**Лабороторна работа №6**

**Тема:** Алгоритм передачі секретних ключів “Diffie-Hellman”

**Мета:** Відпрацювання та закріплення теоретичних відомостей алгоритму “Diffie-Hellman ”

**Короткі відомості:**

Алоритм Діффі - Хеллмана (Diffie-Hellman) - криптографічний протокол, що дозволяє двом і більш сторонам отримати загальний секретний ключ, використовуючи незахищений від прослуховування канал зв'язку. Отриманий ключ використовується для шифрування подальшого обміну за допомогою алгоритмів симетричного шифрування.

Схема відкритого розподілу ключів, запропонована Діффі і Хеллманом, здійснила справжню революцію в світі шифрування, так як знімала основну проблему класичної криптографії - проблему розподілу ключів.

У чистому вигляді алгоритм Діффі - Хеллмана вразливий для модифікації даних в каналі зв'язку, в тому числі для атаки «Man-in-the-middle (людина посередині)», тому схеми з його використанням застосовують додаткові методи односторонньої або двосторонньої аутентифікації.

Припустимо, існує два абонента: Аліса і Боб. Обом абонентам відомі деякі два числа ***g*** і ***p***, які не є секретними і можуть бути відомі також іншим зацікавленим особам. Для того, щоб створити невідомий більш нікому секретний ключ, обидва абонента генерують великі випадкові числа: Аліса - число ***a***, Боб - число ***b***. Потім Аліса обчислює залишок від ділення (1):

***A=g^a mod p*** (1)

і пересилає його Бобу, а Боб обчислює залишок від ділення (2):

***B=g^b mod p*** (2)

і передає Алісі. Передбачається, що зловмисник може отримати обидва цих значення, але не модифікувати їх (тобто, у нього немає можливості втрутитися в процес передачі).

На другому етапі Аліса на основі наявного у неї ***a*** і отриманого по мережі ***B*** обчислює значення (3):

***B^a mod p=g^a\*b mod p*** (3)

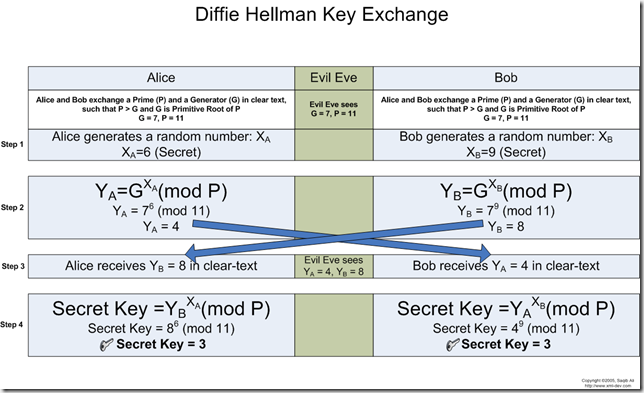
Боб на основі наявної в нього ***b*** і отриманого по мережі ***A*** обчислює значення (4):

***A^b mod p=g^a\*b mod p*** (4)

Як неважко помітити, у Аліси і Боба вийшло одне і те ж число (5):

***K=g^ a\*b mod p*** (5)

Його вони і можуть використовувати в якості секретного ключа, оскільки тут зловмисник зустрінеться з практично нерозв'язною (за розумний час) проблемою обчислення (3) або (4) по перехоплених ***g ^ a mod p*** та ***g ^ b mod p*** , якщо числа ***p, a, b*** обрані досить великими.

******

При роботі алгоритму кожна сторона:

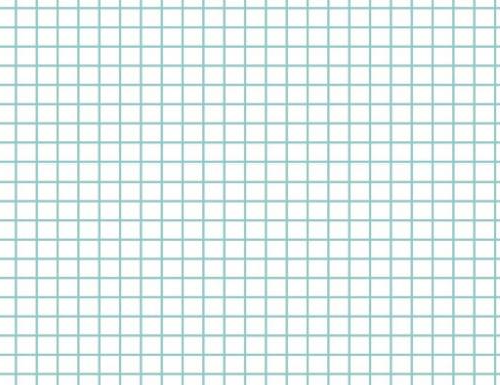
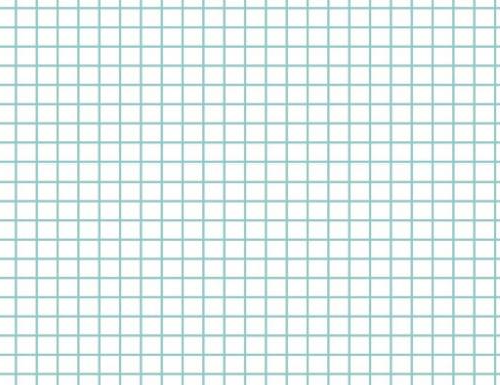
1. генерує випадкове натуральне число ***a*** - закритий ключ
2. спільно з віддаленої стороною встановлює відкриті параметри ***p*** і ***g*** (зазвичай значення ***p*** і ***g*** генеруються на одній стороні і передаються іншій), де

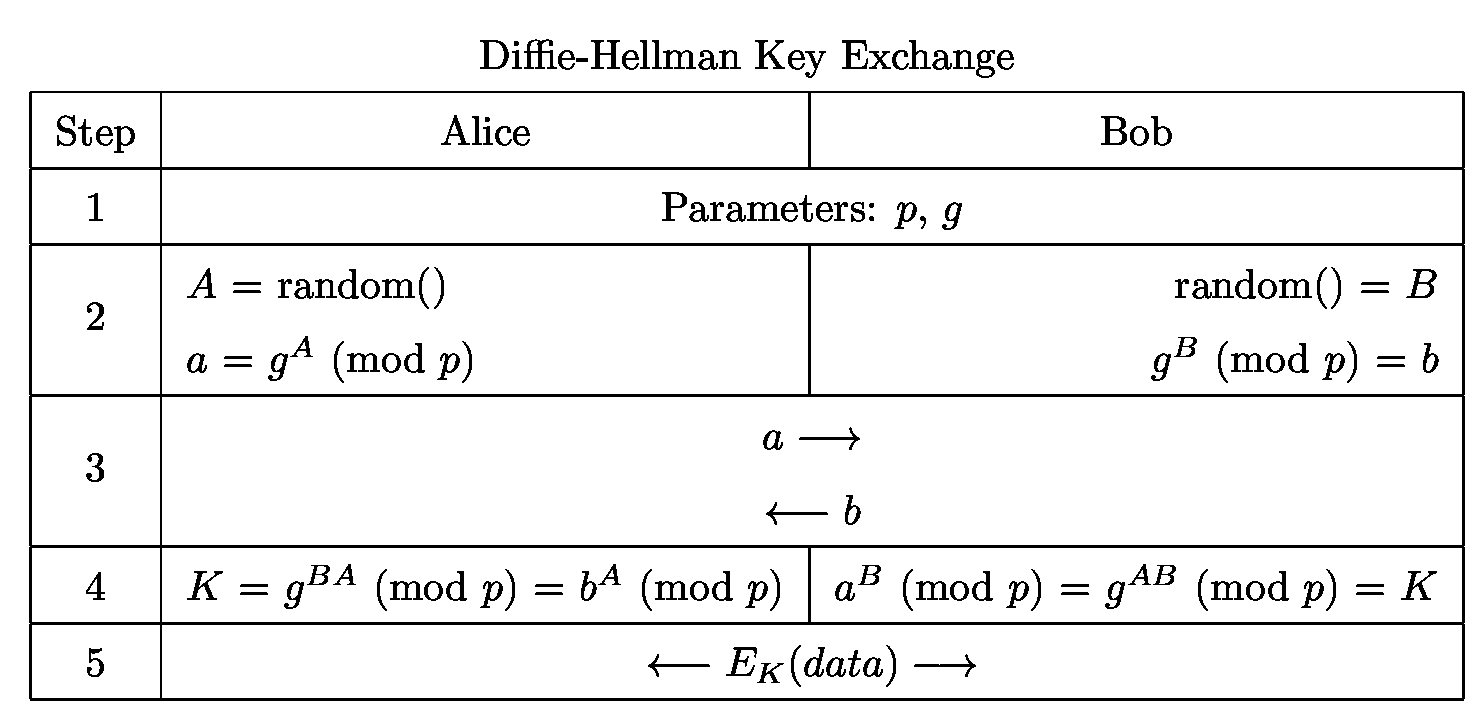
* ***p*** є випадковим простим числом
* ***(P-1) / 2*** також має бути випадковим простим числом (для підвищення безпеки)
* ***g*** є первісним коренем за модулем ***p*** (також є простим числом)

1. обчислює відкритий ключ ***A***, використовуючи перетворення над закритим ключем ***A = g^a mod p***
2. обмінюється відкритими ключами з віддаленою стороною
3. обчислює загальний секретний ключ ***K***, використовуючи відкритий ключ віддаленої сторони ***B*** і свій закритий ключ ***a***

* ***K = B^a mod p***
* ***K*** виходить рівним з обох сторін, тому що:
* ***B^a mod p =*** *(g^b mod p)^a mod p = g^a\*b mod p = (g^a mod p)^b mod p =* ***A^b mod p***

У практичних реалізаціях для ***a*** і ***b*** використовуються числа порядку і ***p*** порядку. Число ***g*** не повинно бути великим і зазвичай має значення в межах першого десятка.





**Висновок:** Алгоритм Diffie-Hellman використовується для обміну секретними ключами, цей алгоритм не можна використовувати для шифрування і дешифрування повідомлень;

***g*** повинно бути примітивом числа ***p*** можна вибирати будь яке число;

***g*** зазвичай одно розрядне число;

***g*** та ***p*** це не секретні числа і являються публічним ключем;

вибір чисел ***g*** та ***p*** можуть впливати на безпеку системи;

***p*** – повинно бути [(n-1)/2] простим числом (1, 2, 5,7, 9, 11) але дуже довгим від цього залежить безпечність цього методи шифрування.