Лабораторна робота №5

Тема: Протокол Е-голосування з розділенням комісії на незалежні частини

Мета: Дослідити протокол Е-голосування з розділенням комісії на незалежні частини

Теоретичні відомості:

Розглядаючи попередні протоколи з участю виборчих комісій, можна було помітити, що зберігалася одна тенденція – організатори виборів могли впливати на їх результати підміняючи бюлетені виборців. Звичайно в деяких протоколах передбачена перевірка свого голосу виборцем, але у випадку порушення протоколу зі сторони ВК (бюлетень був замінений на інший), виборець нічого доказати не зможе.

Вирішити цю проблему можна розділивши бюлетень на частини, які до того ж будуть отримувати різні незалежні ВК. Завдяки цьому жодна з ВК не будуть знати за якого виборця відданий голос в бюлетені навіть, якщо їм вдасться розшифрувати бюлетень до кінця голосування. Даний протокол організації Е-голосування не вирішує проблему змови між ВК, але принаймні ускладнює підміну голосу, оскільки одна ВК може хотіти підробити результати, а друга може на це не погодитися і не надасть їм другу частину бюлетенів.

Звісно в такому випадку ця ВК може спробувати навмання підробити бюлетені, якщо їй вдасться розшифрувати свою частину Е-бюлетенів та проаналізує їх. Але їх аналіз може допомогти лише, якщо в процесі бере участь шифрування, яке є гомоморфним по множенню. Якщо ж шифр гомоморфний по додаванню, то аналіз цій ВК ніяк не допоможе, оскільки варіантів розділення бюлетеня буде надто багато.

Окрім цього це швидше за все призведе до великої кількості помилок під час підрахунку голосів. Оскільки перед підрахунком голосів всі ВК публікують частинки бюлетенів, то виборець може перевірити чи правильно зафіксувала його голос кожна з ВК. Поєднання помилкових бюлетенів (таких, які не

підходять під жодного кандидата) та скарг від виборців на одну з ВК може призвести до викриття шахраювання. Однак, якщо всі ВК погодяться на змову, то шахраювання буде виконане без помилок.

Розглянемо протокол Е-голосування з розділенням комісії на незалежні частини (склад організаторів зіставляє 3 незалежних органи: дві виборчі комісії, які отримують частинки бюлетенів – ВК-1 та ВК-2, та центральна виборча комісія, яка підводить підсумки - ЦВК):

- ЦВК формує список виборців та кандидатів, кандидатам надає ІД номери, за допомогою яких буде проходити голосування. Виборцям також надає ІД номери.
- Кожен виборець обирає свого кандидата, розділяє його ІД номер на довільні множники. Створює 2 бюлетеня, які складаються з різних множників.
- Виборець шифрує обидва бюлетеня відкритим ключем ЦВК, додає до повідомлення свій ІД номер, підписує та надсилає ці повідомлення різним ВК (ВК-1 та ВК-2).
- Обидві ВК перевіряють підписи. Після чого перевіряє чи надходили їй повідомлення з таким ІД номером. Робить відповідну відмітку, що повідомлення від даного виборця отримані. Зберігає ІД номер виборця та зашифровану частину бюлетеня.
- Після надходження всіх бюлетенів, ВК-1 та ВК-2 публікують всі ІД номери та відповідні їм зашифровані частини бюлетенів.
- ЦВК збирає опубліковані дані (ІД виборця та 2 частини бюлетеня), з’єднує обидві частини бюлетеня та розшифровує отриманий шифротекст своїм закритим ключем. Після чого оголошує результати голосування та публікує ІД виборців та відповідні їм бюлетені, щоб виборці могли впевнитися, що на другому етапі також не відбулося шахраювання з боку ЦВК.

Різни шифри можуть бути гомоморфними за різними математичними операціями. В даному випадку розглядається шифр з гомоморфністю по множенню. Тобто це дозволяє нам виконувати математичні операції над шифротекстом, що дозволяє перетворити один шифротекст в інший не розшифровуючи його. У випадку голосування це дозволяє розбивати бюлетені на частини, шифрувати їх, а потім з'єднувати в зашифрованому вигляді. Шифротекст такого з'єднаного бюлетеня може відрізнятися від того, якби ми зашифрували цілий бюлетень, але після розшифрування ми отримаємо однаковий відкритий текст.

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. Він є гомоморфним по множенню.

Процедура генерації ключів:

- Обираємо прості числа *p* та *q*.
- Обраховуємо модуль: $n = p \cdot q$
- 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.

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

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

Для розшифрування повідомлення використовується закритий ключ та формула:

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

Розглянемо приклад шифрування ІД номера 24 та всі варіанти розділення даного ІД на множники, щоб підтвердити гомоморфність по множенню даного шифру. Відкритий ключ у даному прикладі – (7, 33), а закритий ключ – (3, 33).

Розглянемо шифрування та дешифрування числа 24 та пар: 1 та 24, 2 та 12, 3 та 8, 4 та 6. Таким чином ми маємо 4 варіанти розділення даного бюлетеня на частини. Для зручності результати всіх операцій занесені до таблиці.

Значення	Шифрування	Множення	Дешифрування
24	$24^7 \bmod 33 = 18$	-	$18^3 \bmod 33 = 24$
1 та 24	$1^7 \bmod 33 = 1$ $24^7 \bmod 33 = 18$	$1 \times 18 = 18$	$18^3 \bmod 33 = 24$
2 та 12	$2^7 \bmod 33 = 29$ $12^7 \bmod 33 = 12$	$29 \times 12 = 348$	$348^3 \bmod 33 = 24$
3 та 8	$3^7 \bmod 33 = 9$ $8^7 \bmod 33 = 2$	$9 \times 2 = 18$	$18^3 \bmod 33 = 24$
4 та 6	$4^7 \bmod 33 = 16$ $6^7 \bmod 33 = 30$	$16 \times 30 = 480$	$480^3 \bmod 33 = 24$

Чим більше однакових множників фігурує в різних ІД номерах – тим ефективніше буде використання гомоморфного шифру по множенню. Наприклад, якщо найбільший ІД номер в нас 24 і виборець вирішить розділити бюлетень на 1 та 24, то ВК, яка отримає бюлетень з 24 чітко буде розуміти за якого кандидата відданий голос у даному бюлетені. В ідеалі кожному множнику повинно відповідати принаймні два кандидата. Ще більш ефективним способом організації Е-голосування з розділенням бюлетенів є використання шифрування з гомоморфністю по додаванню, що значно збільшить варіативність розділення бюлетенів.

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)*
- 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 $v=r$

Завдання:

Змоделювати протокол Е-голосування з розділенням комісії на незалежні частини будь-якою мовою програмування та провести його дослідження. Для кодування повідомлень використовувати метод RSA, 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 розділенням комісії на незалежні частини.
2. Які переваги та недоліки (порівняно з мінімальним протоколом та ідеальним) має алгоритм Е-протоколу з розділенням комісії на незалежні частини?
3. Які способи шахрайства можуть виникнути у алгоритмі Е-голосування з розділенням комісії на незалежні частини?
4. Опишіть алгоритм ЕЦП DSA.
5. Що являє собою явище гомоморфності в шифруванні? Яку роль грає гомоморфність шифрування в алгоритмах Е-голосування?
6. Опишіть алгоритм шифрування RSA. Чи є даний шифр гомоморфним?
7. Як можна вдосконалити наведений в теоретичних відомостях алгоритм Е-голосування з розділенням комісії на незалежні частини?
8. Що є основною перевагою даного протоколу Е-голосування порівняно із протоколами Е-голосування з посередниками (ВК, ЦВК, БР та ін.), що були розглянуті в попередніх лабораторних роботах? 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