УДК 003.26

Використання криптографічних методів для захисту даних у ПК

Іванов Р.Є., д.т.н., проф. Писаренко Л.Д.

Інформаційні ресурси в сучасних умовах являються одним із найважливіших результатів діяльності людського суспільства. Саме тому проблема захисту інформації на сьогоднішній день є дуже актуальною. Багато відомих причини призвели до виникнення цілої гами методів і засобів захисту інформації. Одним із підходів, щодо вирішення задач захисту інформації є застосування криптографії-одного із методів шифрування .

Метод шифрування / дешифрування називають шифром . Деякі алгоритми шифрування засновані на тому, що сам метод шифрування (алгоритм) є секретним. Нині такі методи представляють лише історичний інтерес і не мають практичного значення. Всі сучасні алгоритми використовують ключ для управління шифруванням і дешифруванням; повідомлення може бути успішно дешифровано тільки якщо відомий ключ. Ключ, використовуваний для дешифрування може не збігатися з ключем, що використовується для шифрування, однак у більшості алгоритмів ключі збігаються.

Алгоритми з використанням ключа діляться на два класи: симетричні (або алгоритми секретним ключем) і асиметричний (або алгоритми з відкритим ключем). Різниця в тому, що симетричні алгоритми використовують один і той же ключ для шифрування і для дешифрування (або ж ключ для дешифрування просто обчислюється по ключу шифровки). У той час як асиметричні алгоритми використовують різні ключі, і ключ для дешифрування не може бути обчислений по ключу шифровки.

Симетричні алгоритми поділяють на потокові шифри і блокові шифри. Потокові дозволяють шифрувати інформацію побітово, в той час як блокові працюють з деяким набором біт даних (зазвичай розмір блоку становить 64 біта) і шифрують цей набір як єдине ціле.

Асиметричні шифри (також іменовані алгоритмами з відкритим ключем) допускають, щоб відкритий ключ був доступний всім . Це дозволяє будь-якому зашифрувати повідомлення. Однак розшифрувати це повідомлення зможе тільки потрібна людина (той, хто володіє ключем дешифрування). Ключ для

шифрування називають відкритим ключем, а ключ для дешифрування - закритим ключем або секретним ключем.

Сучасні алгоритми шифрування/дешифрування досить складні і їх неможливо проводити вручну. Справжні криптографічні алгоритми розроблені для використання комп'ютерами або спеціальними апаратними пристроями. У більшості додатків криптографія виробляється програмним забезпеченням і є безліч доступних криптографічних пакетів.

Взагалі , симетричні алгоритми працюють швидше, ніж асиметричні. На практиці обидва типи алгоритмів часто використовуються разом: алгоритм з відкритим ключем використовується для того, щоб передати випадковим чином згенерований секретний ключ, який потім використовується для дешифрування повідомлення.

Наразі найкращим видом шифрування можна вважати AES шифрування. На сьогодні воно представлено у трьох модифікаціях – AES128 AES192 і AES256. Перший варіант застосовується більше для забезпечення інформаційної безпеки мобільних пристроїв, другий задіяний на більш високому рівні. Як стандарт, ця система була офіційно впроваджена у 2002 році, причому відразу ж її підтримка була заявлена з боку корпорації Intel, що виробляє процесорні чіпи. Суть її, на відміну від будь-якої іншої симетричної системи шифрування, зводиться до обчислень на основі полиноминального подання кодів і операцій обчислення з двовимірними масивами. Як стверджує уряд Сполучених Штатів, для злому довжиною ключа 128 біт дешифратору, нехай навіть найсучаснішого, потрібно близько 149 трильйонів років. Дозволимо собі не погодитися з таким компетентним джерелом. Комп'ютерна техніка за останні сто років зробила стрибок, порівнянний з геометричною прогресією, так що особливо радіти не варто, тим більше, що сьогодні, як виявилося, існують системи шифрування і краще , ніж ті, які США оголосили абсолютно стійкими до злому.

Криптографічний захист можна здійснювати різними способами: апаратним, програмним або програмно-апаратним. Апаратна реалізація криптографічного захисту - найбільш надійний спосіб, але й найдорожчий. Інформація для апаратних засобів передається в електронній формі через порт обчислювальної машини всередину апаратури, де виконується шифрування інформації. Перехоплення та підробка інформації під час її передачі в апаратуру може бути виконана за допомогою спеціально розроблених програм типу "вірус".

Програмна реалізація криптографічного захисту значно дешевша та гнучкіша в реалізації. Але виникають питання щодо захисту криптографічних ключів від перехоплення під час роботи програми та після її завершення. Тому, крім

захисту від "вірусних" атак, потрібно вжити заходів для забезпечення повного звільнення пам'яті від криптографічних ключів, що використовувались під час роботи програм "збирання сміття".Крім того, можна використовувати комбінацію апаратних і програмних механізмів криптографічного захисту. Найчастіше використовують програмну реалізацію криптоалгоритмів з апаратним зберіганням ключів. Такий спосіб криптозахисту є досить надійним і не надто дорогим. Але, вибираючи апаратні засоби для зберігання криптографічних ключів, треба пам'ятати про забезпечення захисту від перехоплення ключів під час їх зчитування з носія та використання в програмі.

Перевага апаратного шифрування над програмним обумовлено декількома причинами. По-перше, апаратне шифрування має більшу швидкість. Криптографічні алгоритми складаються з величезного числа складних операцій, виконуваних над бітами відкритого тексту. Сучасні універсальні комп'ютери погано пристосовані для ефективного виконання цих операцій, а спеціалізоване устаткування вміє робити їх набагато швидше. По-друге, апаратуру легше фізично захистити від проникнення ззовні. Програма, виконувана на персональному комп'ютері, практично беззахисна. Озброївшись відладчиком, зловмисник може внести в неї зміни, і ніхто нічого не помітить. І по-третє, апаратура шифрування більш проста в установці. Дуже часте шифрування потрібно там, де додаткове комп'ютерне устаткування є зовсім зайвим. Телефони, факсимільні апарати і модеми значно дешевше обладнати пристроями апаратного шифрування, чим вбудовувати в них мікрокомп'ютери з відповідним програмним забезпеченням. Навіть у комп'ютерах установка спеціалізованого шифрувального устаткування створює менше проблем, чим модернізація системного програмного забезпечення з метою додавання в нього функцій шифрування даних. Щоб домогтися цього за допомогою програмних засобів, шифрування повинне бути сховане глибоко в надра операційної системи. Але навіть будь-який непрофесіонал зможе приєднати шифрувальний блок з однієї сторони до персонального комп'ютера і до зовнішнього модему з іншої.

Проаналізуваши різного роду статті на тему програмного на апаратного шифрування даних можна прийти до висновку ,що наразі відомо вже багато різних способів шифрування ,але технології розвиваються надзвичайно швидко тому,та система ,яка буда надійною ще пару років тому,можливо вже завтра,хтось підбере ключ до її взлому. Тому,беручи за основу,статті та різні наукові напрацювання в цій галузі необідно постійно вдоскновалювати та модифікувати ті шифри ,які вже є на данний момент. Переглядаючи статті,особливу увагу я звернув на дослідження методів гомоморфного шифрування

інформаційних ресурсів,в основі методу якого полягає реалізація операцій додавання та множення над зашифрованими даними без їх попереднього розшифрування. Дане шифрування може використовуватися в багатьох алгоритмах як частково(RSA,Ель-Гамаля,Пейэ) так і повноцінно(Гентрі).Це шифрування є доволі новим так як тільки в 2009 році була вперше запропонована модель повністю гоморфної криптографічної системи. На даний момент не існує насправді якісної системи захисту інформації ,яка заснована на схемі гоморфного шифрування яка б вирішувала проблеми як конфіденційності, так і зручності використання, швидкості обчислень та продуктивності. Тому в перспективі для ефективного використання такої системи захисту необхідна реалізація, яка б задовольняла наступні умови: - можливість використання при проведенні процедури шифрування та дешифрування повного набору математичних функцій; - точність і швидкість обчислень повинні бути сталими на всіх стадіях шифрування та дешифрування; - кортеж ключів має бути настільки великим, щоб унеможливити можливість атаки повним перебором всіх можливих ключів; - розмір зашифрованих даних та довжина ключа не має значно впливати на продуктивність системи.

Тому,можливість для вдосконалення даного шифрування є і нею необхідно користуватися, адже в цьому шифруванні є ще багато невідомого,те що ще доведеться винайти.

Також ,досить цікавою була стаття С. Брао про пристрої апаратного шифрування даних з інтерфейсом usb. Було запропоновано пристрій шифрування з USB-інтерфейсом, який має структуру USB-ключа. Оскільки в багатьох галузях, де ціна та витрати енергії виходять на передній план, обчислювальна потужність сконцентрована в малих, недорогих центральних процесорах, серед яких домінують 8-бітні мікроконтролери, для використання в пристрої був вибраний малопотужний недорогий мікроконтролер ATmega16. Розроблену конструкцію можна вдосконалювати, збільшуючи функціональні можливості.

Висновки:

Проаналізувавши криптографію в цілому як науку,я прийшов до висновку,що в час розвитку комп’ютерних технологій,захист інформації виходить на перший план. Шифрування потребує постійного вдосконалення ,як апаратно так і програмно.

Література

1. Брао С. Пристрої апаратного шифрування даних з інтерфейсом USB / С. Брао // 69–та студентська науково–технічна конференція : **збірник тез доповідей**, Львів, жовтень–листопад 2011 року / **Національний університет "Львівська політехніка".** – Львів : Видавництво Львівської політехніки, 2011. – С. 172–173.

2. Ільєнко А. «Сучасні методи гомоморфного шифрування інформаційних ресурсів» - **Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні**, вип. 2 (30), 2015 р. - ISSN 2074-9481