# КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ імені ТАРАСА ШЕВЧЕНКА



## ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

**Кафедра прикладних інформаційних систем**

**Звіт до лабораторної роботи №14**

# з курсу

**«Безпека мереж і комп’ютерних систем»**

*Студента 2 курсу*

*групи ПП-21 спеціальності 122 «Комп'ютерні науки» ОП «Прикладне програмування»*

%username%

*Викладач:*

проф. Сайко В.Г.

## Київ – 202

**1.Назва роботи**

Схеми обміну ключами симетричних криптосистем з використанням асиметричного шифрування. Схема Діффі-Хеллмана.

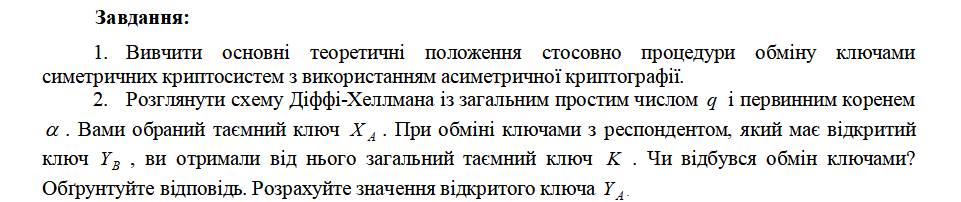
1. **Тема роботи**

Схеми обміну ключами симетричних криптосистем з використанням асиметричного шифрування. Схема Діффі-Хеллмана.

1. **Мета роботи**

Розглянути базові схеми, що реалізують обмін сеансовими ключами за допомогою асиметричних криптоперетворень. Засвоїти реалізацію обміну ключами з використанням еліптичних кривих. Ознайомитися зі схемою Діффі-Хеллмана.

1. **Умова завдання**



1. **Рішення**

Використаємо класичний приклад: Аліса і Боб таємно обирають два випадкових цілих(!) числа sA та sB в інтервалі [0, |G| − 1]. Потім вони таємно обчислють aA = gsA та aB = gsB відповідно, та обмінюються ними (цю передачу можливо відслідкувати). Після цього Аліса обчислює aBA = aBsA = gsBsA, а Боб - aAB = aAsB = gsAsB. При цьому aAB = aBA, тому це число є спільним таємним ключем K для обох.

Отже, тепер Аліса та Боб можуть скористатись відображенням елементів множини G у простір іншої криптосистеми. Наприклад, вони можуть використати блок даних необхідного розміру (зокрема, молодші біти) значення aAB як ключ звичайної блочної криптосистеми.

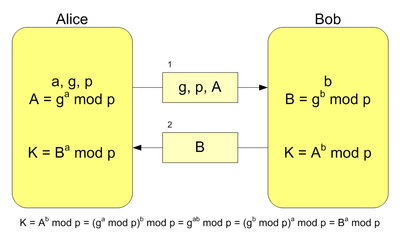


Схема передачі параметрів

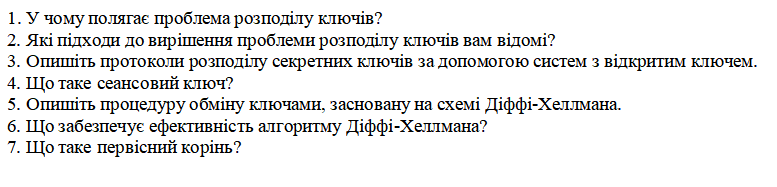
Якщо навести конкретний приклад, то стане зрозуміло, що при

s = 2 - секретний ключ; g = 5 - відкрите просте число; p = 23 - відкрите просте число;

a = 6 - секретний ключ Аліси; A = ga mod p (8) - відкритий ключ Аліси;

b = 15 - секретний ключ Боба та B = gb mod p (19) - відкритий ключ Боба, Аліса та Боб знають усі параметри, окрім секретних ключів одне одного, а сторонній спостерігач, який не втручається у передачу даних, знає усі параматри, окрім усіх секретних ключів (включаючи s, спільний для Боба і Аліси).

**Контрольні запитання:**



1. Протокол вразливий для [атаки «людина посередині»](https://uk.wikipedia.org/wiki/%D0%90%D1%82%D0%B0%D0%BA%D0%B0_%C2%AB%D0%BB%D1%8E%D0%B4%D0%B8%D0%BD%D0%B0_%D0%BF%D0%BE%D1%81%D0%B5%D1%80%D0%B5%D0%B4%D0%B8%D0%BD%D1%96%C2%BB" \o "Атака «людина посередині»). Припустімо, що зловмисник *C* здатен здійснювати підміну повідомлень, якими обмінюються Аліса та Боб. Тоді він може згенерувати числа *s\*A* та *s\*B*, і відповідно, отримати два узгоджених ключа: *gsAs\*B* та *gs\*AsB*. В результаті зловмисник отримує можливість повністю контролювати обмін повідомленнями між Алісою та Бобом. При цьому вони не здатні виявити підміну та вважатимуть, що зв'язуються один з одним.
2. Попереднє поширення сертифікатів,

Протоколи MTI,

Відкритий розподіл ключів із використанням автопідписаних ключів,

Протокол KEA,

Протокол «уніфікована модель»,

Протокол MQV або автентифікація абонентів.

1. Припустимо, що А і В вже обмінялися відкритими ключами. Далі слід виконати наступні дії:

1. Сторона А використовує відкритий ключ сторони В, щоб переслати стороні В шифроване повідомлення, що містить ідентифікатор і оказію, що використовується для ідентифікації даної конкретної транзакції.

2. Користувач В посилає повідомлення користувачу А, зашифроване за допомогою і що містить отриману від нього оказію і нову оказію , згенеровану користувачем В.

3. Сторона А повертає , шифруючи повідомлення відкритим ключем сторони В, щоб гарантувати їй, що його респондентом є сторона А.

4. Учасник А вибирає таємний ключ і посилає учаснику В повідомлення . Шифрування цього повідомлення відкритим ключем сторони В гарантує, що тільки учасник В зможе прочитати його, а шифрування особистим ключем учасника А - що тільки учасник А міг послати його.

5. Сторона В обчислює , щоб відтворити таємний ключ.

У результаті при обміні таємними ключами ця схема гapaнтує як конфіденційність, так і автентифікацію.

1. Ключ, що створюється на основі секретного ключа однієї сторони та відкритого ключа іншої.
2. Користувач А вибирає випадкове ціле число і обчислює **. Таким самим чином користувач В незалежно вибирає випадкове ціле число і обчислює *.* Кожна сторона зберігає значення  в таємниці та робить значення  доступним іншій стороні. Користувач А обчислює ключ за формулою , а користувач В - за формулою *.* Ці дві формули обчислення дають однакові результати, як показано нижче



.

1. Щоб визначити ключ, зновмиснику доведеться вираховати дискретний логарифм.
2. Первісний корінь за модулем m - це ціле число g таке, що:

IMG_256, IMG_256 при IMG_256 де IMG_256 - функція Ейлера.

**Висновки**

В результаті виконання даної лабораторної роботи я розглянув базові схеми, що реалізують обмін сеансовими ключами за допомогою асиметричних криптоперетворень, засвоїв реалізацію обміну ключами з використанням еліптичних кривих, ознайомитися зі схемою Діффі-Хеллмана. Розглянув схему Діффі-Хеллмана із загальним простим числом  і первинним коренем , обраним таємним ключеми . При обміні ключами з респондентом, який має відкритий ключ **, отримав від нього загальний таємний ключ . Обмін ключами відбувся.

Вважаю дану лабораторну роботу виконаною в повному обсязі.