**Міністерство освіти і науки України**

**Національний технічний університет України «Київський політехнічний**

**інститут імені Ігоря Сікорського"**

**Факультет інформатики та обчислювальної техніки**

**Кафедра інформатики та програмної інженерії**

**Звіт**

З лабораторної роботи № 6 з дисципліни

«Протоколи й алгоритми електронного голосування»

“**Протокол Е-голосування без підтвердження**”

| **Виконав(ла)** | *ІП-13 Бабіч Денис* |  |  |
| --- | --- | --- | --- |
|  | (шифр, прізвище, ім'я, по батькові) |  |  |

| **Перевірив(ла)** | *Нестерук А. О.* |  |  |
| --- | --- | --- | --- |
|  | (посада, прізвище, ім'я, по батькові) |  |  |

Київ 2024

**ЛАБОРАТОРНА РОБОТА № 6**

**Тема роботи**: Протокол Е-голосування без підтвердження.

**Мета роботи**: Дослідити протокол Е-голосування без підтвердження.

**Основне завдання:**

Змоделювати протокол Е-голосування без підтвердження будь-якою мовою програмування та провести його дослідження. Для кодування 6 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 підсумків?

**Виконання завдання:**

Для реалізації завдання було створено класи комісій, а саме реєстраційної комісії, яка відповідає за реєстрацію користувачів, видачу їм айді та передачу авторизаційного токену, а також виборчої комісії, яка займається прийомом голосів та створенням пар ключів для кожного виборця. Код цих класів можна побачити на рисунках 1.1 – 1.5.

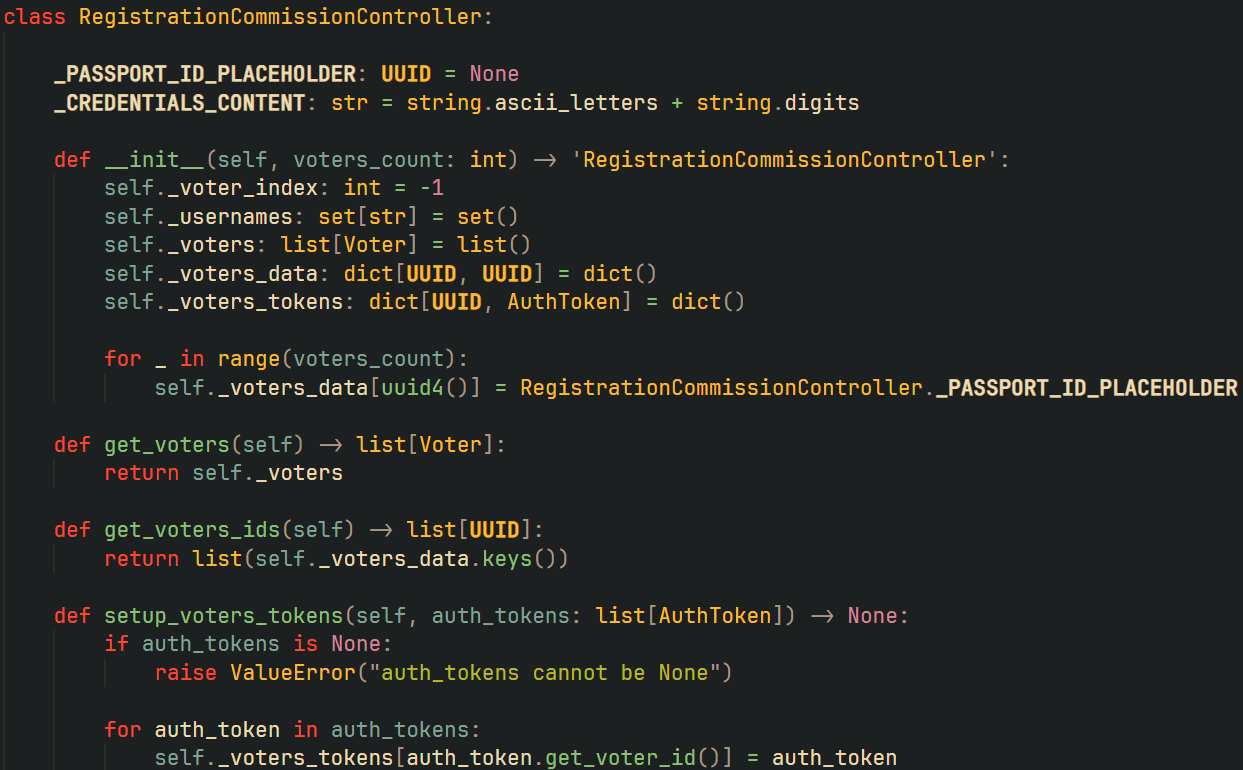


Рисунок 1.1 – Код класу реєстраційної комісії

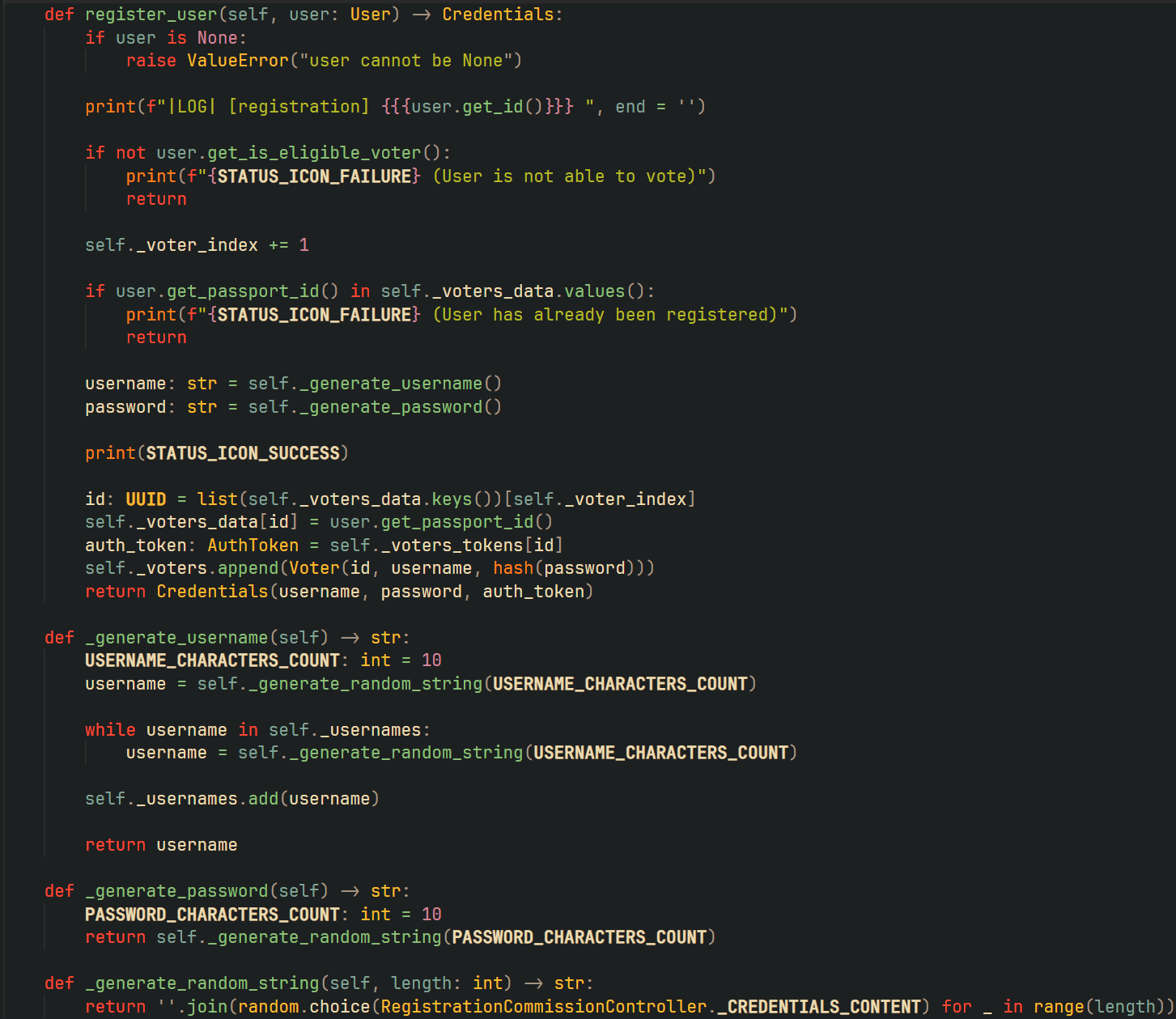


Рисунок 1.2 – Продовження класу реєстраційної комісії



Рисунок 1.3 – Код класу виборчої комісії

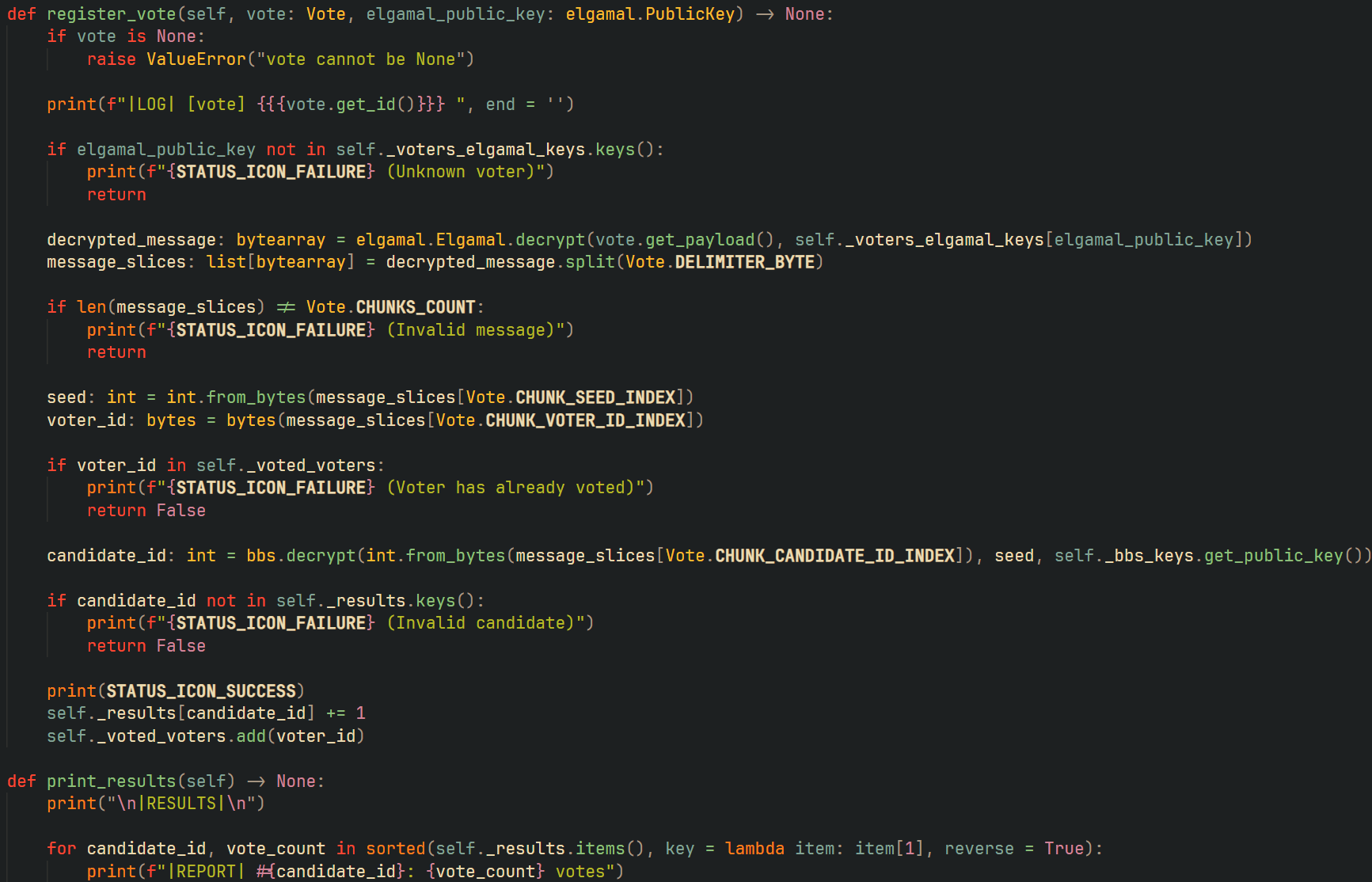


Рисунок 1.4 – Продовження класу виборчої комісії

Ще одним важливим класом є реалізація сервісу проведення електронного голосування, який має методи для авторизації користувачів та голосування. Код відповідного класу можна побачити на рисунках 1.5 – 1.6.

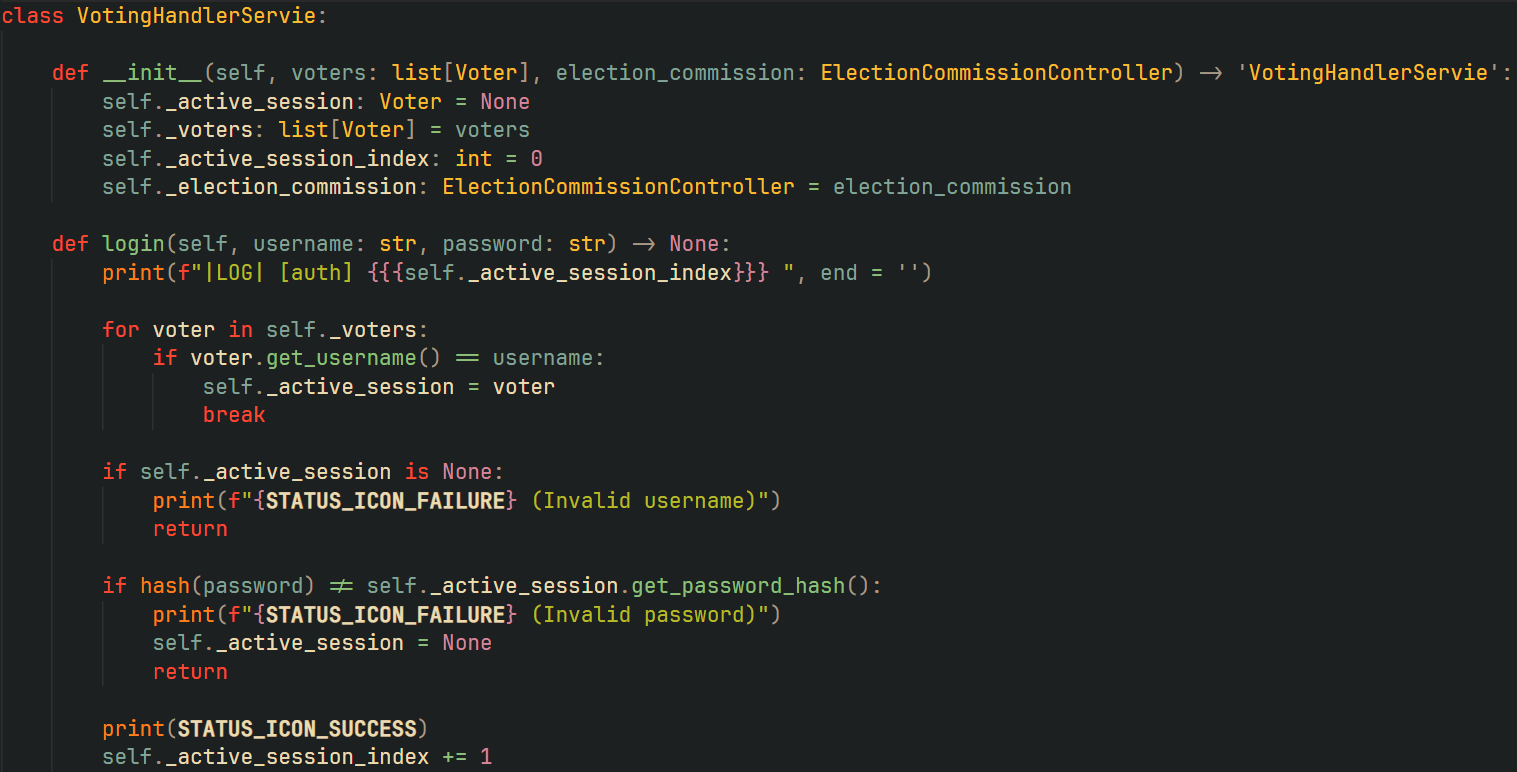


Рисунок 1.5 – Код класу сервісу проведення виборів



Рисунок 1.6 – Продовження класу сервісу проведення виборів

Бюлетень представлений за допомогою класу Vote та зберігає не лише айді кандидата за якого був відданий голос, а й форму-представлення повідомлення у байтах, відповідні зміщення за якими можна знайти необхідні поля для виборчої комісії.



Рисунок 1.7 – Код класу бюлетеня



Рисунок 1.8 – Код реалізації Blum Blum Shub

Реєстраційне комісія видає кожному користувачу відповідний токен автентифікації, який зберігає айді виборця, публічний ключ Ель-Гамаля, який генерується власний для кожного виборця і пару bbs ключів



Рисунок 1.9 – Код класу токену аунтефікації



Рисунок 1.10 – Код верифікації роботи протоколу



Рисунок 1.11 – Продовження коду верифікації роботи протоколу



Рисунок 1.12 – Продовження коду верифікації протоколу

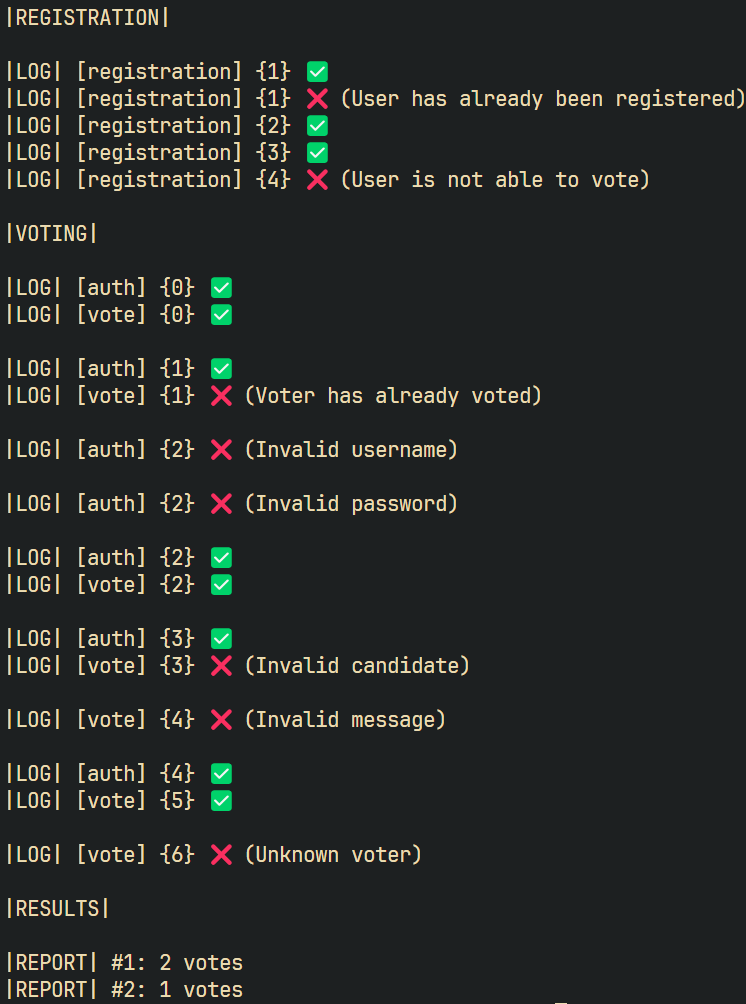


Рисунок 1.13 – Вивід логів симуляції голосування

**Дослідження протоколу:**

1. Перевірити чи можуть голосувати ті, хто не має на це права.

Ні, не можуть, оскільки реєстраційна комісія перед реєстрацією перевіряє чи має користувач право голосу. А виборча комісія не може приймати голос від незареєстрованих користувачів. Звісно, що можливі спроби шахраювання з боку комісій.

1. Перевірити чи може виборець голосувати кілька разів.

Ні, не може, оскільки у повідомленні разом з бюлетенем передається айді виборця і перед зарахуванням голосу перевіряється чи не голосував цей користувач до цього. Також не можна відкидати варіант з шахраюванням з боку комісій.

1. Чи може хтось (інший виборець, ВК, стороння людина) дізнатися за кого проголосували інші виборці?

Якщо перехопити такий бюлетень, то розшифрувати його можна лише з приватним ключем Ель-Гамаля, а також ключами BBS. Виборча комісія загалом може дізнатися хто за кого проголосував, але певний рівень анонімізації досягається завдяки ідентифікації виборця за айді, що приховує справжню особистість.

1. Перевірити чи може інший виборець чи стороння людина проголосувати замість іншого зареєстрованого виборця.

Це можливо у випадку отримання доступу до ідентифікаційного токену іншого користувача та якщо проголосувати раніше за цього виборця.

1. Чи може хтось (інший виборець, ВК, стороння людина) таємно змінити голос в бюлетені?

Інший виборець не може цього зробити у випадку перехоплення, оскільки для цього потрібно розшифрувати повідомлення та знати його структуру. Проте, виборча комісія може легко змінити голос виборця, або віддати його іншому кандидату, оскільки не публікуються бюлетені.

1. Чи може виборець перевірити, що його голос врахований при підведенні кінцевих підсумків?

Ні, оскільки не публікуються фінальний список бюлетенів.

**Висновок:**

У результаті виконання лабораторної роботи було змодельовано протокол електронного голосування без підтвердження, який забезпечує базові вимоги до безпеки та конфіденційності голосування. В процесі моделювання реалізовано систему реєстрації виборців, захист даних за допомогою методів Ель-Гамаля для шифрування повідомлень і BBS-генератора для створення бюлетенів, а також протестовано різні сценарії порушення протоколу.

Аналіз протоколу виявив як його сильні, так і слабкі сторони. Зокрема, протокол успішно блокує доступ до голосування незареєстрованих виборців та сторонніх осіб, проте не гарантує абсолютної анонімності голосування, оскільки виборча комісія має доступ до зашифрованих бюлетенів і може ідентифікувати виборців через їхній ID. Важливо зазначити, що виборці не мають можливості підтвердити врахування своїх голосів, що може знижувати рівень довіри до системи. Також залишається ризик маніпуляцій з боку виборчої комісії, оскільки вона має доступ до бюлетенів і може змінювати результати.

Загалом, виконана робота демонструє базові реальні принципи реалізації електронного голосування та підкреслює ключові аспекти, які потребують подальшого вдосконалення. Для підвищення надійності системи варто впровадити додаткові механізми прозорості, такі як публікація зашифрованих бюлетенів для аудиту, або використання криптографічних методів, що дозволяють перевірити врахування голосів без порушення їхньої конфіденційності.