УДК 004.422.5

Вовк В. С., здобувачка 2 курсу спеціальності
122 Комп'ютерні науки,
Потапова Н. А., канд. екон. наук, доцент,
доцент кафедри інформаційних технологій

ДОСЛІДЖЕННЯ КРИПТОГРАФІЧНИХ ВЛАСТИВОСТЕЙ ХЕШ-ФУНКЦІЇ KECCAK

Донецький національний університет імені Василя Стуса, м. Вінниця

Keccak (вимовляється як «кетчак») – це універсальна криптографічна функція, розроблена Гвідо Бертоні, Джоан Демен, Міхаелем Пітерсом і Жилем Ван Аше. Хоча Keccak може використовуватися і для інших цілей, ця функція найбільш відома як хеш-функція, що забезпечує підвищений рівень безпеки, порівняно зі старими алгоритмами хешування, як от SHA-1 і SHA-2. Keccak-256 була розроблена як кандидат для конкурсу криптографічних хеш-функцій SHA-3, проведеного в 2007 р. Національним інститутом науки і технологій. Keccak став переможним алгоритмом, який у 2015 р. був стандартизований як Федеральний стандарт обробки інформації (FIPS) 202 [1].

Завдяки впровадженню в Keccak унікальної структури, яка продемонструвала більшу безпеку та надійність, ніж інші алгоритми, цей алгоритм був обраний NIST. Із технічного погляду, алгоритм SHA-3 заснований на функціях губки, на відміну від конструкції Меркла–Дамґарда, що використовується в SHA-1 та SHA-2.

Keccak використовується в блокчейні (наприклад, Ethereum та Solana) для забезпечення цілісності даних, а також у сферах кібербезпеки для різних криптографічних застосувань.

Версії Keccak мали $b = 1\,600$ та $c = 2n$, де $n \in \{224, 256, 384, 512\}$. Стан із 1 600 бітів можна розглядати як тривимірний масив бітів a[5][5][64], і кожен біт стану пов'язаний із 3 цілочисельними координатами, a[x][y][z], де x та y беруться за модулем 5, а z – за модулем 64 [2].

Перестановка Keccak складається з 24 раундів, які оперують 1 600 бітами стану. Кожен раунд перестановки складається з п'яти відображень $R = \iota \circ \chi \circ \pi \circ \rho \circ \theta$. Keccak використовує такі угоди про іменування, які допомагають описувати ці відображення:

– Рядок – це набір із 5 бітів із постійними координатами y та z, тобто $a[*][y][z]$.

– Стовпець – це набір із 5 бітів із постійними координатами x та z, тобто $a[x][*][z]$.

– Лінія – це набір із 64 бітів із постійними координатами x та y, тобто $a[x][y][*]$.

– Зріз – це набір із 25 бітів із постійною координатою z, тобто a[*][*][z].

Під час хешування за допомогою keccak256 будь-яка модифікація або зміна рядка призводить до значної зміни хеш-дайджесту. Заміна навіть однієї літери у вхідних даних $A > B$ призводить до значних змін хеш-дайджесту (рис. 1) [3].

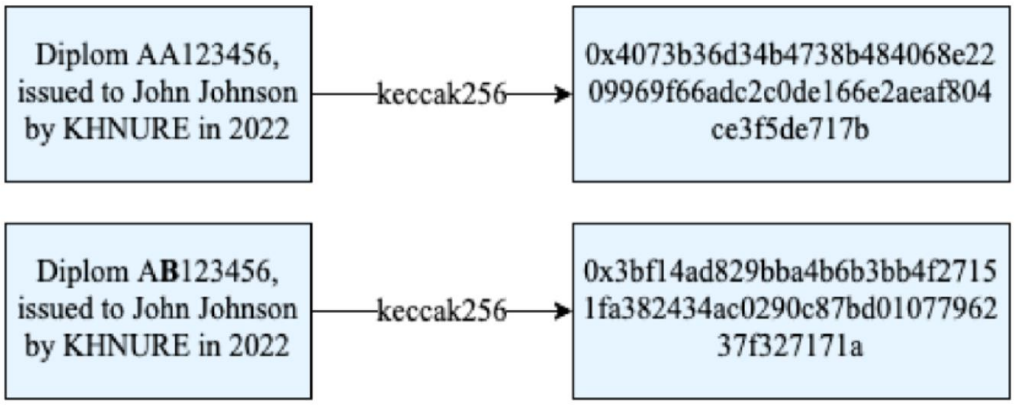


Рисунок 1 – Приклад хешування даних методом keccak256

Враховуючи безпеку та низький рівень можливості атак на SHA-3, цей алгоритм знаходить все більше застосування. Але на цьому все не закінчується. У майбутньому будуть розроблені нові та більш інноваційні хеш-алгоритми. Для криптографічної індустрії важливо постійно еволюціонувати та вирішувати численні проблеми.

Список використаних джерел

1. Antonopoulos A. M., Wood G. Mastering Ethereum: building smart contracts and DApps. Sebastopol: O'Reilly Media, 2018. 424 p.

2. Fast software encryption: 19th International Workshop, FSE 2012, Washington, DC, USA, March 19–21. 2012: revised selected papers / ed. by A. Canteaut. Berlin; Heidelberg: Springer. 2012. 476 p.

3. Group I. S. Trends in the development of science in the modern world. Primedia eLaunch LLC. 2022.

УДК 004.422.5

Головня С. О., здобувачка 2 курсу спеціальності 122 Комп'ютерні науки,
Павлюк О. А., канд. техн. наук, старший викладач кафедри інформаційних технологій

МАШИНА ТЮРІНГА ЯК МОДЕЛЬ ОБЧИСЛЕНЬ: ТЕОРЕТИЧНІ ОСНОВИ ТА СУЧАСНІ ІНТЕРПРЕТАЦІЇ

Донецький національний університет імені Василя Стуса, м. Вінниця

Проблема формального визначення алгоритму є центральною в розвитку теорії обчислень. Щоб описати процес обчислення у строгих математичних термінах, потрібна універсальна модель, здатна відтворювати будь-які логічні та арифметичні дії. Таку модель у 1936 р. запропонував Алан Тюрінг, створивши