Лабораторна робота №3

Тема: Протокол Е-голосування з двома виборчими комісіями

Мета: Дослідити протокол Е-голосування з двома виборчими комісіями

Теоретичні відомості:

У минулих роботах були розглянуті протоколи Е-голосування, в яких ВК може тим чи іншим способом зшахраювати, і одночасно з цим виборці не змогли б довести факт шахрайства, якщо він буде помічений. Разом з цією проблемою, сама ж ВК може створити неіснуючих виборців, від імені яких ВК може сама собі надіслати е-бюлетені з потрібним голосом.

Одним з рішень даної проблеми є розділ ВК на рівнозначні за можливостями та впливом частини. Таким чином жодна з них не буде мати достатньо влади, щоб зшахраювати успішно. Це, наприклад, може бути реалізовано створенням багатьох дрібних ВК, які мають прийняти голоси від обмеженої та фіксованої кількості виборців.

В наступному протоколі використовується централізована реєстрація, якою займається бюро реєстрацій (БР), і окремо виборча комісія (ВК) для підрахунку е-бюлетенів.

Розглянемо протокол Е-голосування з двома виборчими комісіями:

- Кожен виборець відправляє повідомлення до БР, у якому він запитує реєстраційний номер.
- БР повертає виборцю випадковій реєстраційний номер. БР зберігає список даних реєстраційних номерів разом зі списком їх отримувачів на випадок, якщо хтось спробує проголосувати двічі.
- БР відправляє список реєстраційних номерів до ВК.
- Кожен виборець формує для себе випадковий ідентифікаційний номер (самостійно). Після чого він створює повідомлення, в якому міститься даний ідентифікаційний номер, реєстраційний номер від БР та свій е-бюлетень. Шифрує його та підписує і надсилає це повідомлення до ВК.

- ВК перевіряє ЕЦП, розшифровує повідомлення, перевіряє реєстраційний номер по списку, який їй надало БР. Якщо номер є в списку, то ВК вилучає його зі списку, щоб уникнути повторного голосування. ВК добавляє ідентифікаційний номер до списку тих, хто проголосував та одразу зараховує отриманий голос.
- Після закінчення виборчого процесу, ВК публікує результати разом за списком, в якому містяться ідентифікаційні номери виборців та відповідні їм бюлетені.

Кожен виборець може побачити список ідентифікаційних номерів та знайти в ньому свій бюлетень, як і в минулому протоколі. Таким чином він має можливість переконатися, що його бюлетень врахований правильно.

Не слід забувати про те, що кожне повідомлення повинне бути зашифрованим та підписаним, щоб ускладнити підробку. Окрім цього ВК не може змінити бюлетені, оскільки після публікації результатів кожен виборець буде шукати свій ідентифікаційний номер, щоб перевірити бюлетень. Якщо ж виборець не знаходить свій номер чи знаходить його, але з іншим результатом голосування, то він одразу розуміє, що відбувся обман. Але виборець все ще не має жодних доказів для підтвердження помилки в опублікованому списку. Водночас з цим, ВК не може добавити свій бюлетень. Оскільки вони знаходяться під наглядом БР. БР чітко знає скільки виборців зареєстровано, їх ідентифікаційні номери і здатна виявити будь-яке шахрайство.

Однак, стороння особа може зшахраювати просто вгадавши правильний реєстраційний номер. Ймовірність такого порушення можна зменшити, якщо зробити кількість можливих реєстраційних номерів значно більшою ніж кількість реальних виборців. Звичайно ж кожен такий номер генерується абсолютно випадково.

Незважаючи на це, БР повинна бути органом влади, який заслуговує повної довіри, оскільки способи зшахраювати в нього є. Воно може зареєструвати виборців, які не мають права голосувати чи взагалі не існують, також можуть

зареєструвати одного і того ж виборця кілька разів. Даний ризик може бути зведений до мінімуму, якщо БР опублікує список зареєстрованих виборців, але без реєстраційних номерів. Якщо кількість бюлетенів буде більшою ніж кількість виборців з цього списку, то це буде відчити про шахрайство, але якщо виборців навпаки більше ніж бюлетенів, то виявити шахрайство не вдасться. Це буде свідчити лише про те, що не всі виборці проголосували.

Але цей протокол буде вразливим при зговорі БР та ВК, що є цілком ймовірним сценарієм. Якщо вони об'єднають свої наміри зшахраювати, то маючи доступ до баз даних один одного вони зможуть координувати свої дії по створенню неіснуючих виборців та корегувати результати таким чином.

DSA – криптографічний алгоритм з використанням закритого ключа для створення електронного підпису, але не для шифрування, що відрізняє його від алгоритмів RSA та Ель-Гамаля. Підпис створюється секретно закритим ключем, але може бути публічно перевірена відкритим ключем. Алгоритм заснований на важкості обрахунку логарифмів в кінцевих полях.

Для побудови цифрового підпису потрібно виконати наступні кроки:

- Обираємо криптографічну хеш-функцію *H(x)* (на власний вибір)
- Обираємо просте число *q*, розмірність в бітах *N* якого співпадає з розмірністю в бітах значень хеш-функції *H(x)*
- Обираємо просте число *p*, так, щоб значення *(p-1)* ділилося на *q*. Бітною довжиною числа *p* вважається число *L*
- Обираємо число g (так щоб g≠*1*), таке щоб $g = h^{(p-1)/q} \bmod p$, де *h* це деяке випадкове число ($h \in (1; p-1)$).

Ключами вважаються значення:

- Секретний ключ $x \in (0, q)$
- Відкритий ключ $y = q^x \bmod p$

Відкритими параметрами алгоритму вважаються значення *p, q, g, y*. Закритими параметрами лише число *x*. Значення *p, q, g* можуть бути спільними

для групи користувачів і лише числа *x* та *y* являються ключами конкретного користувача. Для підпису повідомлення використовуються секретні числа *x* та *k*, де число *k* повинно бути обране випадковим чином для кожного повідомлення.

Для підпису повідомлення:

- Обираємо випадкове число $k \in (0, q)$
- Обраховуємо $r = (g^k \bmod p) \bmod q$, якщо *r* рівне нулю, то обираємо інше *k*
- Обраховуємо $s = k^{-1}(H(m) + xr) \bmod q$. Якщо *s=0*, то обираємо інше *k*
- Підписом вважається пара *(r, s)* загальною довжиною *2N*

Для перевірки підпису виконуються наступні дії:

- Обраховуємо $w = s^{-1} \bmod q$
- Обраховуємо $u_1 = (H(m) \cdot w) \bmod q$
- Обраховуємо $u_2 = (r \cdot w) \bmod q$
- Обраховуємо $v = ((g^{u_1} \cdot y^{u_2}) \bmod p) \bmod q$
- Підпис вважається вірним, якщо *v=r*

Схема Ель-Гамаля – криптосистема з відкритим ключем, яку засновано на складності обчислення дискретних логарифмів у скінченному полі. Криптосистема включає у себе алгоритм шифрування і алгоритм цифрового підпису.

Для підпису повідомлення *M* спочатку потрібно згенерувати ключі:

- Геренуємо випадкове просте число *p* . У реальних системах велике, або дуже велике просте число. У навчальних задачах обираємо просте у межах першої 1000.
- Обираємо випадкове ціле просте число *g*, *1<g<p*
- Обираємо випадкове ціле число *x*, *1<x<p-2*
- Обраховуємо $y = g^x \bmod p$
- Відкритий ключ – *(p, g, y)*, закритий ключ – *x*

Для шифрування повідомлення *M* виконуємо наступні дії:

- Обирається сесійний ключ, який є випадковим цілим числом k і відповідає умові $1<k<p-1$
- Відкрите повідомлення розбивається на блоки за необхідності (кожен блок m не повинен бути більшим за p)
- Обчислюються значення $a = g^k \bmod p$ та $b = (y^k \cdot M) \bmod p$, де a – лазівка, b – шифротекст.
- Пара блоків даних (a, b) являються криптограмою

Для розшифрування шифротексту виконуємо обрахунок за наступною формулою:

$$M = b(a^x)^{-1} \bmod p$$

Завдання:

Змоделювати протокол Е-голосування з двома виборчими комісіями будь-якою мовою програмування та провести його дослідження. Для кодування повідомлень використовувати метод Ель-Гамаля, для реалізації ЕЦП використовувати алгоритм DSA.

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 врахований при підведенні кінцевих результатів?

Контрольні запитання:

1. Опишіть алгоритм Е-протоколу з двома виборчими комісіями.
2. Які переваги та недоліки (порівняно з мінімальним протоколом та ідеальним) має алгоритм Е-протоколу з двома виборчими комісіями?
3. Які способи шахрайства можуть виникнути зі сторони організаторів Е-голосування?
4. Які способи шахрайства можуть виникнути зі сторони виборця?
5. Опишіть алгоритм шифрування Ель-Гамаля.
6. Опишіть алгоритм ЕЦП DSA. Чи має він якісь переваги чи недоліки порівняно з алгоритмами RSA та Ель-Гамаля?
7. Чи є способи вдосконалення алгоритму Е-протоколу з двома виборчими комісіями? Які?
8. Чи може проводитися Е-голосування без участі виборчих комісій? Якщо так, то як, якщо ні, то чому?

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