Тема 13-14. Криптографічний вид захисту інформації. Поняття шифрування файлів, папок, повідомлень. Засоби здійснення шифрування інформації.

Криптографічний вид захисту інформації

Криптографія — наука про методи перетворення (шифрування) інформації з метою її захисту від зловмисників.

Криптографічні методи захисту інформації - це методи захисту даних із використанням шифрування.

Шифрування — процес застосування шифру і інформації, що захищається, тобто перетворення інформації, що захищається, в шифроване повідомлення за допомогою певних правил, що містяться в шифрі.

Всі відомі способи шифрування розбиті на п'ять груп: підстановка (заміна), перестановка, аналітичне перетворення, гаммування і комбіноване шифрування. Кожен з цих способів може мати декілька різновидів.

Під ***кодуванням*** розуміється такий вид криптографічного закриття, коли деякі елементи даних (не обов'язково окремі символи), що захищаються, замінюються заздалегідь вибраними кодами (цифровими, буквеними, буквено-цифровими поєднаннями і так далі). Цей метод має два різновиди: смислове і символьне кодування. При смисловому кодуванні кодовані елементи мають цілком певний сенс (слова, пропозиції, групи пропозицій). При символьному кодуванні кодується кожен символ тексту, що захищається. Символьне кодування по суті співпадає з підстановлювальним шифруванням.

До окремих видів криптографії відносяться ***методи розтину і стиснення даних***. Розтин полягає в тому, що масив даних, що захищаються, ділиться (розтинається) на такі елементи, кожен з яких окремо не дозволяє розкрити зміст інформації, що захищається. Виділені таким чином елементи даних розносяться по різних зонах пам'яті або розташовуються на різних носіях. Стиснення даних є заміною однакових рядків даних або послідовностей однакових символів, що часто зустрічаються, деякими заздалегідь вибраними символами.

Розтин шифру — процес отримання інформації (відкритого тексту), що захищається, з шифрованого повідомлення (шифртекста) без знання застосованого шифру.

Дешифрування — процес, зворотний шифруванню, що полягає в перетворенні шифрованого повідомлення в інформацію, що захищається, за допомогою певних правил, що містяться в шифрі.

Під ***ключем*** в криптографії розуміють змінний елемент шифру, який застосовують для шифрування конкретних повідомлень.

Одне з центральних місць в понятійному апараті криптографії займає таке поняття, як стійкість шифру. Під ***стійкістю шифру*** розуміють здатність шифру протистояти всіляким методам розтину.

Для того, щоб криптографічні методи перетворення забезпечили ефективний захист інформації, вони повинні задовольняти ряду вимог. У стислому вигляді їх можна сформулювати таким чином:

- складність і стійкість криптографічного захисту повинні вибиратися залежно від об'єму і ступеня секретності даних;
- надійність захисту повинна бути такою, щоб секретність не порушувалася у тому випадку, коли зловмисникові стає відомий метод захисту;
- метод захисту, набір використовуваних ключів і механізм їх розподілу не можуть бути дуже складними;
- виконання процедур прямого і зворотного перетворень повинне бути формалізованим. Ці процедури не повинні залежати від довжини повідомлень;
- помилки, що виникають в процесі виконання перетворення, не повинні розповсюджуватися на текст повною мірою і по системі;
- надмірність, що вноситься процедурами захисту повинна бути мінімальною.

Головна мета шифрування (кодування) інформації - її захист від несанкціонованого читання. Системи криптографічного захисту (системи шифрування інформації) можна поділити за різними

ознаками:

• за принципами використання криптографічного захисту (вбудований у систему або додатковий механізм, що може бути відключений);

• за способом реалізації (апаратний, програмний, програмно-аларатний);

• за криптографічними алгоритмами, які використовуються (загальні, спеціальні);

• за цілями захисту (забезпечення конфіденційності інформації (шифрування) та захисту повідомлень і даних від модифікації, регулювання доступу та привілеїв користувачи);

• за методом розподілу криптографічних ключів (базових/сеансових ключів, відкритих ключів) тощо.

Додаткові механізми криптозахисту - це додаткові програмні або апаратні засоби, які не входять до складу системи. Така реалізація механізмів криптозахисту має значну гнучкість і можливість швидкої заміни. Для більшої ефективності доцільно використовувати комбінацію додаткових і вбудованих механізмів криптографічного захисту.

За способом реалізації 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.

В основу шифрування покладено два елементи: криптографічний алгоритм і ключ.

Криптографічний алгоритм - це математична функція, яка комбінує відповідний текст або іншу зрозумілу інформацію з ланцюжком чисел (ключем) з метою отримання незв’язаного (шифрованого) тексту.

Усі криптографічні алгоритми можна поділити на дві групи: загальні і спеціальні.

Спеціальні криптоалгоритми мають таємний алгоритм шифрування, а ***загальні*** криптоалгоритми характерні повністю відкритим алгоритмом, і їх криптостійкість визначається ключами шифрування. Спеціальні алгоритми найчастіше використовують в апаратних засобах криптозахисту.

Загальні криптографічні алгоритми часто стають стандартами шифрування, якщо їхня висока криптостійкість доведена. Ці алгоритми оприлюднюють для обговорення, при цьому навіть визначається премію за успішну спробу його "злому". Криптостійкість загальних алгоритмів визначається ключем шифрування, який генерується методом випадкових чисел і не може бути повторений протягом певного часу. Криптостійкість таких алгоритмів буде вищою відповідно до збільшення довжини ключа.

Є дві великі групи загальних криптоа лгоритмі в: ***симетричні і асиметричні***. До ***симетричних криптографічних алгоритмів*** належать такі алгоритми, для яких шифрування і розшифрування виконується однаковим ключем, тобто і відправник, і отримувач повідомлення мають користуватися тим самим ключем. Такі алгоритми мають досить велику швидкість обробки як для апаратної, так і для програмної реалізації. Основним їх недоліком є труднощі, пов'язані з дотриманням безпечного розподілу ключів між абонентами системи. Для ***асиметричних криптоалгоритмів шифрування*** і

розшифрування виконують за допомогою різних ключів, тобто, маючи один із ключів, не можна визначити парний для нього ключ. Такі алгоритми часто потребують значно довшого часу для обчислення, але не створюють труднощів під час розподілу ключів, оскільки відкритий розподіл одного з ключів не зменшує криптостійкості алгоритму і не дає можливості відновлення парного йому ключа.

Усі криптографічні алгоритми можна використовувати з різними цілями, зокрема:

• для шифрування інформації, тобто приховування змісту повідомлень і даних;

• для забезпечення захисту даних і повідомлень від модифікації.

З найпоширеніших методів шифрування можна виділити американський алгоритм шифрування ***DES*** (Data Encryption Standart, розроблений фахівцями фірми IBM і затверджений урядом США 1977 року) із довжиною ключа, що може змінюватися, та алгоритм ГОСТ 28147-89, який був розроблений та набув широкого застосування в колишньому СРСР і має ключ постійної довжини. Ці алгоритми належать до симетричних алгоритмів шифрування.

Алгоритм Потрійний DES був запропонований як альтернатива DES і призначений для триразового шифрування даних трьома різними закритими ключами для підвищення ступеня захисту.

RC2, RC4, RC5 - шифри зі змінною довжиною ключа для дуже швидкого шифрування великих обсягів інформації. Здатні підвищувати ступінь захисту через вибір довшого ключа.

IDEA (International Data Encryption Algoritm) призначений для швидкої роботи в програмній реалізації.

Для приховування інформації можна використовувати деякі асиметричні алгоритми, наприклад, алгоритм RSA. Алгоритм підтримує змінну довжину ключа та змінний розмір блоку тексту, що шифрується.

Алгоритм RSA дозволяє виконувати шифрування в різних режимах:

• за допомогою таємного ключа відправника. Тоді всі, хто має його відкритий ключ, можуть розшифрувати це повідомлення;

• за допомогою відкритого ключа отримувача, тоді тільки власник таємного ключа, який є парним до цього відкритого, може розшифрувати таке повідомлення;

• за допомогою таємного ключа відправника і відкритого ключа отримувача повідомлення. Тоді тільки цей отримувач може розшифрувати таке повідомлення.

Але не всі асиметричні алгоритми дозволяють виконувати шифрування даних у таких режимах. Це визначається математичними функціями, які закладені в основу алгоритмів.

Другою метою використання криптографічних методів є захист інформації від модифікації, викривлення або підробки. Цього можна досягнути без шифрування повідомлень, тобто повідомлення залишається відкритим, незашифрованим, але до нього додається інформацію, перевірка якої за допомогою спеціальних алгоритмів може однозначно довести, що ця інформація не була змінена. Для симетричних алгоритмів шифрування така додаткова інформація - це код автентифікації, який формується за наявності ключа шифрування за допомогою криптографічних алгоритмів.

Для асиметричних криптографічних алгоритмів формують додаткову інформацію, яка має назву електронний цифровий підпис. Формуючи електронний цифровий підпис, виконують такі операції:

• за допомогою односторонньої хеш-функції обчислюють прообраз цифрового підпису, аналог контрольної суми повідомлення;

• отримане значення хеш-функції шифрується: а) таємним або відкритим; б) таємним і відкритим ключами відправника і отримувача повідомлення - для алгоритму RSA

• використовуючи значення хеш-функції і таємного ключа, за допомогою спеціального алгоритму обчислюють значення цифрового підпису, - наприклад, для російського стандарту Р.31-10.

Для того, щоб перевірити цифровий підпис, потрібно:

• виходячи із значення цифрового підпису та використовуючи відповідні ключі, обчислити значення хеш-функції;

• обчислити хеш-функцію з тексту повідомлення;

• порівняти ці значення. Якщо вони збігаються, то повідомлення не було модифікованим і

відправлене саме цим відправником.

Ефективність захисту систем за допомогою будь-яких криптографічних алгоритмів значною мірою залежить від безпечного розподілу ключів. Тут можна виділити такі основні методи розподілу ключів між учасниками системи.

1. Метод базових/сеансових ключів. Такий метод описаний у стандарті ISO 8532 і використовується для розподілу ключів симетричних алгоритмів шифрування. Для розподілу ключів вводиться ієрархія ключів: головний ключ (так званий майстер-ключ, або ключ шифрування ключів) і ключ шифрування даних (тобто сеансовий ключ). Ієрархія може бути і дворівневою: ключ шифрування ключів/ключ шифрування даних. Старший ключ у цій ієрархії треба розповсюджувати неелектронним способом, який виключає можливість його компрометації. Використання такої схеми розподілу ключів потребує значного часу і значних затрат.

2. Метод відкритих ключів. Такий метод описаний у стандарті ISO 11166 і може бути використаний для розподілу ключів як для симетричного, так і для асиметричного шифрування. За його допомогою можна також забезпечити надійне функціонування центрів сертифікації ключів для електронного цифрового підпису на базі асиметричних алгоритмів та розподіл сертифікатів відкритих ключів учасників інформаційних систем. Крім того, використання методу відкритих ключів дає можливість кожне повідомлення шифрувати окремим ключем симетричного алгоритму та передавати цей ключ із самим повідомленням у зашифрованій асиметричним алгоритмом формі.

Вибір того чи іншого методу залежить від структури системи і технології обробки даних. Жоден із цих методів не забезпечує "абсолютного" захисту інформації, але гарантує, що вартість "злому" у кілька разів перевищує вартість зашифрованої інформації.

Щоб використовувати систему криптографії з відкритим ключем, потрібно генерувати відкритий і особистий ключі. Після генерування ключової пари слід розповсюдити відкритий ключ респондентам. Найнадійніший спосіб розповсюдження відкритих ключів - через сертифікаційні центри, що призначені для зберігання цифрових сертифікатів.

Цифровий сертифікат - це електронний ідентифікатор, що підтверджує справжність особи користувача, містить певну інформацію про нього, слугує електронним підтвердженням відкритих ключів.

Сертифікаційні центри несуть відповідальність за перевірку особистості користувача, надання цифрових сертифікатів та перевірку їхньої справжності.

Розкриття зашифрованих текстів (в першу чергу знаходження ключа) здійснюється за допомогою методів криптоаналізу. Основними методами криптоаналізу є:

– ***статистичн***і, при яких знаючи статистичні властивості відкритого тексту намагаються досліджувати статистичні закономірності шифротексту і на підставі виявлених закономірностей розкрити текст;

– ***метод вірогідних слів***, в якому при зіставленні деякої невеликої частини шифротекста з відомим фрагментом відкритого тексту намагаються знайти ключ і з його допомогою розшифрувати весь текст. Необхідний фрагмент відкритого тексту можна знайти за допомогою статистичних методів або просто вгадати, виходячи з передбачуваного змісту або структури відкритого тексту.

Оскільки криптографічні методи застосовуються давно, то вже сформульовані основні вимоги до них.

1. Метод повинен бути надійним, тобто відновлення відкритого тексту при володінні тільки шифротекстом, але не ключем повинно бути практично нездійсненним завданням

2. Через труднощі запам'ятовування об'єм ключа не повинен бути великим.

3. Через труднощі, пов'язані з складними перетвореннями, процеси шифрування повинні бути простими.

4. Через можливості появи помилок передачі дешифровка шифротексту, що містить окремі помилки, не повинна привести до нескінченного збільшення помилок в отриманому передбачуваному відкритому тексті.

5. Через труднощі передачі об'єм шифротексту не повинен бути значно більше відкритого

тексту.

Криптографічні перетворення забезпечують вирішення двох головних проблем захисту інформації: проблеми секретності (позбавлення супротивника можливості витягувати інформацію з каналу зв'язку) і проблеми імітостійкості (позбавлення супротивника можливості ввести помилкову інформацію.

Сучасний криптографічний захист інформації здійснюється за допомогою спеціалізованого програмного забезпечення, що дає змогу використовувати складні методи шифрування з мінімальною затратою часу. Ще одним позитивним моментом такого застосування є доступність можливостей зашифрувати важливу інформацію, в тому числі повідомлення, окремі файли і папки звичайним користувачам, адже більшість таких програм доступні для розповсюдження та мають нескладний інтерфейс, звільняють користувача від необхідності знання способів та методів шифрування. Звичайно, якщо йде мова про криптографічний захист банківських систем, інформації стратегічного чи державного значення, то використовують спеціальні криптографічні системи, що складаються з програмних засобів, доступних вузькому колу користувачів, а частіше всього, оригінальними, спеціально створеними засобами.

Програмний комплекс криптографічного захисту інформації «Криптосервер»

Комплекс є сукупністю засобів криптографічного захисту інформації з функціями шифрування інформації, формування та зберігання ключової інформації, а також надання послуг встановлення автентичності даних, які надходять, зберігаються та обробляються в комп’ютеризованих системах оброблення інформації.

Комплекс реалізує наступні функції:

Захист даних - забезпечує захист інформації, яка передається по загальнодоступним мережам, від несанкціонованого ознайомлення й/або модифікації.

Керування - забезпечує конфігурування та налаштування параметрів компонентів Комплексу, необхідних для їх функціонування.

Аудит - дозволяє проводити аналіз записів у файлах протоколів.

Ідентифікація й автентифікація - блокує доступ до можливостей керування Комплексом осіб, що не мають відповідних повноважень.

Захист функціонування - підтримує функціонування Комплексу при спробах порушити цілісність програмного забезпечення або конфігураційної інформації.

Комплекс складається з наступних компонентів:

Центр генерації ключів (ЦГК) - програмний модуль, призначений для генерації закритих і відкритих ключів, а також для запису ключових носіїв для всіх компонентів Комплексу. Центр генерації ключів встановлюється на комп'ютері, що не має мережевих з’єднань.

Центр розподілу ключів (ЦРК) - програмний модуль, призначений для зберігання та видачі мережевими каналами довіреним компонентам Комплексу сертифікатів відкритих ключів, інформації про контур безпеки, що визначає учасників захищеної мережі, та іншої службової інформації.

Модуль шифрування (МШ) - програмний модуль, призначений для побудови захищеної мережі (шлюз ЗМ), який встановлюється на границі ЗМ або границі сегмента ЗМ, що функціонує в інтересах одного, декількох або всіх суб'єктів (об'єктів) даної ЗМ (сегмента ЗМ), що забезпечує створення захищених з'єднань із іншими довіреними модулями шифрування.

Модуль керування (МК) - програмний модуль, призначений для дистанційного керування компонентами Комплексу, такими як ЦРК, МШ.

Компоненти Комплексу обмінюються ідентифікаційною інформацією й виконують процедури автентифікації з використанням сертифікатів відкритих ключів, які запитуються у ЦРК. Захищене з’єднання може бути встановлено тільки після виконання процедур взаємної автентифікації компонентів Комплексу.

На сьогодні існує велика кількість алгоритмів і протоколів шифрування. Серед алгоритмів симетричного криптографії, яких безліч, можна згадати RC4, RC5, CAST, DES, AES і т.д. Оптимальна довжина ключів шифрування для цих алгоритмів - 128 розрядів. Що стосується асиметричного

шифрування, то тут в основному використовуються алгоритми RSA, Diffie-Hellman і El-Gamal, при цьому довжина ключів шифрування звичайно становить 2048 розрядів. Найбільш широко для криптографічного захисту переданих по каналах зв'язку даних, включаючи листи електронної пошти, застосовується протокол SSL, у якому для шифрування даних використовуються ключі RSA.

Популярним пакетом програм для шифрування листування по електронній пошті і будь-яких даних, що зберігаються на жорсткому диску є PGP (Pretty Good Privacy).

В безкоштовному варіанті PGP Desktop Email 9.6 (призначений тільки для приватного некомерційного використання) включені функції шифрування файлів і папок, в платному варіанті опцій значно більше - від шифрованого листування (включаючи через інтернет-пейджери) і створення зашифрованих дисків на локальному комп'ютері до розгортання захищеної локальної мережі.

Переваги:

- Простота і зручність у використанні.
- Вичерпна безпека електронної кореспонденції на шляху від відправника до одержувачу - 100% захист від несанкціонованого доступу і зміни даних.
- Автоматичний пошук відкритих ключів одержувача в інтернет-каталозі PGP Global Directory.
- Загальна інфраструктура ключів для шифрування електронної пошти, миттєвих повідомлень, файлів.
- Створення зашифрованих архівів PGP Zip на одну дію.
- Політики захисту інформації для автоматичного шифрування/дешифрування та цифрового підпису електронних листів з урахуванням адреси одержувача і відправника, а також вмісту і теми листа.
- Шифрування миттєвих повідомлень і пересилаються файлів.
- Перевірені технології.
- Криптозахист даних з використанням перевірених часів технологій, які отримали широке галузеве визнання.
- Підтримка галузевих стандартів і 100% сумісність з рішеннями OpenPGP і S/MIME.
- Програма PGP Desktop Email можна захищати за допомогою ключа PGP або сертифікату X.509. Воно також підтримує існуючі інфраструктури з ключами. • Підтримка смарт-карт/маркеров забезпечує багатофакторну аутентифікацію адміністраторів і користувачів.
- Інтеграція з популярними клієнтами електронної пошти, включаючи MS Outlook, Outlook Express, Eudora, Entourage і Apple Mail.
- Оновлення ПЗ PGP Desktop Email 9.6.

Програма STCLite 3.3 призначена для забезпечення захищеного і шифрованого пересилання поштових повідомлень по мережі Інтернет, а також для шифрованого та безпечного зберігання інформації на знімних носіях і жорстких дисках. Легко та витончено, ви можете зашифрувати вміст вашого листа, переконатися в цьому на власні очі (тому що шифрування виконується не на льоту, коли вже нічого змінити неможливо, а до відправки повідомлення) і спокійно відправити його своєму кореспонденту. При цьому ви можете бути впевнені, що жодних слідів не залишилося у вашому комп'ютері, тому що вся обробка повідомлення ведеться тільки в оперативної пам'яті комп'ютера, без запису інформації на жорсткий диск.

Програма STCLite 3.3 складається з модуля шифрування тексту, модуля шифрування файлів і папок, модуля стеганографії.

КОНТРОЛЬНІ ЗАПИТАННЯ

1. Дайте визначення поняттям «криптографія», «криптографічні методи захисту інформації», «шифрування».
2. Назвіть основні групи шифрування.
3. Що таке кодування? Які типи кодування ви знаєте?
4. В чому суть методів розтину та стиснення даних?
5. Що розуміють під стійкістю шрифту?

6. Сформулюйте основні вимоги до методів криптографічного перетворення.
7. Яка головна мета шифрування (кодування) інформації?
8. Охарактеризуйте способи реалізації криптографічного захисту.
9. Що таке криптографічні алгоритми? На які групи вони поділяються, охарактеризуйте їх.
10. Сформулюйте вимоги до криптографічних методів.
11. Охарактеризуйте програмний комплекс криптографічного захисту інформації «Криптосервер».