Лабораторна робота №2

Тема: Протокол Е-голосування зі сліпими підписами

Мета: Дослідити протокол Е-голосування зі сліпими підписами

Теоретичні відомості:

Незважаючи на те, що організувати голосування досить просто, але забезпечити виконання всіх вимог до секретності та інформаційної безпеки є складним завданням. Використання сліпих підписів може забезпечити відділення бюлетенів від виборців, зберігаючи при цьому процедуру ідентифікації чи автентифікації особистості виборця.

Розглянемо протокол Е-голосування зі сліпими підписами:

- Виборча комісія (ВК) формує список виборців та кандидатів.
- Кожен виборець створює 10 наборів повідомлень, кожен набір містить правильно оформлений бюлетень для кожного можливого результату (наприклад в бюлетені потрібно обрати прізвище одного з двох кандидатів «1» та «2», то кожен набір буде складатися з двох е-бюлетенів, один для кандидата «1», другий для кандидата «2»). Крім цього, кожне повідомлення містить випадковий ідентифікаційний номер, який повинен бути достатньо великим, щоб уникнути збігів з іншими виборцями. Цей номер має бути присутнім на кожному бюлетені від даного виборця, своєрідний ID виборця. За цим ID приховуються персональні дані виборця, які таким чином не розголошуються широкому загалу і, можливо (як варіант), виборчій комісії (ВК).
- Кожен виборець маскує (маскування це не шифрування) всі свої повідомлення (з усього свого пакету) та надсилає їх до ВК разом з множником маскування (ключем), щоби ВК могла розкрити їх частину на свій вибір.

- ВК перевіряє за іменем чи виборець раніше не надсилав їй бюлетені для підпису. ВК відкриває 9 з 10 наборів, на свій вибір, та перевіряє чи всі вони правильно сформовані. Після цього ВК індивідуально підписує кожне повідомлення (в нашому випадку їх 2) з одного набору, що вона не розкривала (з 10-го, наприклад) та надсилає їх назад виборцю підписаними її е-підписом, відмітивши у своєму обліковому реєстрі, що він вже надсилав свої повідомлення на підпис ВК.
- Виборець знімає своє маскування з повідомлень та отримує один набір бюлетенів, підписаний ВК. Оскільки вони не були зашифровані ВК, а лише підписані, то виборець одразу розуміє який з них з голосом за кандидата «1», а який за «2».
- Кожен виборець обирає лише один з отриманих бюлетенів та шифрує його відкритим ключем ВК.
- Виборець відправляє свій один обраний ним бюлетень до ВК.
- ВК розшифровує бюлетені своїм приватним ключем, перевіряє підписи, перевіряє унікальність ідентифікаційного номера, зберігає послідовний (за порядком надходження) номер та підбиває підсумки. ВК публікує результати голосування разом з кожним ID виборця і відповідним бюлетенем.

Перевагою цього протоколу є те, що виборець не може шахраювати (шахраювання дуже ускладнене, а не неможливе) та обманути систему на відміну від простого голосування. Протокол сліпого підпису забезпечує індивідуальність його бюлетеня. Якщо він спробує відправити той самий бюлетень двічі, ВК знайде дублювання ІД номерів на етапі 7 та не буде враховувати новий бюлетень. Якщо ж виборець спробує отримати кілька унікальних бюлетенів на етапі 3, то ВК визначить це на наступному етапі. А створити свої бюлетені шахрай не може, бо він не зможе їх підписати приватним ключем ВК. З тієї ж причині він не зможе перехопити чужий бюлетень.

У випадку, якщо сама ВК має шахрайські наміри, то вона не зможе дізнатися хто як проголосував, оскільки протокол сліпого підпису маскує ІД номер бюлетенів до моменту підведення підсумків. ВК не може встановити зв'язок між підписаним нею раніше бюлетенем, який був замаскований виборцем, та отриманим пізніше «заповненим» бюлетенем від того ж виборця. Опублікований список послідовних ІД номерів та пов'язаних з ними «заповнених» бюлетенів дозволяє виборцям впевнитися, що їх бюлетені були враховані правильно. Але виборець не має жодних доказів для підтвердження помилки в опублікованому списку, відповідно ВК має значні шанси не бути викритою при підробці бюлетенів.

Але проблеми у даного протоколу є. Якщо етап 7 не анонімний, і ВК може записати, хто який бюлетень надіслав, то вона може дізнатися хто за кого проголосував. Але це неможливо, якщо комісія отримує бюлетені в запечатаній урні для голосування і рахує їх пізніше. Хоча ВК і не може встановити зв'язок між виборцями та їх бюлетенями, вона може створити велику кількість підписаних і правильних бюлетенів і зшахраювати, прислави їх сама собі. У випадку ж якщо виборець помітить, що його бюлетень підмінили, то він просто не зможе цього аргументовано довести (таємне голосування виключає розголошення персональних даних виборця у певні періоди голосування, у цьому протоколі вони максимально відділені від бюлетеня і приховані за ID).

За допомогою повністю сліпих підписів один користувач може змусити іншого підписати щось неприйнятне, через що повністю сліпий підпис в багатьох випадках не використовується. Проте, мова йде про рівень відповідальності «сліпого» підписанта. Якщо у коло його відповідальності входить лише засвідчення факту створення кимось (виборцем у певний момент) та існування певного документа (повідомлення, бюлетеня) без знання його змісту, взяття засвідченого «сліпого» документа на облік (для майбутніх порівнянь та можливого розкриття на законних підставах в майбутньому: життєвий цикл документа від створення і до утилізації), за умови гарантування відсутності негативних наслідків для «сліпого» підписанта за незнання змісту

такого документа (форма суспільного договору), то сліпий підпис (або його принципи) ефективно використовується у різних галузях суспільного життя.

Існує спосіб, щоб одна сторона могла дізнаватися, що їй пропонують підписати, і при цьому зберігати корисні властивості сліпих підписів. Головним принципом такої техніки є розрізати потік на частини та випадково обрати з них кандидатів для перевірки (не весь потік). Імовірність зарахування помилки за правду залишається, але є певний шанс, що вона буде виявлена, в залежності від того як часто проводяться перевірки в частині потоку.

Подібним чином працюють сліпі підписи і у електронному голосуванні. ВК отримує набір замаскованих виборцем бюлетенів, вона може зняти маскування з усіх, окрім одного, після чого підпише останній. ВК не знає, що вона підписала. Але, оскільки вона перевірила 90% надісланих документів в пакеті на власний вибір та вони виявилися правильними, то ВК вважає, що і останній набір із двох документів (наприклад, виборець має обрати один із двох бюлетенів: за кандидата 1, або за кандидата 2) є правильний і його можна підписувати (тобто, засвідчувати, брати на облік) і надсилати виборцю.

RSA – криптографічний алгоритм з парою ключів (публічний та приватний), заснований на складності обрахування задачі факторизації великих чисел. Даний алгоритм може застосовуватися як для шифрування (забезпечення конфіденційності), так і для цифрового підпису відкритого документа (забезпечення цілісності та автентичності, достовірності і належності певному суб'єкту, нонрепудіації – унеможливлення відмови від виконаних дій чи прийнятих на себе обов'язків). RSA виконує і комплексну задачу: конфіденційність + цілісність + автентичність е-документа.

Процедура генерації ключів RSA:

- Обираємо прості числа p та q. У реальних системах великі, або дуже великі прості числа. У навчальних задачах обираємо прості у межах першої 1000.

- Обраховуємо їх добуток: $n = p \cdot q$.
- Обраховуємо функцію Ейлера: $\varphi(n) = (p-1) \cdot (q-1)$.
- Обираємо непарне число *e*, яке має бути взаємно просте з $\varphi(n)$ і таке, що $0 < e < \varphi(n)$.
- Обираємо число *d* так, щоб $(e \cdot d) \bmod \varphi(n)$ дорівнював 1 (може бути обчислено за допомогою розширеного алгоритму Евкліда).
- Числа *e* та *d* є ключами RSA.
- Пара ключів *(e, n)* – відкритий ключ, *(d, n)* – закритий ключ.

Для того, щоб зашифрувати повідомлення *m*, його спочатку потрібно представити у числовому вигляді так, щоби $0 \le m < n$. Потім обчислюється зашифрований текст *c*, на відкритому ключі, за допомогою рівняння:

$$c = m^e \bmod n$$

Для розшифрування криптограми *c* використовують закритий ключ та формулу:

$$m = c^d \bmod n \ .$$

Окрім шифрування та звичайного ЕЦП алгоритм RSA також може використовуватися для сліпого ЕЦП. Особливістю даного підпису є те, що сторона, яка підписує документ, не знає його вміст. Розглянемо алгоритм формування сліпого підпису:

- Виборець обирає випадковий множник для маскування *r*, який повинен бути взаємно простим з *n*, тобто НСД(*r*, *n*) = 1.
- Виборець обраховує $m` = m(r)^e \bmod n$ і надсилає m’ до ВК (e, n – відкритий ключ ВК у даному випадку).
- ВК обраховує $s` = m`^d \bmod n$, використовуючи свій закритий ключ *(d, n)*. Для зняття маскування ВК використовує формулу $m = m`(r^{-e}) \bmod n$.
- ВК надсилає *s`* виборцю

- Виборець прибирає своє маскування за допомогою формули $s = s` \cdot r^{-1} \bmod n = m^d \bmod n$ і отримує підписане ВК початкове повідомлення m.

Завдання:

Змоделювати протокол Е-голосування зі сліпими підписами будь-якою мовою програмування та провести його дослідження. Для кодування повідомлень використовувати шифрування RSA, для реалізації ЕЦП використовувати алгоритм RSA.

Умови: В процесі голосування повинні приймати участь не менше 2 кандидатів та не менше 4 виборців. Повинні бути реалізовані сценарії поведінки на випадок порушення протоколу (виборець не проголосував, проголосував неправильно, виборець не має права голосувати, виборець хоче проголосувати повторно, виборець хоче проголосувати замість іншого виборця та інші).

На основі змодельованого протоколу провести його дослідження (Аналіз повинен бути розгорнутим та враховувати всі можливі сценарії подій під час роботи протоколу голосування):

1. Перевірити чи можуть голосувати ті, хто не має на це права.
2. Перевірити чи може виборець голосувати кілька разів.
3. Чи може хтось (інший виборець, ВК, стороння людина) дізнатися за кого проголосували інші виборці?
4. Перевірити чи може інший виборець чи стороння людина проголосувати замість іншого зареєстрованого виборця.
5. Чи може хтось (інший виборець, ВК, стороння людина) таємно змінити голос в бюлетені?
6. Чи може виборець перевірити, що його голос вірно врахований при підведенні кінцевих підсумків?

Контрольні запитання:

1. Описати алгоритм Е-голосування зі сліпим підписом.

2. Якими властивостями ідеального голосування володіє протокол Е-голосування зі сліпим підписом?
3. Що таке сліпий цифровий підпис та для чого він використовується?
4. Опишіть алгоритм сліпого цифрового підпису RSA.
5. Опишіть алгоритм шифрування RSA.
6. Які способи шахраювання доступні виборцю при Е-голосуванні зі сліпим підписом?
7. Які способи шахраювання доступні ВК при Е-голосуванні зі сліпим підписом?

Оформлення звіту:

Звіт повинен бути оформлений шрифтом Times New Roman, розмір – 14, міжрядковий інтервал – 1.5, абзацний відступ – 1.25, вирівнювання – по ширині.

Структура звіту:

- Титульний лист
- Тема, мета, завдання роботи
- Покроковий детальний опис виконання роботи (у випадку виконання роботи у групі – опис виконання лише власної частини роботи)
- Демонстрація роботи протоколу
- Дослідження протоколу
- Висновок