Лабораторна робота №1

Тема: Простий протокол Е-голосування

Мета: Дослідити протокол простого Е-голосування

Теоретичні відомості:

Протокол – це порядок дій між двома або більше сторонами, що призначений для вирішення конкретних задач. Протокол виконується від початку до кінця в конкретній послідовності, кожна дія виконується лише після закінчення попередньої. Для його реалізації потрібно мінімум дві людини і реалізація протоколу повинна закінчуватися певними результатами. Кожен учасник протоколу повинен знати послідовність його дій, не порушувати порядок дій. Протокол повинен бути складений таким чином, щоб не було можливості його неправильно зрозуміти та передбачати дії на всі ситуації, що можуть виникнути під час його реалізації.

Криптографічний протокол – це протокол, що використовує криптографію, що містить в собі деякий криптографічний алгоритм. Учасники протоколу можуть захотіти поділитися секретом друг з другом, разом згенерувати випадкову послідовність символів, підтвердити справжність друг другу, підписати контракт в один і той же час. Сенс застосування криптографії у протоколах – недопустити чи виявити шахрайство або зраду. Головне правило таких протоколів – неможливо зробити чи дізнатися більше ніж визначено в протоколі.

Криптографічні протоколи електронного голосування – протоколи обміну даними для реалізації безпечного таємного електронного голосування через інтернет за допомогою ЕОМ. Цей напрямок криптографії досі активно розвивається, але вже був випробуваний на практиці у безлічі країн, таких як Великобританя, США, Австралія, Австрія, Бельгія, Канада, Франція, Іспанія, Ектонія та інші. Для впевненості в правильності, надійності та конфіденційності таких виборів використовують протоколи з доказаною

захищеністю, які опираються на перевірені криптографічні системи шифрування та ЕЦП.

Учасники можуть безпечно обмінюватися своїми повідомленнями лише зашифрувавши свої повідомлення. Для цього учасники спочатку повинні обрати систему шифрування та обрати ключі. Після чого учасники шифрують свої повідомлення, відправляють їх один одному та після отримання розшифровують.

Для підтвердження справжності документу чи погодження з ним використовуються електронні підписи. Вона забезпечує такі властивості: підпис достовірний, підпис непідробний, підпис не може бути використаний повторно, підписаний документ не можна змінити, від підпису неможливо відмовитися. Однак жодне з цих тверджень не є справедливим, оскільки підписи можуть бути скопійовані та документ може бути змінений вже після підписання.

Використання комп'ютерних виборів можливе лише тоді, коли з'явиться протокол, який одночасно забезпечує безпеку від шахрайства і захищає таємницю особистості. Ідеальний протокол повинен щонайменше відповідати наступним властивостям:

- (1) Голосувати можуть лише ті, хто має на це право.
- (2) Кожен може голосувати не більше одного разу.
- (3) Ніхто не може дізнатися за кого проголосував конкретний виборець.
- (4) Ніхто не може проголосувати замість іншого.
- (5) Ніхто не може таємно змінити чийсь голос.
- (6) Кожен виборець може перевірити, що його голос враховується при підведенні кінцевих результатів.

Розглянемо мінімальний протокол електронного голосування:

- Кожен виборець шифрує свій бюлетень ключем центральної виборчої комісії (ЦВК).

- Кожен виборець посилає свій бюлетень в ЦВК.
- ЦВК розшифровує бюлетені, робить висновки та публікує результати голосування.

Даний протокол має безліч проблем, наприклад ЦВК не може дізнатися звідки отримані бюлетені, чи належить надіслані бюлетені виборцям, що мають право голосувати. Окрім цього невідомо скільки разів голосував кожен виборець. Однак в нього є і позитивні сторони – неможливість зміни бюлетеня іншої особи, але в той же час виникає питання навіщо його змінювати, якщо кожен може голосувати безліч разів.

Розглянемо простий протокол:

- Формування списку кандидатів та виборців.
- Кожен виборець підписує свій бюлетень своїм ключем.
- Кожен виборець шифрує свій бюлетень ключом ЦВК.
- Кожен виборець надсилає свій бюлетень до ЦВК.
- ЦВК розшифровує бюлетені, перевіряє підписи, підводить висновки та публікує результати голосування.

Даний протокол володіє властивостями (1) та (2). Кожен бюлетень підписаний закритим ключем виборця, тому ЦВК знає, хто голосував та як голосував даний виборець. Якщо надходить неправильно підписаний, не підписаний чи повторний бюлетень, то він ігнорується. Окрім цього, завдяки цифровому підпису ніхто не зможе змінити бюлетень, навіть якщо він буде перехоплений.

Проблемою даного протоколу є те, що підпис добавляється до бюлетеня і відповідно ЦВК знає хто за кого проголосував. Використання відкритого ключа заважає зовнішнім зловмисникам зловживати протоколом та дізнаватися хто за кого голосував, але виборцям доводиться повністю довіряти ЦВК.

RSA – криптографічний алгоритм з відкритим ключем, заснований на складності обрахування задачі факторизації великих чисел. Даний алгоритм може застосовуватися як для шифрування, так і для цифрового підпису.

Алгоритм роботи ЕЦП RSA:

1. Генерація ключів
2. Формування ЕЦП:
   2.1. Сформувати повідомлення
   2.2. Захешувати текст
   2.3. Сформувати ЕЦП за допомогою закритого ключа
   2.4. Відправити текст з ЕЦП отримувачу
3. Перевірка ЕЦП
   3.1. Захешувати отриманий текст
   3.2. Отримати хеш з ЕЦП
   3.3. Порівняти два хеша (повинні бути рівні один другому)

Процедура генерації ключів:

- Обираємо прості числа p та q.
- Обраховуємо їх добуток: $n = p \cdot q$
- Обраховуємо функцію Ейлера: $\varphi(n) = (p-1)(q-1)$
- 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.

Алгоритм цифрового підпису починається з попереднього хешування повідомлення. Для обрахунку хеш-образу повідомлення у даній Лабораторній роботі використовується спрощена хеш-функція квадратичної згортки:

$$H_i = (H_{i-1} + M_i)^2 \bmod n,$$

де $H_0=0$, M_i – номер букви в алфавіті, n – частина закритого ключа.

Для формування ЕЦП використовується закритий ключ *(d, n)* та хеш повідомлення *H*. Формула для формування ЕЦП:

$$ЕЦП = H^d \bmod n$$

Для перевірки ЕЦП використовується відкритий ключ *(e, n)*, ЕЦП та хеш повідомлення. Формула для отримання хешу з ЕЦП:

$$H_c = ЕЦП^e \bmod n$$

Для перевірки порівнюємо значення *H* та H_c.

Шифри гамування є досить ефективнішими з точки зору стійкості і швидкості перетворення (шифрування та дешифрування). Для шифрування та розшифрування використовуються елементарні арифметичні операції. Відкрите чи закрите повідомлення і гамма, представлені у числовому вигляді, додаються одне до одного по модулю, тобто результатом даної операції є залишок від ділення доданих чисел поділений на модуль. Дані шифри можуть використовувати додавання по модулю 2, так і додавання по модулю N, серед яких модуль 2 є дуже зручним для програмно-апаратних реалізацій шифрування. Якщо ж за модуль взято 2, то шифрування є аналогічним до операції XOR:

⊕	0	1
0	0	1
1	1	0

Таким чином при даному способі шифрування символи та гамма зображуються у двійковому вигляді, після чого кожна пара двійкових розрядів додається по модулю 2. Процедури шифрування та дешифрування розраховується за наступними формулами:

$$C_i = P_i \oplus K_i \text{ та } P_i = C_i \oplus K_i$$

Завдання:

Змоделювати простий протокол Е-голосування будь-якою мовою програмування та провести його дослідження. Для кодування повідомлень використовувати метод гамування, 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, ЦВК, 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, ЦВК, стороння людина) таємно змінити голос в бюлетені?
6. Чи може виборець перевірити, що його голос врахований при підведенні кінцевих результатів?

Контрольні запитання:

1. Що таке криптографічні протоколи електронного голосування?
2. Опишіть мінімальний протокол електронного голосування.
3. Які переваги та недоліки має мінімальний протокол електронного голосування?

4. Що є ідеальним протоколом електронного голосування?

5. Опишіть простий протокол електронного голосування.

6. Які переваги та недоліки має простий протокол електронного голосування?

7. Що таке ЕЦП, для чого вони використовуються? Опишіть алгоритм ЕЦП RSA.

8. Які види шифрування можуть застосовуватися у криптографічних протоколах електронного голосування? Опишіть алгоритм гамування.

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