**Тема 9**

**ЦИФРОВИЙ ПІДПИС. ЦИФРОВИЙ СЕРТИФІКАТ**

**ПЛАН**

1. Цифровий підпис.
2. Цифровий сертифікат.
3. Захист апаратних пристроїв.
4. ***Циф******ровий підпис***

Алгоритми асиметричного шифрування можуть використовуватись для створення цифрових підписів. Ідея використання цифрового підпису базується на двох фундаментальних положеннях:

* таємний ключ захищений і доступ до нього має тільки власник;
* єдиний спосіб створити цифровий підпис - це використати секретний ключ.

В режимі шифрування даних відкритий ключ використовується для шифрування, а закритий - для дешифрування. В режимі створення цифрового підпису - навпаки: на етапі шифрування використовують таємний ключ, а на етапі дешифрування - відкритий (рис. 9.1).

Оскільки відкритий ключ є вільно доступним, то будь-хто зможе прочитати інформацію, зашифровану таємним ключем. Це не дає можливості засекречувати дані, проте дозволяє засвідчити цілісність змісту повідомлення, шифрований текст розшифровують за допомогою відкритого ключа. Якщо відкритий ключ розшифрував дані, то вони були зашифровані зв'язаним з ним таємним ключем. Якщо при дешифруванні відкритим ключем повідомлення не розшифровується, то повідомлення не було шифроване зв'язаним з ним таємним ключем або було спотворене після шифрування.

Такий прийом дозволяє здійснювати надійну автентифікацію повідомлень, звідси випливає, що все, що ви зашифрували за допомогою вашого таємного ключа, є вашим цифровим підписом.

Цифровий підпис є унікальним для повідомлення. Кожна комбінація повідомлення і таємного ключа буде видавати різні підписи. Криптологи стверджують, що досі не зафіксовано жодної вдалої атаки на цифровий підпис, побудований за допомогою алгоритму RSA.

Оскільки асиметричні алгоритми працюють повільно, то часто з мотивів продуктивності підписують не все повідомлення, а дані, які це повідомлення представляють. Дані, які представляють повідомлення, формують за певними правилами і називають *дайджестом повідомлення.*

Цифровий підпис - це конкретна реалізація криптографічної системи з відкритим ключем. Існує ще поняття електронного підпису. *Електронний підпис -* це будь-який знак або процедура, реалізовані електронними засобами та призначені для зв'язання запису з зобов'язаннями або завірення справжності запису. Прикладами електронного підпису може бути вихідний сигнал складного біометричного пристрою, який працює на розпізнаванні відбитків пальців, а може бути просто ім'я, введене наприкінці повідомлення, що буде відправлене електронною поштою.



Рис. 9.1. Схема використання асиметричної криптографії для

цифрового підпису

Для того, щоб бути переконаним, що відкритий ключ є власністю суб'єкта, який про це декларує, можна скористатись *цифровим сертифікатом.*

***2.******Ц******ифровий сертифікат***

Цифровий сертифікат зв'язує ім'я з відкритим ключем. Він створюється для того, щоб можна було виявити несанкціоновану заміну імені або відкритого ключа. Перегляд цифрового сертифікату повинен дати можливість виявити факт підміни.

Найнадійніший спосіб розповсюдження відкритих ключів -

послуги сертифікаційних центрів - сховищ цифрових сертифікатів.

Сертифікаційні центри несуть відповідальність за:

* перевірку особистості користувача;
* надання цифрових сертифікатів;

-перевірку їх справжності.

Сертифікаційний центр приймає відкритий ключ разом з доказами особистості (якими - залежить від класу сертифіката). Після цього респонденти користувача можуть звертатися до сертифікаційного центру за підтвердженням відкритого ключа користувача.

Відомі сертифікаційні центри (VeriSign, Cyber trust і Nortel) видають цифрові сертифікати, що містять ім'я власника, назву сертифікаційного центру, відкритий ключ для шифрування кореспонденції, термін дії сертифіката (як правило, від шести місяців до року), клас та ідентифікаційний номер цифрового сертифіката.

Виданий цифровий сертифікат може належати до одного з чотирьо х класів, які вказують на ступінь верифікації власника. Сертифікат першого класу отримати найлегше, оскільки тут вимагається мінімальна перевірка біографічних даних (лише імена й адреси електронної пошти). Під час видачі сертифіката другого класу сертифікаційний центр перевіряє посвідчення особистості, номер картки соціального страхування і дату народження. Користувачі, які бажають отримати сертифікат третього класу, повинні бути готові до того, що, крім інформації, необхідної для отримання сертифіката другого класу, сертифікаційний центр пе- ревірить їх кредитоздатність, використовуючи спеціальні установи.

Сертифікат четвертого класу містить ще й інформацію про посаду власника в його установі, але відповідні верифікаційні вимоги тут ще не вироблені остаточно. Чим вищий клас сертифіката, тим вищий ступінь верифікації.

Сертифікаційні центри несуть відповідальність і за ведення й публікацію списку недійсних сертифікатів.

Існують комерційні сертифікаційні центри (VeriSign, Cybertrust і Nortel) і державні (Поштова служба США). Компанія може стати сертифікаційним центром і після цього видавати сертифікати своїм службовцям або іншим компаніям .

***3. Захист апаратн******их пристроїв***

Комп'ютер може вийти з ладу не тільки внаслідок збою операційної системи, дій користувача чи зловмисника, ай в р езультаті збою апаратно го пр истр ою. В зв'язку з цим не мо жна ігнорувати такі істини:

* будь-який механічний або електронний пристрій рано чи пізно відмовить, в тому числі жорсткий диск і материнська плата;
* електрична енергія, що використовується для живлення більшості комп'ютерних систем, може бути непередбачено вимкнена, спотворена шумами, викидами.

Для захисту від збоїв апаратури необхідно вживати наступних заходів:

* забезпечення безперебійного живлення;
* резервування апаратного забезпечення;
* резервування даних.

*Джерела безперебійного живлення*

Висока складність і мініатюрні розміри електронних пристроїв роблять їх дуже чутливими до якості електричного живлення. В той же час якість сучасної енергетичної системи не розрахована на відповідність вимогам до живлення комп'ютерних систем.

Розрізняють чотири типи проблем, властивих енергетичним системам: вимикання живлення; „зашумлення" електричної напруги; викиди напруги; падіння напруги.

Найбільш ефективним захистом при використанні неякісних систем живлення є *джерела безперебійного живлення UPS* (Uninterruptible Power Supply).

*Резервування апаратного забезпечення.*

Комп'ютерні системи деяких організацій повинні функціонувати неперервно. В таких випадках необхідно використовувати обладнання, що передбачає надлишковість на апаратному рівні. Надлишково можуть бути встановлені джерела живлень, вентилятори, мережеві адаптери, центральні процесори, жорсткі диски та інші компоненти. Для забезпечення неперервної роботи використовуються інтерфейси з можливістю заміни компонент без зупинки системи.

*Резервування даних*

Резервування даних - це процедура створення копії даних на випадок виходу з ладу основного носія. Розрізняють:

* безпосереднє (online) резервування;
* майже безпосереднє (nearline) резервування;
* відкладене (offline) резервування.

Відкладене резервування є найбільш поширеним, оскільки легко реалізується і має оптимальне співвідношення вартість/ефективність. Метод передбачає стиснення копій даних і характеризується низькою швидкодією