

УДК 004.056.5

Ковальов І.Є.¹, Козіна Г.Л.²

¹ студ. гр. РТ-819 НУ «Запорізька політехніка»

² канд. техн. наук, доц. НУ «Запорізька політехніка»

ПРОГРАМНА РЕАЛІЗАЦІЯ ТА АНАЛІЗ НА КОЛІЗІЇ АЛГОРИТМУ ГЕШУВАННЯ КУПИНА ДСТУ 7564:2014

Стандарт гешування Купина визначений в ДСТУ 7564:2014, який встановлює алгоритм обчислення геш-значення для послідовностей двійкових символів, що застосовують у криптографічних методах захисту інформації.

Стандарт 7564:2014 застосовують для забезпечення цілісності та автентичності інформації під час її передавання, оброблення і зберігання, зокрема під час використання електронного цифрового підпису.

Мета роботи – програмна реалізація та аналіз на колізії алгоритму гешування купина ДСТУ 7564:2014.

Програмну реалізацію алгоритму гешування було здійснено на мові Python, який за допомогою Iron Python було під'єднано до .NET Framework. За допомогою мови програмування C# та графічної підсистеми WPF було реалізовано графічний інтерфейс користувача.

В якості алгоритму тестування на колізії стала так звана атака «днів народження». Важливо зазначити, що ефективність атаки «Днів народження» залежить від довжини геша та розміру простору повідомлень.

Було здійснено наступні кроки: генеруються випадкові повідомлення та обчислюються їх геші, у випадку співпадіння гешей для різних повідомлень вважається, що колізія знайдена. Для точності результатів було проведено декілька раундів атак.

В результаті дослідження було здійснено по 10 раундів атак на алгоритми з використанням повідомлень, довжиною в 32 по 64 біт. З 72 біт було здійснено 5 раундів атак, з 80 біт 2 раунди та до першої колізії було виконано атаку з використанням тексту довжиною у 88 біт і зведено до таблиці за середніми даними.

В результаті було отримано наступні результати (Таблиця 1) для алгоритму гешування Купина-256 та Купина-512:

Таблиця 1 – Результат проведених атак

Кількість біт повідомлення	Купина-256		Купина-512	
	Спроб перед першою колізією	Час на обчислення	Спроб перед першою колізією	Час на обчислення
32	420	1:18	471	1:26
64	12401	19:15	13943	24:15
80	31578	59:54	33578	1:00:12
88	148545	4:49:18	158545	5:09:18

За отриманими даними було побудовано графік, побудовано лінію тренду та здійснено екстраполяцію даних. В результаті було встановлено наступні дані, які зведено до таблиці 2.

Таблиця 2 – Екстрапольовані дані

Кількість біт повідомлення	Купина-256		Купина-512	
	Спроб перед першою колізією	Час на обчислення	Спроб перед першою колізією	Час на обчислення
96	487380	16:00:00	518454	16:40:00
128	38355174	1248:00:00	41284596	1360:00
256	14711193963 09630	47 867 257 15 2:00:00	17044178322 85730	56 147 049 200 :00:00

Такий самий аналіз було проведено для алгоритмів MD5 та SHA256 і було встановлено, що для 32 бітового повідомлення MD5 та SHA256 дає 148 та 157 спроб відповідно, а для 128 біт 137729200 та 155289240. Таким чином, здійснено реалізацію та аналіз алгоритму гешування стандарту ДСТУ 7564:2014, та можна зробити висновки, що Купина більш ефективна для коротких повідомлень, а MD5 та SHA256 більш стійкий при більшому повідомленні. Але слід врахувати, що це показники для достатньо грубого методу атаки, який не враховує особливості роботи алгоритму гешування, наприклад які досить давно існують для зламу MD5.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Євсєєв С. П., Йохов О. Ю., Король О. Г., Гешування даних в інформаційних системах: монографія – К.: «ХНЕУ», 2013. – 312 с.
2. ДСТУ ISO 7564:2014 Інформаційні технології. Криптографічний захист інформації. Функція гешування [Чинний від 2015-04-01]. Київ, 2015. 39 с. (Інформація та документація).

Зав. кафедри

Володимир ВОСКОБОЙНИК

Відповідальний на факультеті

Олександр ПІРОЖЕНКО