3. Armano G, Marchal S, Asokan N (2016) Real-time client-side phishing prevention add-on. In: 2016 IEEE 36th international conference on distributed computing systems (ICDCS), pp 777–778. https://doi.org/10.1109/icdcs.2016.44

4. Phishing scams and spoof emails at MillerSmiles.co.uk. http://www.millersmiles.co.uk/.

5. Join the fight against phishing. https://www.phishtank.com/.

6. Hawanna VR, Kulkarni VY, Rane RA (2016) A novel algorithm to detect phishing URLs. In: 2016 international conference on automatic control and dynamic optimization techniques (ICACDOT), pp 548–552. https://doi.org/10.1109/icacdot.2016.7877645

7. Hu J, Zhang X, Ji Y, Yan H, Ding L, Li J, Meng H (2016) Detecting phishing websites based on the study of the financial industry webserver logs. In: 2016 3rd international conference on information science and control engineering (ICISCE), pp 325–328. https://doi.org/10.1109/icisce.2016.79

8. Mei C, Leng C, Dayang H, Abang I, Nah S (2016) Feature-based phishing detection technique. J Theor Appl Inf Technol:101–106 Retrieved from https://ir.unimas.my/id/eprint/13943/

9. Phishing Trends & Intelligence Report 2018. https://info.phishlabs.com/hubfs/ 2018PTIReport/ PhishLabsTrendReport_2018-digital.pdf.

УДК 004.056.55

СХЕМА РОЗПОДІЛУ СЕКРЕТУ НА ОСНОВІ КИТАЙСЬКОЇ ТЕОРЕМИ ПРО ОСТАЧІ

Іллюшко Б. О., здобувач вищої освіти гр. КБ-181
Науковий керівник: **Синенко М. А.,** к.ф.м.-н., доцент
Національний університет «Чернігівська політехніка»

Схема розподілу секрету – криптографічний метод, суть якого полягає у розподіленому зберіганні секрентої інформації (наприклад, секретних ключів, паролів) з метою запобігання шахрайству. Секрет розподіляється серед учасників таким чином, що тільки їх коаліція в змозі його відновити. Ймовірність злочинної змови усіх учасників групи, що мають доступ до зберінання частин секрету вважається неймовірно малою. Серед поширених схем розподілу секрету слід відмітити схему Блеклі, яка була створена у 1979 році і базується на твердженні, що система k лінійних лінійно незалежних конгруенцій по простому модулю має один розв'язок, схему Шаміра, яка побудована на ідеї інтерполяції многочлена $(k-1)$-го степеня k точками.

У даній роботі буде розглянуто схему розподілу секрету, ідея побудови якої базується на китайській теоремі про остачі. Доведена близько 100 років до н.е. у наш час ця теорема широко застосовується у криптографії.

Сформулюємо китайську теорему про остачі.

Якщо $m_1, m_2, \dots, m_k$ попарно взаємно прості числа, $(m_i, m_j) = 1, i \neq j$, $a_1, a_2, \dots, a_k$ – довільні цілі числа, то система конгруенцій виду

$$\begin{cases} x \equiv a_1 (mod\ m_1) \\ x \equiv a_2 (mod\ m_2) \\ \dots\dots\dots\dots\dots\dots\dots\dots \\ x \equiv a_k (mod\ m_k) \end{cases}$$

має єдиний розв'язок $x \equiv a (mod\ M)$, де

$M = m_1 m_2 \dots m_k,\ a = \sum_{i=1}^{k} a_i M_i \mu_i,\ M_i = \frac{M}{m_i},\ \ \mu_i = M_i^{-1} (mod\ m_i).$

Розглянемо схему розподілу секрету. Нехай N – секрет. Вибирають попарно різні прості числа $p_1, p_2, \dots, p_k$ і для кожного простого числа p_i знаходять $x_i \equiv N (mod\ m_i)$. Числа x_i –

доля секрету учасників коаліції. Відмітимо, що при виборі простих чисел p_i повинні бути враховані наступні умови:

- добуток $p_1 p_2 \dots p_k > N$. Для цього достатньо вибирати $p_i > \sqrt[k]{N}, i = 1,2, \dots k$;
- будь-які ***(k-1)*** учасників коаліції не можуть відновити секрет без ***k***-го учасника. Для цього достатньо вибирати $p_i \ll \sqrt[k-1]{N}$.

Для відновленя секрету k учасників збираються разом, складають та розв'язують систему конгруенцій відносно невідомого *N:*

$$\begin{cases} N \equiv x_1 (mod\ p_1) \\ N \equiv x_2 (mod\ p_2) \\ \dots\dots\dots\dots\dots\dots\dots\dots \\ N \equiv x_k (mod\ p_k), \end{cases}$$

розв'язок якої і визначає секркт.

Розглянемо приклад. Нехай секрет ***N***=679. Користуючись розглянутою схемою, розділимо його між трьома учасниками коаліції. Спочатку виберемо три простих числа. Оскільки $\sqrt{679} \approx 26{,}06;\ \sqrt[3]{679} \approx 8{,}79,$ необхідно, щоб вибрані прості числа задовільняли умову $8{,}79 < p_i \ll 26$. Нехай $p_1 = 11;\ p_2 = 13;\ p_3 = 19$.

$$679 \equiv 8(mod\ 11);\ 679 \equiv 3\ (mod\ 13); 679 \equiv 14(mod\ 19).$$

Отже, долі секрету учасгиків коаліції відповідно дорівнюють $(x_1 = 8; p_1 = 11)$;

$(x_2 = 3; p_2 = 13)$; $(x_3 = 14;\ p_3 = 19)$. Для відновлення секрету розв'язують систему конгруенцій:

$$\begin{cases} N \equiv 8(mod\ 11) \\ N \equiv 3(mod\ 13) \\ N \equiv 14(mod\ 19) \end{cases}$$

Скористаємось китайською теоремою про остачі. $M = 11 \cdot 13 \cdot 19 = 2717;$

$$M_1 = 13 \cdot 19 = 247;\ M_2 = 11 \cdot 19 = 209;\ M_3 = 11 \cdot 13 = 143;$$

Для визначення $M_1^{-1};\ M_2^{-1};\ M_3^{-1}$ розв'язують конгруенції :

$$247y \equiv 1(mod\ 11); 209y \equiv 1(mod\ 13); 143y \equiv 1(mod\ 19).$$

$$M_1^{-1} = 9;\ M_2^{-1} = 1;\ M_3^{-1} = 2.$$

Таким чином,

$$N = 8 \cdot 247 \cdot 9 + 3 \cdot 209 \cdot 1 + 14 \cdot 143 \cdot 2 = 22206 \equiv 679(mod\ 2717).$$

Список використаних джерел

1. О. І. Оглобліна, Т. С. Сушко, Ю. В. Шрамко. Елементи теорії чисел: навч. посіб. – Суми: Сумський державний університет, 2015. – 186 с.
2. Венбо Мао. Современная криптография. Теория и практика. М: Вильямс, 2005. – 768 с.
3. Маховенко Е. Б. Теоретико-числовые методы в криптографии. М.: Гелиос АРВ, 2006.– 320 с.