Лабораторна робота № 16

Електронний цифровий підпис на основі симетричної криптосистеми

Мета: розробити спрощену систему ЕЦП на основі симетричного криптоалгоритму з участю арбітра

Обладнання: персональний комп'ютер, будь-яка мова програмування, криптобібліотека, де реалізовано симетричний шифр та фунцію хешування.

Теоретична частина

Електронний цифровий підпис можна реалізувати не тільки за допомогою асиметричних криптосистем, хоча це найпростіше й безпечніше. Можливо підписати документ й за допомогою симетричних криптоалгоритмів, хоча такий підпис насправді реалізується за допомогою деякого арбітра, якому довіряють усі сторони інформаційного обміну. Назвем цього арбітра Центром підписування (ЦП). Насправді це він підписує документи для учасників обміну інформацією, а не вони самі. В цьому і є основний недолік такого підпису.

Сам протокол симетричного підпису виглядає наступним чином.

У процесі підписування беруть участь три сутності: Сторона А, яка хоче надіслати підписаний документ Стороні В, і Центр підписування ЦП, якому повністю довіряють сторони інформаційного обміну. Довіра дуже важлива, оскільки компрометація ЦП призводить до руйнування усієї системи підпису.

Обидві сторони зареєстровані у ЦП і мають унікальні ідентифікатори (Id_A, Id_B) та ключі симетричної системи шифрування, K_A та K_B відповідно. Крім цього сторони домовляються про використання певної криптографчної хеш-функції H(M) для захисту цілісності повідомлень та економії трафіку.

Для того, щоби Сторона А підписала документ М, а Сторона В перевірила її підпис, необхідно виконати такі кроки.

Крок 1. А генерує повідомлення М, шифрує його на свому ключі $C=E_{KA}(M)$ та відправляє ЦП таку інформацію:

A-> ЦП: (Id_A, Id_B, C, H(M));

Крок 2. ЦП бере з бази даних ключ шифрування K_A, розшифровує С: $M=D_{KA}(C)$, отримує документ М, обчислює його хеш-образ Н'(М). Якщо при порівнянні Н'(М)=Н(М), то ЦП вважає, що документ саме той, який йому надіслав А, під час блукання Інтернетом не сталося підміни або спотворення інформації.

Крок 3. ЦП зашифровує повідомлення М на ключі K_B: $C'=E_{KB}(M)$ і надсилає стороні В таку інформацію:

ЦП->В: (Id_A, C', H(M)).

Крок 4. Сторона В розшифровує повідомлення $M'=D_{KB}(C')$, обчислює його хеш-образ Н(М'). Якщо Н(М')=Н(М), вона вважає, що повідомлення М підписано стороною А, причому це саме те повідомлення, яке відправила сторона А. Таким чином, ЕЦП підтверджено.

Звичайно, це дуже проста схема, яка має очевидні недоліки. Зокрема, ЦП може підмінити повідомлення своїм, обчислити свій хеш-образ для нього та надіслати цю інформацію від імені будь-якого користувача. Тому довіра до ЦП дуже важлива.

Практична частина

Необхідно реалізувати викладений в теоретичній частині протокол ЕЦП за допомогою обраної криптобібліотеки.

Архітектура системи може бути довільною: клієнт-сервер, окремі модулі тощо.

Вимоги до функціоналу:

1. Система повинна дозволяти ЦП реєструвати клієнтів: привласнювати їм унікальний ідентифікатор будь-якої конструкції на вибір розробника; генерувати унікальні ключі симетричної криптосистеми.

2. Надавати можливість перевірки приналежності певного клієнта до системи ЕЦП та відмовляти у сервісі незареєстрованим особам, запропонувавши їм зареєструватися.

3. Приймати від зареєстрованих клієнтів інформаційного обміну зашифровані документи та файли на підпис.

4. Зашифровувати та розшифровувати надані для накладання ЕЦП документи та файли.

5. Утворювати ЕЦП на основі симетричної криптосистеми за протоколом, викладеним у теоретичній частині.

6. ЦП повинен надавати можливість утворювати хеш-образ та порівнювати його з надісланим клієнтами.

7. Кожен клієнт повинен мати можливість зашифровувати/розшифровувати надіслану їм інформацію; утворювати/перевіряти справжність отриманого хеш-образу.

Таким чином, система ЕЦП повинна забезпечувати протокол ЕЦП, викладений у теоретичній частині.

Після закінчення розробки необхідно підготувати звіт з лабораторної роботи, який повинен містити:

а) протокол Ваших дій;

б) приклади утворення та перевірки ЕЦП;

в) відповіді на контрольні запитання.

Альтернативою звіту може бути скрін-каст з аудіо-поясненнями, виконаний власноруч, який демонстрував би роботу розробленої системи.

Контрольні запитання

1. Що таке електронний цифровий підпис? Які його відмінні та спільні риси з особистим підписом людини?
2. Які типи ЕЦП Ви знаєте? В чому їх відмінності та спільні риси?
3. Охарактеризуйте протокол ЕЦП на основі симетричної криптосистеми, його переваги та недоліки.
4. Охарактеризуйте протоколи ЕЦП на основі асиметричної криптосистеми, їх переваги та недоліки.
5. Які завдання для електронного документообігу виконує ЕЦП?
6. Створення якої інфраструктури необхідно для підтримки ЕЦП? Чому виникла така необхідність?