УДК 004.056:681.5.04

Хоменко Ж.М., канд. техн. наук. старш. викладач,
Домбровський Є.М., магістрант
Державний університет «Житомирська політехніка»

ПІДСИСТЕМА ЗАБЕЗПЕЧЕНЯ БЕЗПЕКИ У СИСТЕМІ УПРАВЛІННЯ РОЗУМНИМ БУДИНКОМ (СИСТЕМИ ШИФРУВАННЯ)

Розумний будинок – житловий будинок сучасного типу, організований для проживання людей за допомогою автоматизації і високотехнологічних пристроїв. Під «Розумним» будинком слід розуміти систему, яка забезпечує безпеку та ресурсозбереження (в тому числі і комфорт) для всіх користувачів. У найпростішому випадку вона повинна вміти розпізнавати конкретні ситуації, що відбуваються в будинку, і відповідним чином на них реагувати: одна з систем може управляти поведінкою інших по заздалегідь виробленим алгоритмам. Крім того, від автоматизації декількох підсистем забезпечується синергетичний ефект для всього комплексу.

Робота присвячена розробці системи управління розумним будинком, що включає в себе контроль над усіма параметрами, а саме: освітлення, температура, вологість; і підсистеми для безпечної передачі даних на основі PKI. Велика увага приділяється на алгоритми шифрування, такі як: RSA, AES, DES (Triple DES), еліптичні криві, Base64; і схеми захисту: симетричні, з відкритим ключем, PKI. Проведена порівняльна характеристика вищевказаних алгоритмів, визначено їх недоліки та сфери застосування. Розроблений модуль безпечної передачі даних може бути використаний в будь-якому клієнт-серверному додатку, забезпечуючи таким чином високу надійність.

Система управління являє собою сукупність апаратних та програмних засобів, які насамперед націлені на економічність, тобто на зниження можливих розходів (електроенергія, тепло) користувача, а також надає додаткові можливості, наприклад, контроль присутності.

Симетричне шифрування передбачає використання одного і того ж ключа і для зашифрування, і для розшифрування. До симетричних алгоритмах застосовуються дві основні вимоги: повна втрата всіх статистичних закономірностей в об'єкті шифрування і відсутність лінійності. Прийнято розділяти симетричні системи на блокові і потокові. У блокових системах відбувається розбиття вихідних даних на блоки з подальшим перетворенням за допомогою ключа.

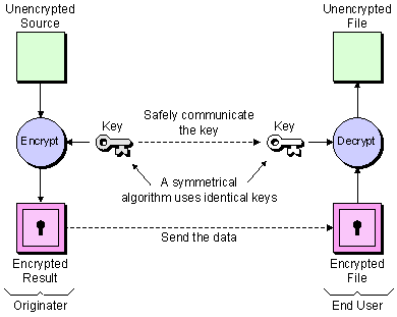

Рис. 1 Симетрична криптосистема

У поточних системах виробляється якась послідовність (вихідна гамма), яка в подальшому накладається на саме повідомлення, і шифрування даних відбувається потоком по мірі генерування гами. Схема зв'язку з використанням симетричною криптосистеми представлена на рисунку.

Схема зв’язку з використанням симетричною криптосистеми, де M – відкритий текст, K – секретний ключ, який передається по закритому каналу.

Зазвичай при симетричному шифруванні використовується складна і багатоступенева комбінація підстановок і перестановок вихідних даних, причому ступенів (проходів) може бути безліч, при цьому кожній з них повинен відповідати «ключ проходу». Операція підстановки виконує перша вимога, що пред'являється до симетричного шифру, позбавляючись від будь-яких статистичних даних шляхом перемішування бітів повідомлення за певним заданим законом. Перестановка необхідна для виконання другої вимоги – додання алгоритмом нелінійності. Досягається це за рахунок заміни певної частини повідомлення заданого обсягу на стандартне значення шляхом звернення до вихідного масиву.

Симетричні системи мають як свої переваги, так і недоліки перед асиметричними. До переваг симетричних шифрів відносять високу швидкість шифрування, меншу необхідну довжину ключа при аналогічній стійкості, велику вивченість і простоту реалізації. Недоліками симетричних алгоритмів вважають в першу чергу складність обміну ключами зважаючи на велику ймовірність порушення секретності ключа при обміні, який необхідний, і складність управління ключами у великій мережі.