Схема Порогового Розподілення Секрету «*k*,*n*»

Володимир Лужецький
кафедра Захисту Інформації
Вінницький національний технічний університет
Вінниця, Україна
v.luzhetskyi@vntu.edu.ua

Микита Ціхоцький
кафедра Захисту Інформації
Вінницький національний технічний університет
Вінниця, Україна
nik.tsikhotskyi@vntu.edu.ua

Threshold Secret Sharing Scheme «*k*,*n*»

Volodymyr Luzhetskyi
Doctor of Technical Science, Professor, Head of Information Security Department
Vinnytsia National Technical University
Vinnytsia, Ukraine
v.luzhetskyi@vntu.edu.ua

Mykyta Tsikhotskyi
Information Security Department
Vinnytsia National Technical University
Vinnytsia, Ukraine
nik.tsikhotskyi@vntu.edu.ua

***Анотація* — Запропоновано математичну модель порогової схеми розподілення секрету (*k*,*n*). З використанням даної моделі можна виконати розподілення секрету для будь-яких *k* та *n* (*k*<*n*) таким чином, що лише *k* учасників разом зможуть відновити секретне повідомлення.**

***Abstract* — A mathematical model of the secret distribution threshold scheme (*k*,*n*) is proposed. Using this model, we can perform secret distribution for any *k* and *n* (*k*<*n*) in such a way that only *k* participants together can recover the secret message.**

Ключові слова* — *порогова схема; процес розподілення секрету; процес відновлення секрету; дилер; коаліція учасників; секретний ключ; перестановка байтів.

Keywords* — *threshold scheme; secret distribution process; secret recovery process; dealer; coalition of participants; secret key; byte permutation.

I. Вступ

У сучасному світі де все більші обсяги інформації обробляються, передаються або зберігаються у мережі існує велика загроза компрометації важливих даних. Також важливим аспектом безпеки інформації є загроза втрати даних цілком або частково, що може призвести до критичних наслідків різного масштабу залежно від сфери діяльності. Ефективним підходом до забезпечення безпеки інформації від втрати є розподілення даних на декілька частин між різними учасниками або технічними вузлами з введенням додаткових даних. Але ці додаткові дані не повинні створювати потенційні загрози конфіденційності інформації. Для вирішення цієї та інших проблем захисту було запропоновано використовувати схеми розподілення секрету.

Схема розподілення секрету (*СРС*) передбачає два процеси: розбиття на частини та відновлення за певною сукупністю частин [1]. Ці процеси відбуваються за участі дилера та учасників групи.

У пороговій схемі розподілення секрету (*k*,*n*) дилер розбиває секрет на *n* частин і надсилає певну їх сукупність кожному з *n* учасників групи [2]. Відновлення секрету відбувається за умови наявності коаліції з *k* учасників групи та за обов'язкової участі дилера . Але будь-які $k-1$ або менше учасників коаліції не забезпечують можливість відновлення секрету **M**. Отже, навіть якщо $n-k$ частин знищено або загублено, є можливість відновити **M** з решти *k* часток. Крім того, навіть якщо будуть викрадені $k-1$ часток, будь-яка інформація про **M** не буде доступна зловмиснику. Це означає, що схема *СРС* безпечна як проти знищення, так і проти крадіжки. Також варто зазначити, що схема *СРС* є безумовно безпечною, оскільки дана схема не базується на жодному припущенні щодо обчислювальних труднощів, подібних до розкладання цілих чисел на множники або обчислення дискретних логарифмів [3].

Відомі порогові схеми розподілення секрету створюють частини, які за обсягом дорівнюють обсягу повідомлення **M**. Це є одним із недоліків таких схем. Другим недоліком порогових схем розподілення секрету є використання відносно складних обчислень.

Метою дослідження є усунення вказаних недоліків, а саме зменшення обсягу частин секрету та пришвидшення процесу розподілення, та відновлення секрету.

II. Основна частина

Процес розбиття повідомлення реалізує дилер з використанням секретного ключа. Цей ключ є базою для правила формування частин повідомлення.

Повідомлення **M** розбивається на *n* частин:

$$\mathbf{M} = m_1, m_2, ..., m_n . \quad (1)$$

Кожен з учасників групи отримує свою частину секрету, яку їм видає дилер:

$$\mathbf{P}_l, \text{ де } l = 1,...,n. \quad (2)$$

Набір даних $\mathbf{P}_l$ визначається таким чином:

$$\mathbf{P}_l = \{m_{l+j}\}, \quad (3)$$

для $j = 0,...,r-1$; $r = n-k$, якщо $l + j > n$, то $l + j - n$.

Дилер у себе зберігає значення D, яке обчислюється за формулою:

$$D = m_1 \oplus m_2 \oplus ... \oplus m_n. \quad (4)$$

Для відновлення секрету дилер має отримати від коаліції не менше ніж k частин, на основі яких і власних даних відновлює усі частини повідомлення, а потім з використанням секретного ключа відновлює все повідомлення.

Приклад. Нехай маємо порогову схему (3,5).

$r = 5-3 = 2$; $l = 1,...,5$; $j = 0;1$

Результати формування частин секрету:

$\mathbf{P}_1 = \{m_{1+j}\} = \{m_1, m_2\}$;

$\mathbf{P}_2 = \{m_{2+j}\} = \{m_2, m_3\}$;

$\mathbf{P}_3 = \{m_{3+j}\} = \{m_3, m_4\}$;

$\mathbf{P}_4 = \{m_{4+j}\} = \{m_4, m_5\}$;

$\mathbf{P}_5 = \{m_{5+j}\} = \{m_5, m_1\}$, $5+j$ для $j = 1$ більше за 5, тому $5+1-5 = 1$.

$D = m_1 \oplus m_2 \oplus m_3 \oplus m_4 \oplus m_5$

Приклад відновлення повідомлення **M** коли 3 учасники надали свої частини $\mathbf{P}_1 = \{m_1, m_2\}$, $\mathbf{P}_2 = \{m_2, m_3\}$, $\mathbf{P}_3 = \{m_3, m_4\}$. При цьому є частини m_1, m_2, m_3, m_4 і потрібно відновити частину m_5. Для цього дилер використовує свої дані D:

$m_5 = D \oplus m_1 \oplus m_2 \oplus m_3 \oplus m_4$.

Далі маючи всі частини дилер з використанням секретного ключа відновлює вихідний секрет **M**.

Приклад неможливості відновлення повідомлення **M** коли свої частини надали лише 2 учасники $\mathbf{P}_1 = \{m_1, m_2\}$, $\mathbf{P}_2 = \{m_2, m_3\}$. При цьому є частини m_1, m_2, m_3. Для відновлення секрету **M** потрібно ще значення m_4, m_5. Однак дилер не зможе їх відновити використовуючи свої дані D.

Для запропонованого методу порогового розподілення секрету обсяг частин учасників групи обчислюється за формулою:

$$C_\Gamma = C_M \cdot r.$$

Частина дилера має обсяг $\frac{C_M}{n}$. Таким чином спільний обсяг даних дорівнює $C = C_M \frac{(rn+1)}{n}$.

Для відомих схем розподілення секрету обсяг частин дорівнює $C_B = C_M \cdot n$.

Отже, запропонований метод забезпечує зменшення обсягу частин в $K = \frac{n^2}{rn+1}$ разів.

Наприклад, для схеми (3,5) обсяг зменшується у 2,2 рази.

Пришвидшення процесів розподілення і відновлення секрету досягається за рахунок формування частин шляхом перестановки байтів повідомлення **M**. Перестановку пропонується реалізовувати з використанням генератора псевдовипадкових чисел, описаного в роботі [4].

III. Висновки

Особливість запропонованої схеми порогового розподілення секрету полягає в тому, що частини секрету формуються лише з байтів повідомлення, що переставляються певним чином і кожен учасник групи отримує r частин. Саме це забезпечує зменшення обсягу усіх даних, що зберігають учасники групи та пришвидшення процесів розподілення і відновлення секрету.

Література References

[1] B. Masucci. Sharing multiple secrets: Models, schemes and analysis. Des. Codes Cryptography, 39(1):89–111, 2006. (дата звернення: 26.04.2024).

[2] Лужецький В. А. Комплексний захист інформації в медичній інформаційній системі // Актуальні задачі медичної, біологічної фізики та інформатики. Матеріали доповідей та виступів всеукраїнської науково-практичної конференції з міжнародною участю 27 квітня 2022 року Вінниця. – Вінниця: Едельвейс. – С. 75-78. (дата звернення: 28.04.2024).

[3] A. Beimel. Secret-sharing schemes: a survey. In Chee Y.M. et al., editor, Coding and Cryptology. IWCC 2011. Lecture Notes in Computer Science, Vol. 6639. Springer, Berlin, https://doi.org/10.1007/ 978-3-642-20901-7 2. (дата звернення: 29.04.2024).

[4] Лужецький В. А. Метод формування перестановок довільної кількості елементів / В. А. Лужецький, І. С. Горбенко // Захист інформації. - 2013. - т. 15, № 3. - С. 262-267. - Режим доступу: http://nbuv.gov.ua/UJRN/Zi_2013_15_3_1 . (дата звернення: 30.04.2024).