УДК 004

І.С. ДЕРЕЖЕНЕЦЬ, ***О.М. МАЛИХ***, доцент

Алгоритмічна і програмна реалізація симетричної криптографічної системи із закритим ключем

Дана бакалаврська робота присвячена криптографії. Формально криптографія (з грецької - «тайнопис») визначається як наука, що забезпечує секретність повідомлення. І якщо раніше криптографія здебільшого служила виключно державним інтересам, то з приходом інтернету її методи стали надбанням приватних осіб і широко використовуються хакерами, борцями за свободу інформації та будь-якими особами, які бажають в тій чи іншій мірі зашифрувати свої дані в мережі. Серед усього спектру методів захисту даних від небажаного доступу особливе місце займають криптографічні методи. На відміну від інших методів, вони спираються лише на властивості самої інформації і не використовують властивості її матеріальних носіїв, особливості вузлів її обробки, передачі та зберігання.

В даний час особливо актуальною стала оцінка вже використовуваних криптоалгоритмов. Завдання визначення ефективності засобів захисту найчастіш більш трудомістке, ніж їх розробка, вимагає наявності спеціальних знань і, як правило, більш високої кваліфікації, ніж задача розробки.

Мета даної роботи полягає в огляді криптографічних систем захисту даних, алгоритмічної та програмної реалізації алгоритму шифрування. Для реалізації обраний симетричний алгоритм DES із закритим ключем.

Шифрування з закритим ключем засновано на тому, що доступ до ключа має тільки авторизований персонал. Цей ключ повинен триматися в секреті. Якщо ключ буде розкритий, стороння людина зможе отримати несанкціонований доступ до зашифрованої інформації.

Надійність такого шифрування залежить від декількох факторів. По-перше, алгоритм шифрування повинен бути досить складним, щоб неможливо було розшифрувати повідомлення за наявності лише шифрованого тексту. По-друге, основним фактором надійності традиційного шифрування є таємність ключа, в той час як сам алгоритм може бути і несекретним. Тому передбачається, що повинна бути забезпечена практична неможливість розшифровки повідомлення на основі знання шифрованого тексту, навіть якщо людині відомий алгоритм шифрування/дешифрування. Іншими словами не потрібно забезпечувати секретність алгоритму - достатньо забезпечити секретність ключа.

Саме ця особливість схеми традиційного шифрування обумовлює її широку популярність і визнання. Відсутність необхідності зберігати в секреті

алгоритм дає виробникам можливість реалізувати алгоритми шифрування даних у вигляді дешевих загальнодоступних мікросхем, якими оснащені сьогодні багато сучасних систем.

Найбільш широко використовуваним алгоритмом із закритим ключем є стандарт Data Encryption Standard (DES). Цей алгоритм, розроблений компанією IBM в сімдесятих роках минулого століття, прийнятий як американський стандарт для комерційних і несекретних урядових комунікацій

Типові області застосування DES:

- шифрування аудіо і відео даних для кабельного телебачення, відеоконференцій, дистанційного навчання, VoIP
- захист комерційної та фінансової інформації, що відображає кон'юнктурні коливання
- лінії зв'язку через модем, роутер або ATM лінію, GSM технологію
- смарт-карти
- загальнодоступний пакет конфіденційної версії електронної пошти PGP і в OpenPGP

Алгоритм DES широко застосовується для захисту фінансової інформації: так, один з модулів повністю підтримує операції TripleDES для емісії та обробки кредитних карт VISA, EuroPay та інших карт.

Дана робота складається з п'яти розділів.

Перша глава присвячена огляду криптографії в цілому, принципам роботи криптосистем, огляду і порівнянню сучасних криптографічних систем захисту даних, таким як симетричні і асиметричні методології шифрування, хеш-функції, механізми аутентифікації, електронні підписи і тимчасові мітки.

Друга глава присвячена алгоритмичному опису симетричного алгоритму шифрування DES, в ній докладно описані всі етапи шифрування за даною схемою.

Третя глава містить опис програмної реалізації криптосистеми DES. Тут вказані особливості мови C# і середовища програмування Microsoft Visual Studio, обраних для реалізації програми, а також нюанси структури розробленого програмного продукту.

Четверта і п'ята глави присвячені розрахунку економічного обґрунтування, охороні праці та навколишнього середовища відповідно.

Список літератури:

1. Столлингс В. Криптография и защита сетей. – К.: Вильямс, 2001. – 56 с.

2. Жельников В. Криптография от папируса до компьютера. – М.: ABF, 1996. – 335 с. .