## Індивідуальне практичне завдання

## Керування ключами. Алгоритм шифрування Діффі - Хеллмана

### *Теоретичні відомості*

При симетричному шифруванні обидві сторони, що беруть участь в обміні даними, повинні одержати однакові ключі, до яких сторонні учасники позбавлені доступу. Одночасно із цим необхідна часта зміна ключів, щоб зменшити обсяг даних, що втрачаються через розкриття ключа зловмисником. Тому надійність будь-якої криптосистеми залежить від системи розподілу ключів, що використовується. Система розподілу ключів являє собою систему доставки ключів сторонам, що планують обмін даними, і не дозволяє іншим сторонам скористатися цими ключами.

Розподіл ключів можна організувати різними способами.

1 Ключ може бути обраний однією стороною та фізично доставлений іншій стороні, що бере участь у процесі обміну даними.

2 Ключ може вибрати третя сторона та фізично доставити його учасникам обміну.

3 Якщо сторони, які беруть участь в обміні, вже використовують який-небудь ключ, то одна із сторін може передати іншій стороні новий ключ, зашифрований з використанням старого.

4 Якщо обидві сторони обміну мають криптографічно захищені канали і зв'язки із третьою стороною, то остання може доставити ключ учасникам обміну по цих захищених каналах.

5 Ключ може бути генерований обома учасниками обміну з використанням алгоритму генерації.

Схеми 1 та 2 припускають передачу ключів з рук у руки. Цей спосіб прийнятний при канальному шифруванні, але у випадку наскрізного шифрування фізична доставка ключа є практично неприйнятною.

Схему 3 можна застосувати як для канального, так і для наскрізного шифрування, але якщо зловмисникові стане коли-небудь відомо значення одного із ключів, то йому стануть відомі і всі наступні ключі.

Варіант схеми 4 часто застосовується при наскрізному шифруванні. Так за доставку ключів учасникам обміну відповідає якийсь центр розподілу ключів (ЦРК). При цьому кожен користувач одержує свій унікальний ключ, використовуваний ним разом із ЦРК для організації доставки ключів.

Використання ЦРК припускає організацію ієрархії ключів. Зв'язок між ЦРК і учасником майбутнього обміну шифрується з використанням *сеансового* ключа. Як правило, сеансовий ключ використовують для конкретного логічного з'єднання і надалі більше не застосовують. Сеансовий ключ одержують від

центра тими самими каналам, які використовуються для організації зв'язку між кінцевими користувачами – учасниками майбутнього обміну даними. Відповідно сеансові ключі передаються в зашифрованому вигляді, а для шифрування використовують *головний* ключ, спільний для ЦРК і кінцевого користувача.

Прикладом реалізації схеми 5 може бути ***алгоритм генерації ключів Діффі-Хеллмана***.

Алгоритм Діффі-Хеллмана допомагає обмінюватися секретним ключем для симетричних криптосистем з використанням каналу, захищеного від модифікації, тобто дані, передані цим каналом, можуть бути прослухані, але не змінені. У цьому випадку дві сторони можуть створити однаковий секретний ключ, жодного разу не передавши його по мережі, згідно з таким алгоритмом.

Припустимо, що обом учасникам обміну відомі деякі два натуральні числа $M$ і $N$, де $N$ – просте число . Вони можуть бути відомі й усім іншим зацікавленим особам. Для того щоб створити невідомий більше нікому секретний ключ, обидві сторони генерують випадкові числа: перший абонент – число $X$, другий абонент – число $Y$.

Потім перший абонент обчислює значення

$$L_A = M^X \bmod N$$

і пересилає його другому учаснику, а другий учасник обчислює значення

$$L_B = M^Y \bmod N$$

і передає його першому.

Зловмисник одержує обидва значення $L_A$ та $L_B$, але модифікувати їх (втрутитися в процес передачі) не може.

На другому етапі перший абонент, на основі наявного в нього числа $X$ й отриманого по мережі числа $L_B$, обчислює значення

$$K_A = L_B^X \bmod N ,$$

а другий абонент на основі наявних у нього чисел $Y$ та $L_A$ обчислює значення

$$K_B = L_A^Y \bmod N .$$

Неважко переконатися, що в обох учасників вийшло те саме число $K_A = K_B$:

$$K_A = L_B^X \bmod N = (M^Y)^X \bmod N = M^{YX} \bmod N =$$
$$= M^{XY} \bmod N = (M^X)^Y \bmod N = L_A^Y \bmod N = K_B.$$

Числа $K_A, K_B$ можуть використовуватися як ключі при обміні даними з використанням традиційних систем шифрування.

Наприклад, нехай абонентам $A$ і $B$ відомі деякі два числа $M$ =17 й $N$=23.

Абонент $A$ генерує випадкове число $X$=3 й обчислює значення

$$L_A = 11^3 \, mod \, 23 = 14.$$

Абонент $B$ генерує випадкове число $Y=5$ й обчислює значення

$$L_B = 17^5 \, mod \, 23 \equiv 21.$$

Абонент $A$ передає абонентові $B$ значення $L_{A,}$, а абонент $B$ абонентові $A$ значення $L_B$. Кожний з абонентів $A$ та $B$ обчислюють секретний ключ згідно з прийнятими даними $L_A$ і $L_B$.

A: $K_A = 21^3 \bmod 23 = 15$,

B: $K_B = 14^5 \bmod 23 = 15$.

При спробі визначити значення чисел $X$ та $Y$ за перехопленим значенням $L_A$ і $L_B$ супротивник зіштовхнеться із задачею дискретного логарифмування, що є важко розв'язною.

Алгоритм Діффі-Хеллмана працює тільки на лініях зв'язку, надійно захищених від модифікації.

**Індивідуальні завдання:**

1 Виконайте алгоритм генерації ключів Діффі-Хеллмана для чисел $M, N, X, Y$:

$M=17, N=23, X=5, Y=8$;
$M=13, N=31, X=7, Y=12$;
$M=19, N=29, X=6, Y=9$.

2 Розгляньте схему Діффі-Хеллмана з простим числом $N=11$ та $M=2$.

1) Якщо користувач $A$ має відкритий ключ $L_A=9$, то яким буде значення таємного ключа $X$ користувача $A$?

2) Якщо користувач $B$ має відкритий ключ $L_B=3$, то яким буде спільний таємний ключ?

3. Проведіть генерацію власних ключів за алгоритмом Діффі-Хеллмана.