**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 № 1 з дисципліни

«Протоколи й алгоритми електронного голосування»

“**Простий протокол Е-голосування**”

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

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

Київ 2024

**ЛАБОРАТОРНА РОБОТА № 1**

**Тема роботи**: Простий протокол Е-голосування.

**Мета роботи**: Дослідити протокол простого Е-голосування.

**Основне 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
4. кого проголосували інші виборці?
5. Перевірити чи може інший виборець чи стороння людина проголосувати замість іншого зареєстрованого виборця.
6. Чи може хтось (інший виборець, ЦВК, стороння людина) таємно змінити голос в бюлетені?
7. Чи може виборець перевірити, що його голос врахований при підведенні кінцевих результатів?

**Виконання завдання:**

Сам бюлетень голосування представлений у вигляді класів VoteRecordPayload та SignedVoteRecord, де клас VoteRecordPayload представляє протокол без rsa-підпису, у якому зберігається айді кандидата, за який був відданий голос та контрольна хеш-сума на основі цього значення. Також реалізований алгоритм гамування через інтерфейс IGammaEncryptor. Повний код можна побачити на рисунку 1.1.



Рисунок 1.1 – Код класу VoteRecordPayload

Клас SignedVoteRecord фактично є класом-обгорткою навколо VoteRecordPayload, у якому через композицію зберігається посилання на об’єкт VoteRecordPayload і додається власне поле електронного цифрового підпису (ЕЦП). Повний код можна побачити на рисунку 1.2.

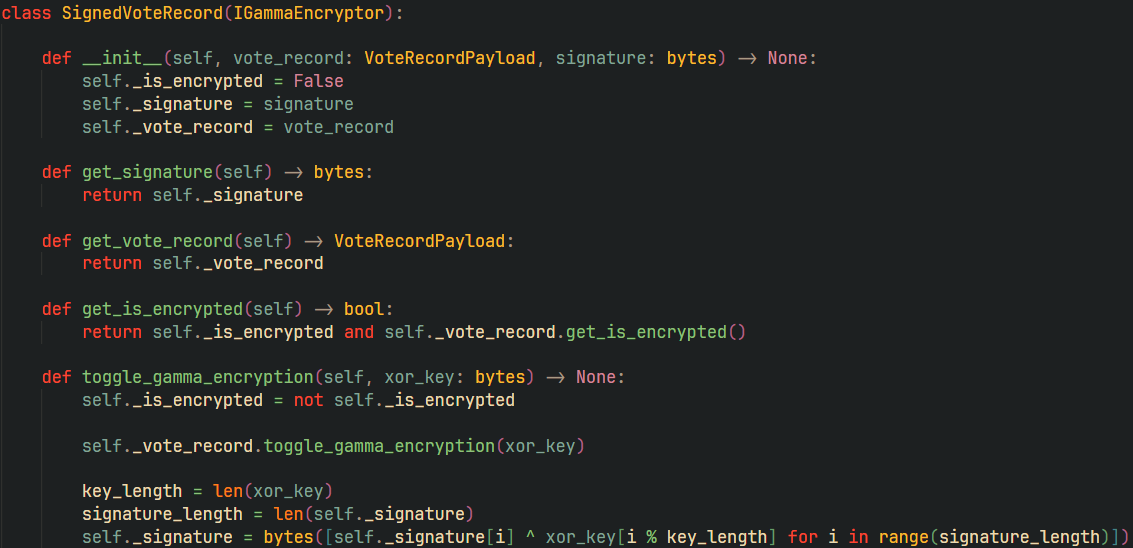
****

Рисунок 1.2 – Повний код класу SignedVoteRecord

Виборець реалізований за допомогою класу VoterController, у якому зберігаються айді, прапорець можливості голосування, приватне поле закритого rsa-ключа, публічне поле відкритого ключа. У цього контролеру є метод vote, який створює протокол без підпису з занесеним значення кандидата та метод sign, який створює підписаний бюлетень, створюючи ЕЦП на основі значення айді кандидата, за якого виборець віддав голос. Варто також згадати про використання перечислення VoterDebugMode, який використовуватиметься під час тестування різних сценаріїв проведення голосування. Повний код класу VoterController можна побачити на рисунку 1.3.

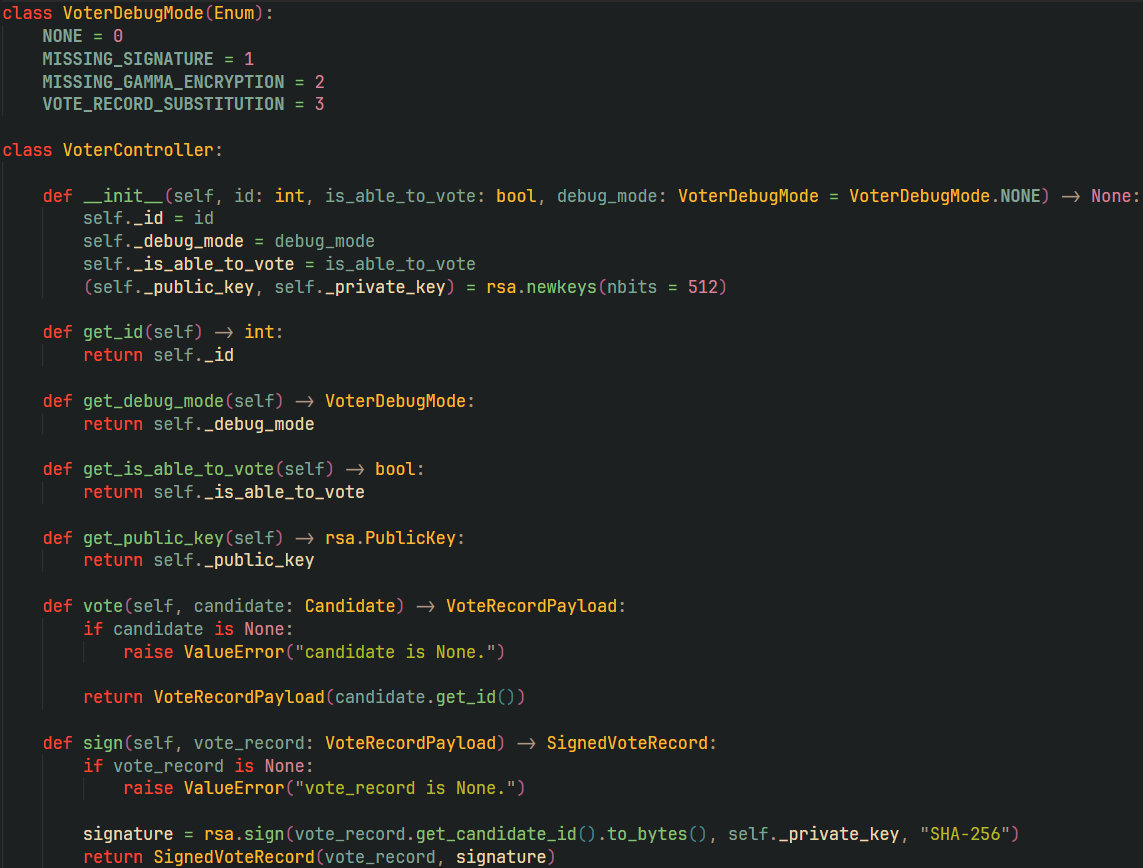
****

Рисунок 1.3 – Код класу VoterController

Останнім важливим класом є CommissionController, який представляє ЦВК та має поле ключа гамування, яким шифруються бюлетені перед відправкою, словник, у який відбувається підрахунок голосів, список верифікованих виборців та 2 важливі методи, а саме process\_voter та register\_vote. Метод process\_voter відповідає за верифікацію виборця та створення протоколу (рис. 1.4). За допомогою \_verfiy\_voter відбувається валідація людини, а саме перевірка чи має виборець можливість голосувати й чи не голосував виборець до цього (рис. 1.5). Метод \_create\_protocol відповідає за роботу над створенням бюлетеню (ініціалізація, підпис, шифрування гамування), де використовуються значення з перечислення VoterDebugMode для реалізації різних сценаріїв поведінки, а саме відсутність підпису, відсутність шифру гамування та спроба підміни голосу. Повний код методу \_create\_protocol можна побачити на рисунку 1.6.

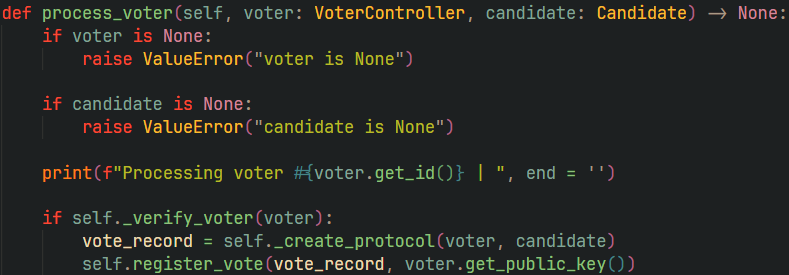
****

Рисунок 1.4 – Код методу process\_voter

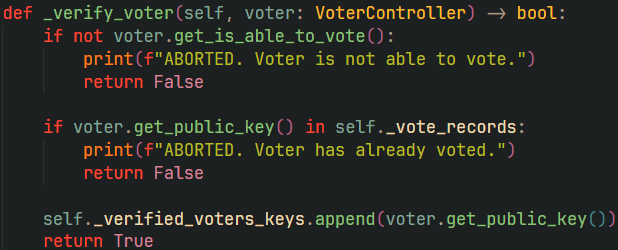


Рисунок 1.5 – Код методу \_verify\_voter

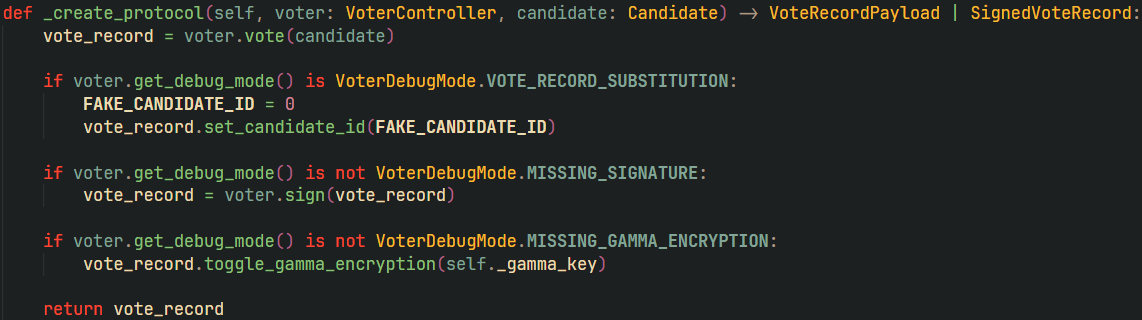


Рисунок 1.6 – Код методу \_create\_protocol

Ще одним важливим методом є register\_vote, у якому бюлетень і зараховується у фінальний результат та у випадку виявлення порушення голос відкидається. Відбуваються наступні перевірки: наявність шифру гамування, чи підписаний бюлетень, чи був валідований виборець з відповідним публічним ключем, після дешифрування алгоритму гамування перевіряється хеш-сума бюлетеня та верифікація rsa-підпису й зарахування голосу (рис. 1.7)

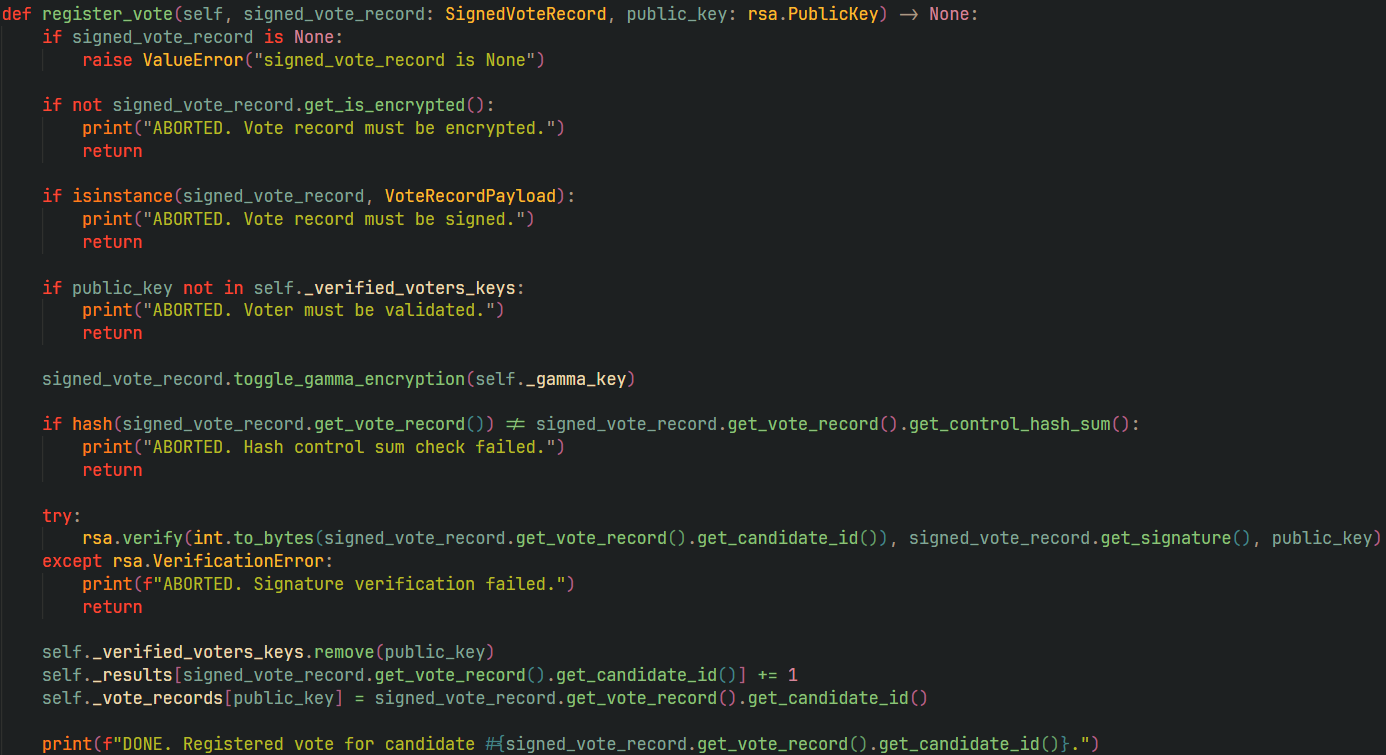
****

Рисунок 1.7 – Код методу register\_vote

Вміст модуля main можна побачити на рисунку 1.8.



Рисунок 1.8 – Код у модулі main

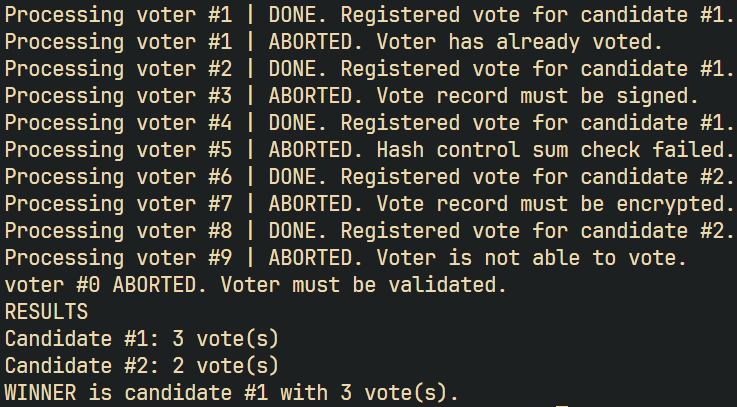


Рисунок 1.9 – Отриманий вивід

**Дослідження протоколу:**

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

Ні, не можуть, оскільки перед цим відбувається валідація у методі process\_voter. Навіть у випадку, якщо цей бюлетень просто кинути без верифікації, як це робить voter\_0, то голос не буде зарахований, оскільки користувач не знаходиться у списку верифікованих виборців. Але потрібно довіряти ЦВК, оскільки вона має можливість фальсифікувати етап валідації виборця.

1. Перевірити чи може виборець голосувати кілька разів.

Ні, не може, оскільки зберігається список відкритих ключів виборців, які проголосували і на етапі валідації нового відбувається його валідація завдяки перевірці списку на наявність ключа поточного виборця. Але потрібно довіряти ЦВК, оскільки вона має можливість фальсифікувати етап валідації виборця.

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

Оскільки це простий алгоритм голосування, то ЦВК знає за кого проголосував кожен виборець за замовчуванням. Та й загалом всім відомо ключ шифрування гамування ЦВК, тому у випадку перехоплення такого бюлетеня він може бути легко розсекречений.

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

Ні, оскільки кожен бюлетень підписується електронним підписом, що гарантує приналежність бюлетеня до людини, яка його підписала.

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

У ЦВК є повнота прав над бюлетенем у моменті, коли він потрапив до неї, тому голос може бути перенаправлений за іншого кандидата. Проте, бюлетень неможливо змінити у випадку перехоплення, оскільки не буде співпадати хеш-сума повідомлення на етапі валідації бюлетеня.

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

Ця функція не передбачена простим протоколом голосування. Проте, її досить просто реалізувати шляхом перевірки наявності відкритого ключа користувача у списку ключів виборців, які проголосували.

**Висновок:**

У ході виконання лабораторної роботи було змодельовано та досліджено простий протокол електронного голосування. Основним завданням було реалізувати модель голосування з використанням алгоритмів RSA для електронного підпису та гамування для шифрування повідомлень, а також провести дослідження різних сценаріїв, що можуть виникати в процесі голосування.

Під час дослідження було встановлено, що протокол надійно перевіряє, чи має виборець право голосувати, а користувачі, які не пройшли верифікацію, не можуть подати свій голос. Також кожен виборець може проголосувати лише один раз, і це забезпечується перевіркою відкритого ключа. Протокол захищений від можливості проголосувати замість іншого виборця, оскільки кожен бюлетень підписується унікальним електронним підписом виборця і голос неможливо змінити без порушення хеш-суми, що гарантує захист від несанкціонованої модифікації при перехопленні бюлетеня. Проте, ЦВК має можливість змінити бюлетень після його дешифрування, що є загальною вразливістю цього протоколу.

Таким чином, даний протокол має базові функції захисту й верифікації, однак не може повністю гарантувати анонімність та захищеність голосів від ЦВК. Це дозволяє зробити висновок, що для реальних систем електронного голосування слід впроваджувати додаткові заходи безпеки, які захистять як таємницю голосування, так і результат голосування від втручання сторонніх осіб чи організацій.