УДК 004.

Северина Ю.А., спеціаліст, Скрипник І.А., к.ф-м.н., доцент , науковий керівник

ПРАКТИЧНА РЕАЛІЗАЦІЯ ФОРМАЛЬНИХ МЕТОДІВ РОЗРОБКИ КРИПТОГРАФІЧНИХ ПРОТОКОЛІВ

Запорізька державна інженерна академія, кафедра ПЗАС

Сучасний світ – це світ інформаційного прогресу. Неможливо уявити навіть одного дня без, таких звичних для нас, смартфонів, планшетів, комп'ютерів та інших сучасних пристроїв. Всесвітня мережа Інтернет охопила майже весь світ і стала доступною та звичайною для кожного з нас. Багато хто має профілі в соціальних мережах та активно користується інтернет – банкінгом. А чи є наші дії у всесвітній мережі безпечними для нас? Чи безпечними є Інтернет – банки? Чи можуть гарантувати соціальні мережі конфіденційність нашого спілкування? Відповіді на ці питання не завжди задовільні. Вирішенням проблем захисту інформації займається наука криптографія [1,2].

Метою дипломної роботи є реалізація роботи криптографічних протоколів та покрокова демонстрація роботи кожного з протоколів.

Дипломна робота реалізована у вигляді чату. Тобто, система має два застосунки: клієнт та сервер. Спроектовано два автомати-препроцесори Мура: для клієнтської частини та для серверної. Мають бути реалізовані та сформовані в окремі бібліотеки криптографічні алгоритми шифрування такі, як DES та RSA. На клієнтській частині застосунку має відображатися покрокова робота обраного протоколу.

Чат може використовуватися користувачами для спілкування, яке буде безпечним у мережі. А, також, може використовуватися викладачами та вчителями для наочної демонстрації роботи протоколів. Учні та студенти можуть самостійно використовувати програму під час вивчення криптографічних протоколів.

Протокол – це послідовність чітко визначених дій, які виконуються двома або більшою кількістю учасників. Криптографічний протокол – це протокол, який використовує криптографію. В дипломній роботі реалізовано такі види криптографічних протоколів:

- авторизації, реєстрації;
- протокол аутентифікації Нідхема – Шрьодера;
- протокол ідентифікації Фіата – Шаміра;
- гібридний протокол шифрування даних;
- шифрування даних на основі електронно-цифрового підпису (ЕЦП).

В роботі криптографічних протоколів використовуються такі криптографічні алгоритми шифрування, як DES та RSA. DES є блочним алгоритмом шифрування з довжиною блоку 64 біта та симетричними ключами довжиною 56 біт. На практиці зазвичай ключ має довжину 64 біти, де кожен 8 біт використовується для контролю парності інших бітів ключа. Серед недоліків DES виділяють: наявність слабких ключів, невелика довжина ключа, надлишковість ключа, що обумовлена контролем парності для кожного окремого байта ключа. RSA – це алгоритм, де ефективно реалізована одностороння функція з секретом. Стійкість RSA базується на складності факторизації великих простих цілих чисел, а, також, залежить від складності обернення односторонніх функцій.

Для протоколів авторизації/реєстрації було використано алгоритм Хаффмена для побудови криптограм. Протокол Нідхема – Шрьодера використовує алгоритм RSA у своїй роботі, як і протокол Фіата – Шаміра. В роботі гібридного протоколу шифрування задіяні два криптографічні алгоритми - DES та RSA. При шифруванні даних на основі ЕЦП використовується тільки алгоритм RSA.

На клієнтській стороні застосунку користувач має змогу відстежувати роботу криптографічних протоколів покроково.

Існує декілька видів формального представлення криптографічних протоколів. Одним з них є представлення протоколів у вигляді автоматів. Тобто, вхідним алфавітом такого автомату будуть служити відкриті або зашифровані дані, в залежності від кроку та протоколу. Станами такого автомату-препроцесору будуть назви функції, що мають виконатися на цьому етапі роботи протоколу. Даний формальний метод представлення роботи протоколів є ефективним та зручним. Автомат-препроцесор передбачає тільки ті дії, що є правильними, всі інші дії, що не передбачені протоколом, характеризуються як помилка. Якщо зловмисник змінив деякі дані, для власної користі, то автомат їх відкине та завершить роботу протоколу, попередивши учасників про вторгнення. Формальне представлення протоколу у вигляді автомату є зручним. Автомат представляється найчастіше або у вигляді таблиці переходів, або у вигляді діаграми станів. Ці способи наочно демонструють кроки роботи протоколу.

Для дипломної роботи було спроектовано два автомати, що мають працювати на клієнтській та серверній частиніх [3,4]. Автомати вийшли об'ємними, тому зберігати їх у вигляді таблиці або діаграми станів не є доцільним. Було прийнято рішення зберігати автомат у вигляді списку переходів для кожного стану.

Проект був реалізований у середовищі розробки *Microsoft Visual Studio*, яке є дуже зручним у використанні та надає багато можливостей для роботи. Програмною платформою стала *Microsoft .NET*, мова реалізації C# з використанням технології WPF. Технологія WPF надає своїм користувачам можливість реалізації власного неповторного дизайну застосунку. Мова програмування C# є однією з мов програмування, сумісних з технологією WPF. C# надає можливості швидко та зручно реалізовувати поставлені задачі, за допомогою своїх засобів.

Серверна частина представляє застосунок, що прослуховує вхідні з'єднання від клієнтів, а також надає можливість адміністратору відслідковувати роботу серверу та клієнтів, продивляючись Log-файл.

Клієнтська частина представляє собою застосунок, що має привабливий та зручний інтерфейс, надає можливість користувачу зареєструватися та авторизуватися у системі. Авторизований користувач отримує змогу обрати співрозмовника з переліку всіх авторизованих на даний момент користувачів, обрати протоколи, що будуть виконуватися та надіслати повідомлення.

Висновки:

- Було досліджено роботу криптографічних протоколів та криптографічних алгоритмів, таких, як DES та RSA. Приведені криптографічні алгоритми були реалізовані та сформовані в бібліотеки.
- Були спроектовані автомати-препроцесори Мура для клієнтської та серверної частини. Було реалізовано автомат-препроцесори та сформовано в бібліотеку для подальшого використання.
- Було реалізовано два застосунки: клієнт та сервер. На стороні клієнта та на стороні сервера були реалізовані функції, що є станами автомату та функції, що виконують дії криптографічних протоколів.
- По завершенню реалізації було проведено тестування, виявлені та виправлені всі помилки.

Література

1. Шнейер Б. Прикладная криптография / Брюс Шнейер., 2002. – 816 с.
2. Баричев С. Г. Основы современной криптографии: Учебное пособие / С. Г. Баричев, Р. Е. Серов., 2002.
3. Биркгоф Г. Современная прикладная алгебра / Г. Биркгоф, Т. Барти., 1976
4. Льюис Ф. Теоретические основы проектирования компиляторов. / Ф. Льюис, Д. Розенкранц, Р. Стирнз., 1979.