36. Сутність моделі протоколу розподілення таємниці та його реалізація ?

Модель протоколу:

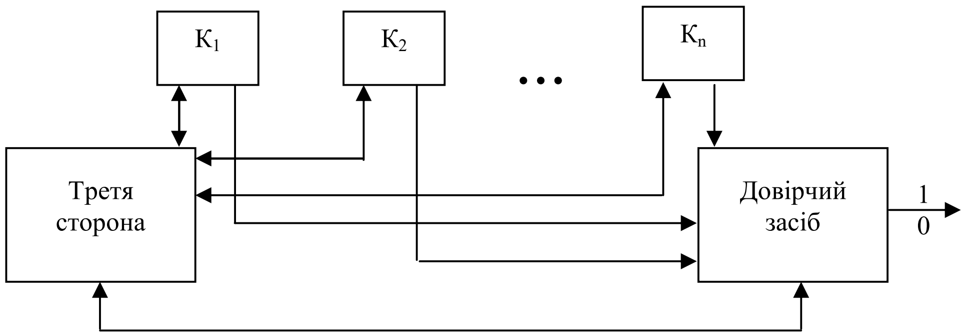
Протокол розділюваної таємниці – багатосторонній протокол, в якому приймають участь одночасно К із n суб’єктів і в результаті їх узгодженої дії виробляється або розділюваний ключ, або розділювана таємниця, що в подальшому використовується в управлінні критичною технологією.

Загальна модель:

приймає участь n суб’єктів;

розділювана таємниця може бути здійснена за згоди К суб’єктів.

На малюнку представлена модель протоколу розділюваної таємниці.



Третя сторона виробляє часткові ключі $K_1, K_2, ..., K_n$. Після цього передає їх до користувачів, забезпечуючи конфіденційність, справжність, доступність, спостережливість. Користувачі передають $K_1, K_2, ..., K_n$ довірчій стороні забезпечуючи конфіденційність, справжність, доступність, спостережливість. Частки ключів повинні зберігатись з крипто живучістю. У довірчій стороні повинна бути захищена функція:

$\Psi(K_1, K_2, K_k) = K_{AK}$.

<u>Приклад реалізації протоколу: Протокол Шаміра</u>

Розподіл таємниці в системі здійснюється за схемою Шаміра з параметрами к=5. Необхідно:

1) обрати розмір поля GF(p), над яким здійснюється розподіл таємниці;

2) сформувати загальний секрет S_0;

3) обчислити часткові секрети S_i;

4) сформувати загальний секрет $S_0^{'}$, отримавши, часткові S_i, використовуючи інтерполяційну формулу Лагранжа.

Розв’язок.

1) спочатку формуємо просте число $P > P_{доп}$, наприклад, для наглядності P=37;

2) породжуємо випадково загальний секрет S_0, що є елементом поля GF(p), тобто $1 \le S \le P-1$. Наприклад, S=29;

3) оскільки к=5, то формуємо випадково к-1=4 коефіцієнтів a_1, a_2, a_3, a_4. Наприклад, $a_1 = 7$, $a_2 = 31$, $a_3 = 18$, $a_4 = 27$. Як a_0 вибираємо S_0, тому $a_0 = S_0$;

4) присвоюємо кожному із об’єктів чи суб’єктів числові значення ідентифікаторів $i_1 = 16, i_2 = 3, i_3 = 24, i_4 = 35, i_5 = 7$;

5) поліном f(x) має вид: $f(x) = (a_0 + a_1 x^1 + a_2 x^2 + a_3 x^3 + a_4 x^4) \bmod P$, підставимо в нього числові дані, отримаємо:

$$f(x) = (29 + 7x^1 + 31x^2 + 18x^3 + 27x^4) \bmod 37.$$

Знаходимо часткові секрети, підставивши в поліном $x = i_1 \div i_4$, тобто

$f(16) = (29 + 7*16 + 31*16^2 + 18*16^3 + 27*16^4) \bmod 37 = 93 \bmod 37 = 19 \bmod 37$;

$f(3) = (29 + 7*3 + 31*3^2 + 18*3^3 + 27*3^4) \bmod 37 = 79 \bmod 37 = 5 \bmod 37$;

$f(24) = (29 + 7*24 + 31*24^2 + 18*24^3 + 27*24^4) \bmod 37 = 108 \bmod 37 = 34 \bmod 37$;

$f(35) = (29 + 7*35 + 31*35^2 + 18*35^3 + 27*35^4) \bmod 37 = 94 \bmod 37 = 20 \bmod 37$;

$f(7) = (29 + 7*7 + 31*7^2 + 18*7^3 + 27*7^4) \bmod 37 = 115 \bmod 37 = 4 \bmod 37$.

Таким чином: $S_1 = f(i_1) = 19$,

$S_2 = f(i_2) = 5$,

$S_3 = f(i_3) = 34$,

$S_4 = f(i_4) = 20$,

$S_5 = f(i_5) = 4$.

В подальшому $S_0 = 29$ встановлюється в довірений засіб як загальний секрет. Часткові секрети $S_1 - S_5$ розповсюджуються в системі з забезпеченням цілісності, справжності, доступності та спостережливості.

Нехай необхідно виробити загальний секрет, причому всі об'єкти (суб'єкти) згодні. В цьому випадку кожний з них передає свій секрет в довірений пристрій, забезпечивши їх цілісність, справжність та конфіденційність.

В засобі, якому довіряють, здійснюється відновлення f(x). Для цього використовується інтерполяційна формула Лагранжа $f(x)=\sum_{e=1}^{k} f(i_e)\prod_{j\neq e}(\frac{x-i_j}{i_e-i_j})$. Підставивши в цей вираз числові значення, отримаємо:

$$f(x)=(19*\frac{x-3}{16-3}*\frac{x-24}{16-24}*\frac{x-35}{16-35}*\frac{x-7}{16-7}+5*\frac{x-16}{3-16}*\frac{x-24}{3-24}*\frac{x-35}{3-35}*\frac{x-7}{3-7}+$$

$$+34*\frac{x-16}{24-16}*\frac{x-3}{24-3}*\frac{x-35}{24-35}*\frac{x-7}{24-7}+20*\frac{x-16}{35-16}*\frac{x-3}{35-3}*\frac{x-24}{35-24}*\frac{x-7}{35-7}+$$

$$+4*\frac{x-16}{7-16}*\frac{x-3}{7-3}*\frac{x-24}{7-24}*\frac{x-35}{7-35}=\frac{19}{17784}*(x^2-27x+35)*(x^2-5x+23)+$$

$$+\frac{5}{34944}*(x^2-3x+14)*(x^2-5x+23)+\frac{34}{-31416}*(x^2-19x+11)*(x^2-5x+23)+$$

$$+\frac{20}{187264}*(x^2-19x+11)*(x^2+6x+20)+\frac{4}{-17136}*(x^2-19x+11)*(x^2+15x+26)$$

Проведемо підрахунки зворотних елементів:

$17784=24\,\mathrm{mod}\,37$ $\quad \frac{37}{24}=1+\frac{13}{24};\ \frac{24}{13}=1+\frac{11}{13};\ \frac{13}{11}=1+\frac{2}{11};\ \frac{11}{2}=5+\frac{1}{2};\ \frac{2}{1}=2.\ \ k=4$

$a_0=1,\ a_1=2,\ a_2=3,\ a_3=17$ $\qquad y=17\,\mathrm{mod}\,37.$

$34944=16\,\mathrm{mod}\,37$ $\quad \frac{37}{16}=2+\frac{5}{16};\ \frac{16}{5}=3+\frac{1}{5};\ \frac{5}{1}=5.\ \ k=2$

$a_0=2,\ a_1=7,$ $\qquad y=7\,\mathrm{mod}\,37.$

$-31416=34\,\mathrm{mod}\,37$ $\quad \frac{37}{34}=1+\frac{3}{34};\ \frac{34}{3}=11+\frac{1}{3};\ \frac{3}{1}=3.\ \ k=2$

$a_0=1,\ a_1=12,$ $\qquad y=12\,\mathrm{mod}\,37.$

$187264=7\,\mathrm{mod}\,37$ $\quad \frac{37}{7}=5+\frac{2}{7};\ \frac{7}{2}=3+\frac{1}{2};\ \frac{2}{1}=2.\ \ k=2$

$a_0=5,\ a_1=16$ $\qquad y=16\,\mathrm{mod}\,37.$

$$-17136 = 32 \bmod 37 \quad \frac{37}{32} = 1 + \frac{5}{32};\ \frac{32}{5} = 6 + \frac{2}{5};\ \frac{5}{2} = 2 + \frac{1}{2};\ \frac{2}{1} = 2.\ \ k = 3$$

$$a_0 = 1,\ a_1 = 7,\ a_2 = 15 \qquad\qquad y = (-1)^3 * 15 \bmod 37 = 22 \bmod 37.$$

$$f(x) = (19*17*(x^4 - 5x^3 + 23x^2 - 27x^3 + 24x^2 + 8x + 35x^2 + 10x + 28) +$$
$$+5*7*(x^4 - 5x^3 + 23x^2 - 3x^3 + 15x^2 + 5x + 14x^2 + 4x + 26) +$$
$$+34*12*(x^4 - 5x^3 + 23x^2 - 19x^3 + 21x^2 + 7x + 11x^2 + 19x + 31) +$$
$$+20*16*(x^4 + 6x^3 + 20x^2 - 19x^3 - 3x^2 - 10x + 11x^2 + 29x + 35) +$$
$$+4*22*(x^4 + 15x^3 + 26x^2 - 19x^3 + 11x^2 + 24x + 11x^2 + 17x + 27)) \bmod 37 =$$
$$= (27x^4 + 24x^3 + 31x^2 + 5x + 16 + 35x^4 + 16x^3 + 7x^2 + 19x + 22 + x^4 + 13x^3 +$$
$$+18x^2 + 26x + 31 + 24x^4 + 21x^3 + 6x^2 + 12x + 26 + 14x^4 + 18x^3 + 6x^2 + 19x + 8) \bmod 37 =$$
$$= (27x^4 + 18x^3 + 31x^2 + 7x + 29) \bmod 37.$$

У результаті було відновлено початковий поліном, де f(0) і є загальний секрет.