Гутич І. І., магістрант,
спеціальність «Комп'ютерна інженерія»
Гапак О. М., доцент кафедри комп'ютерних систем та мереж
Ужгородський національний університет

СИСТЕМА ДЛЯ ГЕНЕРУВАННЯ ТА АНАЛІЗУ КРИПТОГРАФІЧНИХ ПРОТОКОЛІВ

З кожним роком в сучасному світі підвищується рівень ролі інформації, яка починає займати все більш вагоме значення у функціонуванні державних і суспільних інститутів та житті кожної людини.

В умовах сучасного світу формується новий вид трудової діяльності, пов'язаний із здобуттям, поширенням і зберіганням інформації. Паралельно з цим катастрофічно зростає ціна втрат в разі виникнення помилок у функціонуванні або зниження надійності систем обробки і передачі інформації. З підвищенням цінності інформації та її ролі в суспільстві, відповідно зростає і важливість її захисту.

При обміні інформацією між учасниками часто виникає ситуація, коли інформація не є конфіденційною, але важливий факт надходження повідомлень в неспотвореному вигляді, тобто наявність гарантії, що ніхто зможете не підробити повідомлення. Така гарантія називається забезпеченням цілісності інформації і також є одним із завдань криптографії.

Серед всього спектру методів захисту інформації особливе місце займають саме криптографічні методи. Криптографічний захист завжди був найбільш ефективним напрямом захисту персональних конфіденційних даних користувачів, який залежить від вибору алгоритму шифрування та методу управління криптографічними ключами.

При побудові криптографічних систем необхідно вирішувати багато питань безпечного інформаційного обміну, наприклад:

- чи дійсно повідомлення прийшло від конкретного відправника;
- чи не було воно підмінене або сфабриковано ким-небудь іншим;
- чи було повідомлення створено даними відправником, або він просто переслав чиєсь повідомлення;
- чи не є повідомлення (наприклад, про оплату будь-якого товару) повторно відправленим;
- і так далі.

Усі ці та подібні питання належать до галузі досліджень, що отримала назву протоколи забезпечення безпеки [1; 2].

З огляду на це, дослідження криптографічних протоколів захисту інформації є актуальною задачею.

Метою роботи є розробка програмного засобу для генерування та аналізу криптографічних протоколів.

Встановлена мета обумовлює наступні завдання:

- генерування криптографічних протоколів на основі вибраних налаштувань;
- реалізації програмної системи оцінки криптографічних протоколів;
- моделювання роботи генерованого криптографічного протоколу.

Дану систему можна використовувати в навчальних цілях, для кращого розуміння принципів роботи криптографічних протоколів.

Таким чином, широке використання і постійне збільшення об'єму інформаційних потоків викликає постійне зростання інтересу до криптографічних протоколів.

В сучасному світі кваліфікований ІТ-фахівець повинен володіти основами інформаційної безпеки, знати в цій області нормативну базу, вміти аналізувати і оцінювати загрози інформаційної безпеки, мати досвід застосування сучасних методів і засобів захисту інформаційних систем.

Проблему аналізу і оцінки криптографічних протоколів допомагає вирішити дана система. Вона легка в розширенні і може в майбутньому бути використана для дослідження нових криптографічних протоколів.

Список використаних джерел

1. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке / Шнайер Б. – Москва : ТРИУМФ, 2002.
2. Деднев М.А. Защита информации в банковском деле и электронном бизнесе. / Деднев М.А., Дильнов Д.В., Иванов М.А. – Москва : КУДИЦ- ОБРАЗ, 2004.