СУЛИМА Д. О., РЕЗАНОВА В. Г.

АЛГОРИТМІЧНЕ ТА ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ КРИПТОГРАФІЧНОЇ СИСТЕМИ НА ОСНОВІ МЕРЕЖІ ФЕЙСТЕЛЯ В ЛЕГКІЙ ПРОМИСЛОВОСТІ

SULYMA D.A., REZANOVA V.G.

ALGORITHMS AND SOFTWARE OF CRYPTOGRAPHIC SYSTEM BASED ON THE FEISTEL NETWORK IN LIGHT INDUSTRY

The cryptographic system is a service that enables the user to encrypt or decrypt information for further transmission on computer networks or for secure storage on a hard disk. It should be presented in the form of a window application with an intuitive interface so that the system can be used by ordinary users.

For encryption and decryption, an algorithm based on the Feistel network was chosen, since it is block and using a symmetric key, that is, during operation, the data that needs to be encrypted is split into blocks of the same length and encrypted or decrypted with the same key.

The structure of the encryption algorithms was named after Horst Feistel, one of the developers of the Lucifer encryption algorithm and developed on the basis of the DES (Data Encryption Standart) algorithm, the former (but still widely used) US encryption standard. Among other algorithms based on the Feistel network, one can give an example: the domestic standard of encryption GOST 28147-89 (and more modern GOST R 34.12-2015), as well as other known algorithms: RC5, BlowFish, TEA, CAST-128.

Вступ

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.

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.

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. Серед інших алгоритмів, заснованих на мережі Фейстеля, можна навести приклад: вітчизняний стандарт шифрування ГОСТ 28147-89 (та більш сучасний ГОСТ Р 34.12-2015) , а також інші відомі алгоритми: RC5, BlowFish, TEA, CAST-128.

Постановка завдання

Основною метою дослідницького проекту є розробка алгоритмічного та програмного забезпечення для зашифровування або розшифровування

інформації, для подальшої передачі в комп'ютерних мережах або для безпечного зберігання.

Основними функціональними точками продукту мають стати:

1. Генерація паролю з заданою кількістю символів (до 32 символів);
2. Перегляд та вибір файлу на жорсткому диску користувача;
3. Перегляд інформації про файл;
4. Введення паролю користувачем;
5. Можливість сховати символи паролю;
6. Перегляд зашифровани або розшифрованих файлів в визначених каталогах.

Об'єктом дослідження є забезпечення безпеки важливої інформації легкої промисловості, наприклад, ескізів нового спецодягу.

Основна частина

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.

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.

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).

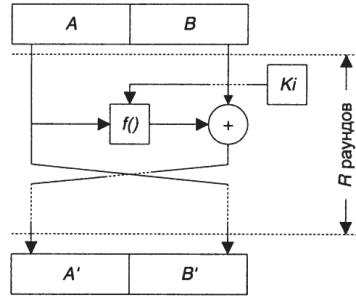

Рисунок 1 - Мережа Фейстеля

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.

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. Панасенко С. Алгоритмы шифрования. Специальный справочник / Панасенко С. – Санкт-Петербург: «БХВ-Петербург», 2009 – 531 с.

ДВОРЯК М. В., ДЕМКІВСЬКА Т. І.

РОЗРОБКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ ПРОГНОЗУВАННЯ ПОКАЗНИКІВ ДІЯЛЬНОСТІ СТРАХОВОЇ КОМПАНІЇ

DVORIAKP. V., DEMKIVSKA T. I.

SOFWTWARE DEVELOPMENT FOR FORECASTING INDEXES OF INSURANCE COMPANIES

Annotation – A large number of calculations, calculations, predictions are mostly processed in tabular editors, such as Excel, for which certain skills and knowledge are needed. And the user can easily commit an error when using a table editor. Normally, it's not easy to work in a spreadsheet editor with a lot of input data. The aim of the work is to simplify the simulation of processes and determine the best model, implement a friendly interface. At the same time, implement integration of software with popular table editors. Implement support for importing and exporting data to popular formats (.xlsx, .csv). Use a relational database to implement the authentication and authorization function of the user, as well as to save the result of the calculation for subsequent viewing or export.

This application should solve part of the listed needs. The solution must be built in advance to target several platforms, including web applications. This will allow you to cover the maximum number of users who may be interested in the product.

Keywords:personal data manager, forecasting, insurance indexes, software

Вступ

Велика кількість розрахунків, калькуляцій, прогнозувань здебільшого опрацьовується в табличних редакторах, наприклад Excel, для використання яких потрібні певні вміння та знання. А також користувач може легко допустити помилку при користуванні табличним редактором. Зазвичай це не просто, працювати в табличному редакторі з великою кількістю вхідних даних. Ціль роботи максимально спростити моделювання процесів та визначення кращої моделі, реалізувати дружній інтерфейс. В той самий час реалізувати інтеграцію програмного забезпечення із популярними табличними редакторами. Даний додаток має вирішити частину перерахованих потреб. Рішення має бути