31. В чому сутність механізму встановлення ключів та як він може бути реалізований у вигляді криптографічного протоколу?

Найпоширенішими протоколами є протоколи встановлення спільної таємниці (ключа). Під *протоколом встановленням ключів* будемо розуміти протокол або процес, за допомогою якого спільний ключ стає доступним двом та більше суб'єктам – учасникам протоколу, і надалі використовується ними при виконанні криптографічних перетворень. Протокол встановлення ключів може бути розділений на протокол узгодження та передачі ключів, а також встановлення статичних і динамічних ключів.

Протокол узгодження ключів – це частковий протокол встановлення ключів, при виконанні якого спільний ключ одержують два або більше суб'єкти, таким чином, щоб ніякий інший об'єкт не зміг визначити його результуюче значення.

Протокол передачі ключів – це метод (механізм) встановлення ключів, при якому одна сторона формує (створює) або іншим способом одержує секретне значення і безпечно передає його іншій стороні.

Узгодження розподіленої таємниці (ключа) – це таке обчислення таємниці (ключа) двома або більше суб'єктами, коли кожен з них не в змозі попередньо обчислити таємний ключ окремо (один) з заданою ймовірністю.

Загальний порядок встановлення ключів:
узгодження таємниці;
вироблення ключа;
підтвердження ключа;
передавання ключа (один із суб'єктів вибирає ключ і передає іншому суб'єкту).

При виконанні протоколів треба реалізовувати:

узгодження спільної інформації та параметрів;
налаштування параметрів.

При побудуванні протоколів в групі точок еліптичних кривих дуже важливим є перевіряння відкритих ключів та базової точки:

$$Q_i, P_i, G \qquad \begin{matrix} (X_{Q_i}, Y_{Q_i}), \\ (X_{P_i}, Y_{P_i}). \end{matrix}$$

При проективному представленні $(X_{P_i}, Y_{P_i}, Z_{P_i})$

$Q_i = d_i G (\mathrm{mod}\, q)$.

Якщо ключ є викривлений, то він може не входити в циклічну групу порядку n і тому гарантії того що порядок теж n немає.

Перевіряння належності Q_i, P_i, G еліптичній кривій:

$$y^2 = x^3 + ax + b (\mathrm{mod}\, p).$$

Для проективного базису ЕК над полем $GF(2^m)$

$$Y^2 + XYZ \equiv X^3 + aX^2Z^2 + bZ^6 (\mathrm{mod}(x),2).$$

Для поля $GF(2^m)$, $q = 2^m$, еліптична крива у афінному базисі задається у вигляді:

$$y^2 + xy \equiv x^3 + ax^2 + b(\mathrm{mod}\, f(x),2).$$

Для захисту від таких загроз запропоновано використовувати кофакторне множення, де кофактор (h) – це коефіцієнт, що зв'язує порядок кривої з порядком базової точки G.

$$U = h \cdot n.$$

Суб'єкти А та В хочуть встановити між собою спільну таємницю, на основі неї виробити діючий ключ. При цьому, попередньо вони можуть згенерувати симетричні або асиметричні ключі та розповсюдити їх захищеним шляхом.

Нехай особисті ключі $h_x \in H$, а також є деякі елементи $g \in G$, існує відображення $y = F(h_x \cdot g)$. Для А і В справедливо співвідношення:

$$F(h_A, (F(h_B, g))) = F(h_B, F(h_A, g)), \quad (6.3.1)$$

при цьому знайти значення $F(h_i, F(h_j, g))$ при невідомих h обчислювально неможливо.

Для кожного $h_x \in H$ існує також відкритий ключ:

$$P_x = F(h_x, g);$$

$$P_x = y. \quad (6.3.2)$$

Тоді існують інтерактивні протоколи встановлення ключів, які вимагають одну, дві або три взаємодії при встановленні ключів.

$$K_{AB} = Y_B^{X_A} (\mathrm{mod}\, P) = \Theta^{X_B X_A} (\mathrm{mod}\, P);$$

$$0 < K_{AB} < P;$$

$$P \geq 2^{1024}. \quad (6.3.3)$$

6.3.2 Аналіз крипто протоколів встановлення ключів (узгодження ключів)

Протокол з нульовим проходом та кофакторним множенням.

Суб'єкти А та В формують особисті ключі d_A та d_B відповідно. Потім формують відкриті ключі:

$$P_A = d_A \cdot G,$$

$$P_B = d_B \cdot G; \quad (6.3.4)$$

та передають їх один одному.

Суб'єкт А формує:

$$K_{AB} = d_A \cdot P_B = d_A \cdot d_B \cdot G. \quad (6.3.5)$$

Суб'єкт В формує:

$$K_{BA} = d_B \cdot P_A = d_B \cdot d_A \cdot G. \quad (6.3.6)$$

$$K_{AB} = K_{BA}.$$

Протокол узгодження розподіленої таємниці та довгострокових ключах з нульовим проходом та кофакторним множенням.

Пропонується ввести:

- кофактор $h = \frac{U}{n}$;

- деяке значення l.

Коли не ставиться задача узгодженості з іншим протоколом:

$h = \frac{U}{n},\ l = 1$.

Коли вимагається узгодженість:

$h = \frac{U}{n},\ l = h^{-1} (\mathrm{mod}\, n)$.

Коли кофакторне множення не використовується:

$h = 1,\ l = 1$.

$P_A = (d_A \cdot l)(h \cdot G)$.

$K_{AB} = (d_A \cdot l)(h \cdot P_B)$; (6.3.7)

$K_{BA} = (d_B \cdot l)(h \cdot P_A)$. (6.3.8)

аналіз протоколів передавання ключів

Два суб'єкти хочуть обмінятись таємними повідомленнями, для цього треба виробити ключ по відкритому каналу. Ключ повинна виробляти одна із сторін. Повинні забезпечуватись:

автентифікація передавання ключа;

захист від раніше переданих повідомлень;

конфіденційність ключа.

Реалізація протоколу.

Нехай суб'єкт А генерує таємний ключ К та формує блок відкритих даних:

$BS = A \| K \| TVP \| Text1$,

де А – ідентифікатор суб'єкта А;

TVP – позначка часу (порядковий номер повідомлення);

К – таємний ключ.

TVP дозволяє відрізнити повтор повідомлення.

Направлений шифр (E_B, D_B), де D_B – особисте перетворення, а E_B – відкрите перетворення суб'єкта В.

$E_B(BS) = E_B(A \| K \| TVP \| Text1)$.

Якщо використовується RSA, то:

$BS_i^{E_B} (\mathrm{mod}\, N_j)$.

Далі, суб'єкт А передає E_B суб'єкту В.

$D_B = (E_B(BS)) = DB(E_B(A \| K \| TVP \| Text1))$.

Характеристики протоколу:

протокол однопрохідний;

автентифікація суб'єкта В;

не забезпечує крипто живучості.