# ЛАБОРАТОРНА РОБОТА № 4. АЛГОРИТМ ОБМІНУ КЛЮЧАМИ ДІФФІ-ХЕЛЛМАНА

## 4.1 Мета роботи

Отримати навички безпечного обміну ключами по каналу зв'язку, які надалі можуть бути використані в якомусь алгоритмі шифрування. Реалізувати програмно (на будь-якій мові програмування) роботу алгоритму Діффі-Хеллмана [5].

## 4.2 Теоретичні відомості

Сам алгоритм Діффі-Хеллмана може застосовуватися тільки для обміну ключами.

Алгоритм заснований на труднощі обчислень дискретних логарифмів. Дискретний логарифм визначається наступним чином. Вводиться поняття примітивного кореня простого числа Q як числа, чиї ступені створюють всі цілі від 1 до Q – 1. Це означає, що якщо A є примітивним коренем простого числа Q, тоді числа A mod Q, $A^2$ mod Q, . . . , $A^{Q-1}$ mod Q є різними і складаються з цілих від 1 до Q – 1 з деякими перестановками. У цьому випадку для будь-якого цілого Y <Q і примітивного кореня A простого числа Q можна знайти єдину експоненту X, таку, що $Y = A^X \bmod Q$, где $0 \leq X \leq (Q - 1)$

Експонента X називається дискретним логарифмом, або індексом Y, на підставі A mod Q. Це позначається як

$$\mathrm{ind}_{A,\,Q}(Y).$$

### 4.2.1 Алгоритм обміну ключами Діффі-Хеллмана

Загальновідомі елементи:

Q – просте число

A – примітивний корінь Q, A<Q

Створення пари ключів користувачем B:

– вибір випадкового числа $X_B$ (закритий ключ), $X_B<Q$

– знаходження числа $Y_B$ (відкритий ключ), $Y_B=A^{X_B} \bmod Q$

Створення пари ключів користувачем C:

– вибір випадкового числа $X_C$ (закритий ключ), $X_C<Q$

– знаходження числа $Y_C$ (відкритий ключ), $Y_C=A^{X_C} \bmod Q$

Створення загального секретного ключа користувачем B:

$$K=(Y_C)^{X_B} \bmod Q$$

Створення загального секретного ключа користувачем C:

$$K=(Y_B)^{X_C} \bmod Q$$

Передбачається, що існують два відомі всім числа: просте число Q і ціле A, яке є примітивним коренем Q. Припустимо, що користувачі B і C хочуть обмінятися ключем для алгоритму симетричного шифрування. Користувач B вибирає випадкове число $X_B<Q$ і обчислює $Y_B = A^{X_B} \bmod Q$. Аналогічно користувач C незалежно вибирає випадкове ціле число $X_C<Q$ і обчислює $Y_C=A^{X_C} \bmod Q$. Кожна сторона тримає значення X в секреті і робить значення Y доступним для іншої сторони. Тепер користувач B обчислює ключ як $K=(Y_C)^{X_B} \bmod Q$, і користувач C обчислює ключ як $K=(Y_B)^{X_C} \bmod Q$. В результаті обидва отримають одне і те ж значення.

Таким чином, дві сторони обмінялися секретним ключем. Так як $X_B$ і $X_C$ є закритими, противник може отримати тільки наступні значення: Q, A, $Y_B$ і $Y_C$. Для обчислення ключа атакуючий повинен зламати дискретний логарифм, тобто обчислити $X_C = \text{ind } a, q\ (Y_C)$.

Безпека обміну ключами в алгоритмі Діффі-Хеллмана випливає з того факту, що, хоча відносно легко обчислити експоненти по модулю простого числа, дуже важко вирахувати дискретні логарифми. Для великих простих чисел завдання вважається нерозв'язним.

Слід зауважити, що даний алгоритм уразливий для атак типу "man-in-the-middle". Якщо противник може здійснити активну атаку, тобто має можливість

не тільки перехоплювати повідомлення, а й замінювати їх іншими, він може перехопити відкриті ключі учасників $Y_B$ і $Y_C$, створити свою пару відкритого та закритого ключа і послати кожному з учасників свій відкритий ключ. Після цього кожен учасник обчислить ключ, який буде спільним з противником, а не з іншим учасником. Якщо немає контролю цілісності, то учасники не зможуть виявити подібну підміну.

## 4.3 Завдання до виконання роботи

– створити програмну реалізацію алгоритму обміну ключами Діффі-Хеллмана;

– реалізувати чат для трьох і більше користувачів;

– створити приємний та зрозумілий інтерфейс для перевірки зробленої роботи;

– сформувати звіт в електронному вигляді.

## 4.4 Зміст звіту

– титульний лист;

– мету лабораторної роботи;

– завдання і тексти програм;

– результати виконання програм;

– висновки.

## 4.5 Контрольні питання

1. Для чого створені алгоритми обміну ключами?
2. Що мається на увазі під поняттям примітивного кореня простого числа?
3. Як створюються пари ключем для обох сторін?
4. З чого виходить, що обмін ключами по алгоритму Діффі-Хеллмана вважається безпечним?
5. Що таке атака типу "man-in-the-middle"?