Лабораторна робота №6

Тема: Протокол Е-голосування без підтвердження

Мета: Дослідити протокол Е-голосування без підтвердження

Теоретичні відомості:

У попередніх лабораторних роботах були розглянуті протоколи Е-голосування, які задовольняють найважливіші вимоги такі як таємність голосування та правильність результатів. Вони мають багато відмінностей у рівні безпеки та ефективності застосування, але вони мають одну спільну рису – вони дозволяють виборцю довести, що він віддав голос за того чи іншого кандидата, завдяки чому стає можливим для виборців продавати свої голоси. Вирішити цю проблему можна досить простим способом – не дати виборцю можливість довести покупцеві голосів, що він дійсно віддав голос за потрібного кандидата.

Однак запобігання такому сценарію не дасть нам якісно забезпечити відсутність шахраювання з боку виборчих комісій. Можна вважати, що скупка голосів це рідке явище і варто надати перевагу контролю над ВК, оскільки все знаходиться в її руках і відповідно ВК може робити з отриманими бюлетенями все, що їй заманеться. Але в такому випадку варто поставити питання: кого важче підкупити – виборця чи ВК, тобто хто швидше за все погодиться на пропозицію підкупу – виборець, який буде вважати, що один голос нічого не змінить, а легкі гроші на дорозі не лежать, чи ВК, яка являється державним органом (часто розділеним на кілька окремих незалежних частин), що спрямований на забезпечення коректного проведення безпечного чесного голосування.

Основна ідея в забезпеченні непідтверджуваного голосування полягає в попередній фізичній реєстрації виборців з наданням їм частинки інформації (токена), яка буде використана у подальших кроках голосування. Фізична реєстрація виборців може відбуватися задовго до проведення виборів та лише одноразово за життя виборця, тобто це не повинно викликати великих проблем.

В даному токені містяться ключі для шифрування та ідентифікатор виборця, які йому (виборцю) невідомі, тобто самостійно (вручну) зашифрувати повідомлення виборець не зможе, лише за допомогою використання токена, який надасть всю потрібну інформацію для створення бюлетеня.

Розглянемо протокол Е-голосування без підтвердження (в процесі бере участь бюро реєстрації (БР) та виборча комісія (ВК)):

1) Підготовка:
   - БР підраховує кількість потенційних виборців, генерує потрібну кількість ІД номерів та надсилає їх до ВК.
   - ВК створює таку ж кількість ключів (відкритих та закритих) для генератора випадкових бітів. Для шифрування бюлетенів ключі генеруються однакові для всіх виборців. ВК зберігає ІД виборців та відповідний їм закритий ключ.
   - ВК створює токени, які містять в собі ІД виборців та їх відкриті ключі та надсилає їх до БР.
2) Реєстрація:
   - Виборець фізично приходить до БР, надає інформацію про себе (наприклад заповнює анкету для реєстрації).
   - БР зберігає дані виборця, додає до них серійний номер токену, який буде наданий виборцю, та видає даний токен виборцю. Також надає логін та пароль до програмного додатку, через який проходить Е-голосування.
3) Голосування:
   - Виборець встановлює програмний додаток для Е-голосування на свій пристрій (персональний комп’ютер наприклад), входить до свого профілю. Після чого підключає токен до свого пристрою.
   - Виборець обирає кандидата, за якого хоче віддати свій голос, та запускає процес формування Е-бюлетеня та його шифрування.
   - Програмний додаток використовує інформацію із токену для шифрування Е-бюлетеня та відправляє його до ВК (остаточне

повідомлення виглядає наступним чином: $E_2(E_1(M), x_0, ID)$, де M – бюлетень, $E_1()$ – шифрування бюлетеня, x_0 – перше значення генератора бітів, ID – ІД номер виборця, $E_2()$ – шифрування загального повідомлення).

4) Підрахунок голосів:
   - ВК протягом певного періоду часу отримує всі повідомлення від виборців.
   - ВК розшифровує бюлетені та підводить підсумки.
   - ВК публікує результат голосування.

Основними недоліками даного протоколу є те, що виборець повинен повністю довіритися БР та ВК. Вірогідність того, що їм потрібно буде зшахраювати досить низька, оскільки це органи, що створені для забезпечення коректного проведення виборів, але така ймовірність (ймовірність підкупу ВК третьою стороною) існує. Проте ймовірність підкупу виборця значно вища, оскільки це водночас і дешевше і легше. В даному протоколі вся інформація яка доступна виборцю це кандидат, за якого він проголосував, відповідно перехоплення шифротексту виборцю не надасть важливої інформації для його розшифрування.

Разом з тим, ВК не знає хто (особистість) надсилає їй бюлетені. В неї є список всіх зареєстрованих ІД номерів, але вона не знає які з них кому належать. Незважаючи на це, незареєстрований виборець всеодно не зможе надіслати повідомлення до ВК, оскільки для цього потрібно мати доступ до додатку для Е-голосування та мати токен, який надає БР. Навіть спроба викрадення токену не дасть можливості сторонній людині проголосувати, оскільки в неї не буде доступу до додатку.

В той же час така анонімність виступає недоліком, оскільки для підтвердження свого голосування виборець може просто передати свій токен та інформації для доступу до додатку третій особі. Але в такому випадку виборець втрачає право голосу і на наступні голосування, оскільки токени можуть не

змінюватися протягом багатьох голосувань. Окрім того, виборець для підтвердження свого голосу може запросити третю особу (покупця), щоб проголосувати під його наглядом. Оскільки голосування електронне, то неможливо забезпечити норми очних голосувань – голосування наодинці. Але уникнення таких сценаріїв можна забезпечити лише хіба присутністю виборця на виборчій дільниці, що повністю руйнує принцип електронного голосування.

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:

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

Генератор Blum Blum Shub (BBS) – генератор псевдовипадкових чисел, заснований на теорії квадратичних залишків.

Існує 2 простих числа p та q, конгруентних 3 по модулю 4, це закритий ключ. Їх добуток $n=p*q$ є відкритим ключем. Безпека схеми опирається на складність розкладання n на множники.

Для шифрування повідомлення M спочатку вибирається випадкове число x, взаємно просте з n. Потім обчислюється $x_0=x^2 \bmod n$. x_0 – служить початковою послідовністю для генератора псевдовипадкових бітів BBS, а вихід генератора використовується в якості потокового шифру. Кожне наступне значення обраховується за формулою: $x_{i+1}=x_i^2 \bmod n$. Можемо побітно виконати XOR M з виходом генератора. Генератор видає біти b_i (молодший значущий біт x_i), тому:

$M=M_1, M_2, M_3, \ldots M_i$

$c=M_1*b_1, M_2*b_2, M_3*b_3, \ldots M_i*b_i$, де i – це довжина відкритого тексту.

Розшифрувати це повідомлення можна тільки одним способом – отримати x_0 і з цієї стартової послідовності запустити генератор BBS, виконуючи XOR виходу з шифротекстом. Тільки той хто знає p та q, зможе розшифрувати повідомлення.

Особливістю цього алгоритму є те, що для отримання x_i необов'язково обчислювати всі попередні значення, якщо відома початковий стан генератора x_0 і числа p та q. i-те значення може бути обчислене за формулою:

$$x_i = x_0^{2^n \bmod \lambda(n)} \bmod n$$

де $\lambda(n)$ – найменше спільне кратне чисел $(p-1)$ і $(q-1)$.

Завдання:

Змоделювати протокол Е-голосування без підтвердження будь-якою мовою програмування та провести його дослідження. Для кодування

повідомлень використовувати метод Ель-Гамаля, для кодування Е-бюлетеня використовувати метод BBS.

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 без підтвердження.
2. Які переваги та недоліки (порівняно з мінімальним протоколом та ідеальним) має алгоритм Е-протоколу без підтвердження?
3. Які способи шахрайства можуть виникнути у алгоритмі Е-голосування без підтвердження?
4. Опишіть алгоритм псевдовипадкового генератора BBS. Які є способи його застосування в протоколах Е-голосування?

5. Яким чином забезпечується неможливість продажу голосів у виборців? Чи є ці способи ефективними?
6. В чому полягає специфіка забезпечення безпеки від продажу голосів?
7. Кому варто більше довіряти: виборцю чи ВК? Чому?
8. Опишіть алгоритм Ель-Гамаля.

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