УДК 004.056.55

РОЗРОБКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ ШИФРУВАННЯ ПЕРСОНАЛЬНИХ/КОРПОРАТИВНИХ ДАНИХ

Студ. М.В.Курлов, гр. МгІТ-2-18
Науковий керівник доцент Т.І. Демківська
Київський національний університет технологій та дизайну

Мета і завдання. Метою даного дослідження є розробка додатку для гарантування безпеки даних користувача для подальшої роботи з сервісами, шо потребують авторизації. Завданням дослідження є порівняння та вибір підходів гарантування безпеки даних, що підвищує захист облікових записів та подальшого їх використання. У дослідженні використано метод шифрування AES для збереження персональних даних користувача. Дослідження проводиться з метою покращення безпеки в повсякденній роботі користувача. Додатковими можливостями мають бути: аутентифікація та авторизація користувача, можливість редагування та видалення даних.

Об'єкт та предмет дослідження. Предметом дослідження є технології збереження даних користувача, алгоритми шифрування. Об'єктом дослідження є методи забезпечення захисту даних.

Результати дослідження. Дуже важливою частиною будь-якого проекту є безпека даних. Безпека даних включає в себе організаційну та інформаційну частини. Організаційна частина відповідає за те, щоб користувача наперед проінструктували щодо правил безпеки на підприємстві, при роботі з комп'ютером тощо. Під інформаційною безпекою розуміється захищеність даних в комп'ютерній системі, тобто технічна реалізація методів захисту.

На сьогодення все гостріше стає питання безпеки даних. Зазвичай користувач використовує для запису своїх даних авторизації, банківських карток та іншого або папір або використовуючи електронні таблиці Excel, текстові редактори Word або Блокнот, що не є дуже надійним, бо дані зберігаються у відкритому вигляді. Відображення даних при такому їх зберіганні знижує надійність і робить не зручним їх зберігання та пошук. Дані можуть бути розташовані у різних файлах, пошук необхідних даних може зайняти багато часу. У будь-якому випадку, додаток, який централізує та захищає дані, буде корисним і полегшить роботу користувачів при роботі в мережі інтернет і не тільки.

Додаток розрахований для невеликих підприємств з використанням спільних аккаунтів, також для користувачів у яких багато банківських карток, персональних аккаунтів від різноманітних ресурсів, соціальних мереж тощо. Користувач реєструється на будь-якому ресурсі, за допомогою менеджера паролів генерується надійний пароль. На кожного окремого користувача формується окремі налаштування, а також окремий каталог, і ці дані не доступні для перегляду між обліковими записами. Існуючі додатки для шифрування персональних даних здебільшого використовують застарілі алгоритми, відсутні альтернативних способів автентифікації користувача окрім майстер-ключа. Мета даного програмного додатку поєднати виявлені переваги та позбавити зазначених недоліків.

Додатковими можливостями продукту можуть бути різноманітні інтеграції: із платіжними системами і банкінгами або соціальними мережами.

Серед засобів реалізації було обрано наступний стек технологій, мов програмування та алгоритмів: .Net Core, C#, AES.

Advanced Encryption Standard (AES), також відомий як Rijndael (Рендалл) - симетричний алгоритм блочного шифрування (розмір блоку 128 біт, ключ 128/192/256 біт). Для ключа 128 біт алгоритм має 10 раундів у яких послідовно виконуються операції(Рис.1):

- subBytes() - нелінійна заміна байтів використовуючи таблицю замін(S-box)
- shiftRows() - працює з рядками таблиці State, циклічно зсуваються на r байтів по горизонталі, залежно від номера рядка
- mixcolumns() (у 10-му раунді пропускається) - чотири байти кожної колонки State змішуються, використовуючи для цього зворотну лінійну трансформацію
- AddRoundKey() - кожен байт стану об'єднується з RoundKey використовуючи операцію XOR

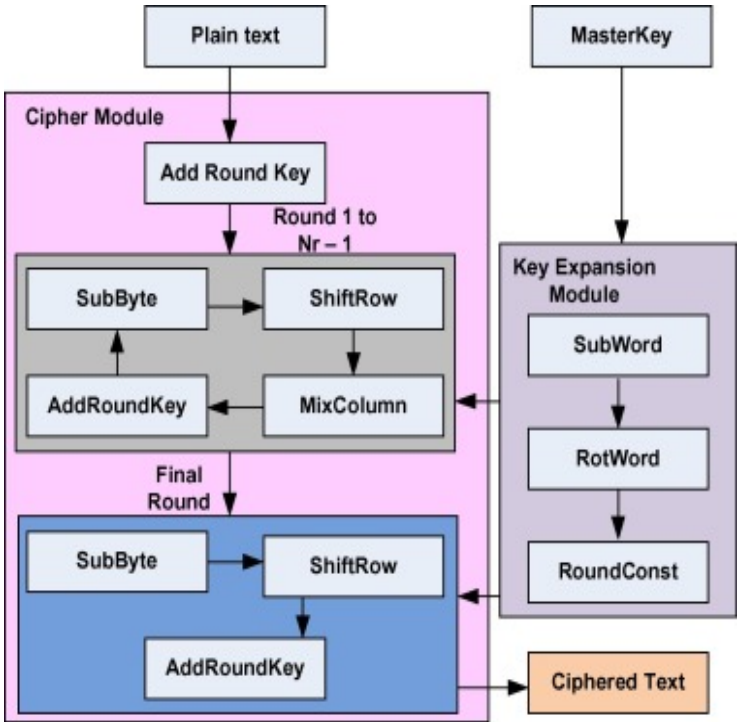

Рис.1 Алгоритм шифрування AES

Задачі що має вирішувати додаток є наступними:

1. шифрування персональних даних авторизації;
2. авторизація по PIN-коду;
3. розширена captcha;
4. авторизація за допомогою фізичного носія;
5. підтримка багатьох користувачів;
6. додавання\зміна існуючих\видалення даних;
7. можливість бекапу на зовнішній носій;
8. генерація випадкових паролів.

Використання даного програмного продукту дозволяє користувачам генерувати унікальний пароль для кожного ресурсу окремо та надійно зберігати їх. Користувачі можуть також зберігати в додатку банківські картки і додаток сам нагадає про перевипуск її, коли виходить строк дії. Також даний додаток виконує функцію шифрування та архівування файлів з важливою інформацію використовуючи оптимальний алгоритм.

Висновки. Розроблено програмне забезпечення, яке призначене для безпечного збереження та використання персональних даних. Розроблено додаток, який побудований на сучасних технологіях і має простий та зрозумілий інтерфейс задля створення більш цілісного користувацького досвіду.

Ключові слова. Менеджер персональних даних, криптографія, захист персональних даних, корпоративний захист, безпека даних.

ЛІТЕРАТУРА

1. Advanced Encryption Standard (AES) [Electronic resource] / en.wikipedia.org. 2017. – Rijndael: https://uk.wikipedia.org/wiki/Advanced_Encryption_Standard.
2. Andrew Troelsen - Pro C# 7 With .NET and .NET Core, 2017
3. Wenbo Mao - Modern Cryptography: Theory and Practice, 2004
4. AES Round 1 Information. // http://csrc.nist.gov — January 26, 2001.