файл, який аналізується для виведення метаданих. Потім необхідно вказати пароль, який буде використовуватись як ключ для алгоритму шифрування. Якщо довжина паролю менше 16 символів то він буде розширений до 16 символів. Необхідно підтвердити дії. Система перевіряє розширення файла, якщо розширення не ".LOL", то файл буде переданий в функцію шифрування, в іншому випадку в функцію розшифрування. Користувачу повідомляється про початок процесу. Коли процес шифрування або розшифрування закінчився, вихідному файлу присвоюється відповідне ім'я, та зберігається в відповідний каталог з назвами «Зашифровані файли», «Розшифровані файли». Користувач може натиснути кнопку «Показати в каталозі», щоб отримати швидкий доступ до файла.

Висновки. Алгоритми на основі мережі Фейстеля можуть бути сконструйовані таким чином, що для шифрування та розшифрування може використовуватись один й той же код алгоритму-різниця між цими операціями може бути лише в порядку застосування ключів

Така властивість алгоритма найбільш корисна при його апаратній реалізації або на платформах з обмеженими ресурсами; в якості прикладу такого алгоритма можна навести «Магма» як частину стандарта ГОСТ Р 34.12-2015;

Алгоритми на основі мережі Фейстеля є найбільш вивченими-таким алгоритмам посвячена дуже велика кількість криптографічних досліджень, що є беззаперечною перевагою як при розробці алгоритма, так і при його аналізі.

Розроблена система має простий, зрозумілий інтерфейс. Вона надає користувачу можливість зашифрувати або розшифрувати файли без зайвих зусиль, виконавши прості дії.

Ключові слова: криптографічна система, алгоритми шифрування, мережа Фейстеля, симетричні алгоритми шифрування, блокові алгоритми шифрування, безпека даних.

ЛІТЕРАТУРА

1. Encryption [Electronic resource] / en.wikipedia.org. – 2017. – Mode of access : https://en.wikipedia.org/wiki/Encryption.
2. ГОСТ 28147-89 [Electronic resource] / en.wikipedia.org. – 2017. – Mode of access : https://ru.wikipedia.org/wiki/%D0%93%D0%9E%D0%A1%D0%A2_28147-89.
3. Захист інформаційних ресурсів / Василь Франчук. - К.:Редакції газет природничо-математичного циклу, 2012. - 112 с. - (Бібліотека «Шкільного світу»).
4. Панасенко С. Алгоритмы шифрования. Специальный справочник / Панасенко С. – Санкт-Петербург: «БХВ-Петербург», 2009 – 531 с.
5. Смарт Н. Криптография / Смарт Н. – Москва : «Техносфера», 2005. – 524 с.