# Лабораторна робота №4

**Тема:** Протокол Е-голосування з перемішуванням

**Мета:** Дослідити протокол Е-голосування з перемішуванням

**Теоретичні відомості:**

Протокол Е-голосування з перемішуванням також відомий як голосування без центральної виборчої комісії, що відповідно означає, що ВК в ньому не використовується, а виборці проводять голосування самостійно, слідкуючи за дотриманням протоколу та запобігаючи шахраюванню. Головним недоліком такого протоколу Е-голосування є те, що чим більше виборців бере участь у голосуванні, тим більш складна буде реалізація голосування. Процедура Е-голосування з перемішуванням не є доцільною (обмежень по кількості виборців протокол не має, зростає лише складність), якщо у процесі бере участь більше 5-ти виборців, оскільки це значно ускладнить протокол.

Загальний вигляд протоколу Е-голосування з перемішуванням:

- Бажаючі проголосувати формують список виборців.
- Виборці створюють бюлетені та зашифровують їх за встановленими правилами (спочатку бюлетень шифрується ключами в спадаючому порядку, далі перед кожним шифруванням до отриманого шифротексту додається випадковий рядок. Другий етап також шифрується ключами в спадаючому порядку).
- Всі виборці надсилають свої зашифровані бюлетені першому виборцю.
- Перший виборець розшифровує всі бюлетені своїм ключем та видаляє випадкові рядки, впевнюється, що його бюлетень присутній, перемішує всі бюлетені та надсилає наступному виборцю за списком по зростанню. Кожен наступний виборець повторює ті ж дії, доки не дійде до останнього. Після цього всі бюлетені знову надсилаються першому виборцю за списком.

- Перший виборець розшифровує всі отримані бюлетені, перевіряє присутність свого бюлетеня, підписує всі бюлетені та надсилає їх всім учасникам Е-голосування. Кожен наступний виборець по списку за зростанням перевіряє вірність ЕЦП попереднього виборця та повторює ті ж дії з бюлетенями. Останній виборець надсилає підписаний результат всім виборцям.
- Всі виборці перевіряють ЕЦП та впевнюються, що їх бюлетені присутні.
- З усіх бюлетенів видаляються випадкові рядки та підраховуються результати.

Розглянемо протокол Е-голосування з перемішуванням детальніше. Нехай в ньому беруть участь 4 виборці: A, B, C та D, які ведуть голосування з двома варіантами голосу (вибору: вибір1 та вибір2), та мають свої відкриті та закриті ключі. Розглянемо етапи реалізації такого голосування:

- Кожен виборець формує свій Е-бюлетень, після чого робить наступне:
    - Додає до свого Е-бюлетеня довільний рядок, зберігає рядок.
    - Шифрує результати попереднього етапу відкритим ключем D.
    - Шифрує результати попереднього етапу відкритим ключем C.
    - Шифрує результати попереднього етапу відкритим ключем B.
    - Шифрує результати попереднього етапу відкритим ключем A.
    - Додає новий випадковий рядок до результату попереднього етапу та шифрує отримане відкритим ключем D. Він записує даний випадковий рядок.
    - Додає новий випадковий рядок до результату попереднього етапу та шифрує отримане відкритим ключем C. Він записує даний випадковий рядок.
    - Додає новий випадковий рядок до результату попереднього етапу та шифрує отримане відкритим ключем B. Він записує даний випадковий рядок.

- Додає новий випадковий рядок до результату попереднього етапу та шифрує отримане відкритим ключем A. Він записує даний випадковий рядок. (Якщо виразити функцію шифрування як *Fc*, випадковий рядок як *Rs*, Е-бюлетень як *Ev*, то повідомлення на даному кроці буде мати наступний вигляд: $Fc_A(Rs_5, Fc_B(Rs_4, Fc_C(Rs_3, Fc_D(Rs_2, Fc_A(Fc_B(Fc_C(Fc_D(Ev, Rs_1)))))))$. Кожен виборець зберігає результати кожного з проміжних етапів обрахунку, які будуть використані в подальших етапах протоколу.)

- Кожен виборець надсилає отримане повідомлення до A.
- A розшифровує всі бюлетені за допомогою свого закритого ключа та видаляє випадкові рядки на даному рівні.
- A перемішує зашифровані бюлетені та надсилає їх B. (На даному етапі повідомлення стало коротшим на один рівень і виглядає наступним чином: $Fc_B(Rs_4, Fc_C(Rs_3, Fc_D(Rs_2, Fc_A(Fc_B(Fc_C(Fc_D(Ev, Rs_1)))))))$)
- B розшифровує всі бюлетені своїм закритим ключем та перевіряє чи є серед них його бюлетень. Після чого він видаляє всі випадкові рядки на даному рівні, перемішує ці, все ще зашифровані, бюлетені та надсилає результат C. (На даному етапі повідомлення стало коротшим на один рівень і виглядає наступним чином: $Fc_C(Rs_3, Fc_D(Rs_2, Fc_A(Fc_B(Fc_C(Fc_D(Ev, Rs_1)))))))$)
- C розшифровує всі бюлетені своїм закритим ключем та перевіряє чи є серед них його бюлетень. Після чого він видаляє всі випадкові рядки на даному рівні, перемішує ці, все ще зашифровані, бюлетені та надсилає результат D. (На даному етапі повідомлення стало коротшим на один рівень і виглядає наступним чином: $Fc_D(Rs_2, Fc_A(Fc_B(Fc_C(Fc_D(Ev, Rs_1))))))$)
- D розшифровує всі бюлетені своїм закритим ключем та перевіряє чи є серед них його бюлетень. Після чого він видаляє всі випадкові рядки на даному рівні, перемішує ці, все ще зашифровані, бюлетені та

надсилає результат A. (На даному етапі повідомлення стало коротшим на один рівень і виглядає наступним чином: $Fc_A(Fc_B(Fc_C(Fc_D(Ev, Rs_1)))))$)

- A розшифровує всі бюлетені своїм закритим ключем та перевіряє чи є серед них його бюлетень. Після чого він підписує результат, перемішує бюлетені та надсилає результат B, C та D. (На даному етапі повідомлення виглядає наступним чином: $S_A(Fc_B(Fc_C(Fc_D(Ev, Rs_1)))))$)
- B перевіряє та видаляє ЕЦП A, потім розшифровує всі бюлетені своїм закритим ключем та перевіряє чи є серед них його бюлетень. Після чого він підписує результат, перемішує бюлетені та надсилає результат A, C та D. (На даному етапі повідомлення виглядає наступним чином: $S_B(Fc_C(Fc_D(Ev, Rs_1))))$)
- C перевіряє та видаляє ЕЦП B, потім розшифровує всі бюлетені своїм закритим ключем та перевіряє чи є серед них його бюлетень. Після чого він підписує результат, перемішує бюлетені та надсилає результат A, B та D. (На даному етапі повідомлення виглядає наступним чином: $S_C(Fc_D(Ev, Rs_1)))$)
- D перевіряє та видаляє ЕЦП C, потім розшифровує всі бюлетені своїм закритим ключем та перевіряє чи є серед них його бюлетень. Після чого він підписує результат, перемішує бюлетені та надсилає результат A, B та C. (На даному етапі повідомлення виглядає наступним чином: $S_D(Ev, Rs_1)$)
- A, B та C перевіряють та видаляють ЕЦП D. Всі впевнюються, що їх бюлетені все ще присутні у цьому наборі.
- Зі всіх бюлетенів видаляються довільні рядки та підраховуються результати голосування.

Цей протокол працює досить надійно та дозволяє виявити спроби шахрайства одного з учасників голосування. На відміну від інших попередніх розглянутих протоколів Е-голосування, протоколу з перемішуванням не

потрібна третя «довірена» сторона у вигляді ЦВК, ВК чи БР. Розглянемо сценарії порушення протоколу.

Припустимо, що хтось хоче добавити зайвий бюлетень до загальної групи. В такому випадку перший виборець помітить, що йому було надіслано більше бюлетенів, ніж є виборців. У випадку ж якщо це зробить хтось вже після початку поетапного розшифрування, то зайвий бюлетень помітить наступний виборець.

Ще одним варіантом шахрайства є підміна бюлетеня. Оскільки бюлетень шифрується багатьма відкритими ключами, то кожен може зробити стільки правильних бюлетенів, скільки йому потрібно. Протокол розшифрування складається з двох частин: перша частина це кроки 3-7, друга частина це кроки 8-11. Якщо хтось спробує замінити бюлетень на другому етапі, то шахрайство буде виявлене одразу, оскільки кожен крок бюлетені підписуються та надсилаються всім виборцям. Відповідно кожен виборець може перевірити чи знаходиться його бюлетень досі в процесі. У випадку порушення протоколу таким способом виборець може припинити процес виконання протоколу. Підміна бюлетеня в першій частині протоколу розшифрування може бути успішною, але шахрайство все ж виявиться при переході у другу фазу. В нашому випадку в нас є 4 виборця, якщо підміну зробить A, то B, C та D помітять заміну свого бюлетеня ще на першому етапі. Але якщо виборець A буде чесним і підміну виконає виборець B, то в нього є шанс підмінити бюлетень виборця A, який не буде виявлений до другого етапу. Але якщо він замінить бюлетень C чи D, то заміна буде розкрита ще на першому етапі (виборці можуть розпізнати лише свій бюлетень, кому належить решта бюлетенів - невідомо).

Ще одна річ, яку може бажати вчинити зловмисник, це дізнатися власників отриманих E-бюлетенів (хто за кого проголосував). Через перестановку бюлетенів ніхто не зможе виконати протокол у зворотному напрямку та пов’язати отримані бюлетені з конкретними виборцями. Видалення

випадкових рядків також допомагає зберегти анонімність виборців. Якщо ці рядки будуть лишатися, то за допомогою повторного шифрування бюлетенів можна інвертувати перемішування голосів. Самі ж випадкові рядки потрібні протоколу для того, щоб навіть однакові бюлетені в зашифрованому вигляді виглядали по різному на кожному етапі протоколу.

Головним недоліком даного протоколу є те, що для його реалізації потрібно виконати велику кількість обрахунків. До того ж чим більше виборців приймає участь у голосуванні, тим складніше відбувається реалізація протоколу. В реальних виборах участь будуть брати мільйони виборців, що робить даний протокол непридатним для виконання у таких умовах.

Ще одним дрібним недоліком виборів є те, що один з виборців (той, хто буде виконувати останній пункт протоколу, в нашому випадку це виборець D) дізнається результати виборів раніше за інших. Це звичайно на хід виборів не вплине, оскільки виборці після кожного етапу перевіряють свій бюлетень, але надає певну перевагу виборцю D. Наприклад, уявимо ситуацію, що голосування призведе до падіння чи росту акцій певної компанії, то виборець D зможе до оголошення результату продати свою долю акцій чи навпаки купити їх, щоб отримати вигоду. З іншого боку те ж саме може зробити і ЦВК, оскільки вони також першими дізнаються результати виборів.

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 це сукупність *(p, g, y)*, закритий ключ це *x*

Для створення підпису виконуємо наступні дії:

- Створюємо хеш-дайджест повідомлення *M*: $m = h(M)$
- Створюємо випадкове число *k*, яке повинне бути випадковим цілим числом *1<k<p-1*, так щоб бути взаємнопростим з *p-1* і обчислюється $r = g^k \bmod p$
- Обчислюємо число $s = (m - xr)k^{-1} \bmod (p-1)$
- Підписом повідомлення *M* вважається пара *(r, s)*

Перевіряється даний підпис за допомогою відкритого ключа *(p, g, y)* та підпису *(r, s)*:

- Перевіряється дві умови *0<r<p* і *0<s<p-1*. Якщо хоча б одна з них не виконується, то підпис вважається недійсним.
- Обчислюється хеш-дайджест $m = h(M)$
- Підпис вважається справжнім, якщо виконується рівність: $y^r r^s = g^m \bmod p$

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.

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 чисел *(e, n)* – відкритий ключ, а *(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:

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

**Завдання:**

Змоделювати протокол Е-голосування з перемішуванням будь-якою мовою програмування та провести його дослідження. Для кодування повідомлень використовувати метод RSA, для реалізації ЕЦП використовувати алгоритм Ель-Гамаля.

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 перемішуванням.
2. Які переваги та недоліки (порівняно з мінімальним протоколом та ідеальним) має алгоритм Е-протоколу з перемішуванням?
3. Які способи шахрайства можуть виникнути у алгоритмі Е-голосування з перемішуванням?
4. Опишіть алгоритм ЕЦП Ель-Гамаля.
5. Опишіть алгоритм шифрування RSA.
6. Опишіть особливості Е-протоколу з перемішуванням.
7. Які переваги та недоліки має протокол з перемішуванням порівняно з протоколами з посередниками.

**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