Белорусский государственный университет
Механико-математический факультет
Кафедра дифференциальных уравнений и системного анализа

Аннотация к магистерской диссертации

“Поиск коллизий функций хеширования”

Жуковец Даниил Александрович

руководитель Чергинец Дмитрий Николаевич

2021

Магистерская диссертация содержит: 30 страниц, 8 таблиц, 2 иллюстрации, 11 использованных источников литературы.

Ключевые слова: ХЭШ-ФУНКЦИЯ, MD5, КОЛЛИЗИЯ, SHA-1, ДИФФЕРЕНЦИАЛЬНАЯ АТАКА, ТУННЕЛИРОВАНИЕ, АТАКА SHATTERED, ДИФФЕРЕНЦИАЛ КОЛЛИЗИИ, КРИПТОСТОЙКОСТЬ, ДИФФЕРЕНЦИАЛЬНАЯ ХАРАКТЕРИСТИКА.

Объект исследования: криптографические функции хеширования.

Предметом исследования являются коллизии функций хеширования.

Целью магистерской диссертации является разработка алгоритмов построения коллизий криптографических функций хеширования.

Криптографические функции хеширования используются: при авторизации, для хранения пароля, при шифровании, при формировании электронной цифровой подписи и других областях, требующих подтверждения оригинальности данных. Так как криптографические хеш-функции используются для подтверждения неизменности исходной информации, то возможность быстрого отыскания коллизии для них обычно равносильна дискредитации. Если хеш-функция используется для создания цифровой подписи, то умение находить для неё коллизии фактически равносильно умению подделывать цифровую подпись. Поэтому исследование криптостойкости криптографических функций хеширования является весьма актуальной задачей.

В магистерской диссертации были получены следующие результаты:

- Изучены некоторые существующие методы нахождения коллизий в частности дифференциальная атака и туннелирование на примере функции MD5. Так же подробно описаны достаточные условия для построения коллизионных сообщений.
- Рассмотрен практический взлом алгоритма SHA-1 под названием SHAttered. И реализация данной атаки для построения pdf-файлов с одинаковым хешем
- Проанализированы некоторые способы разработки алгоритма построения коллизий.

The master's thesis contains: 30 pages, 8 tables, 2 illustrations, 11 references.

Keywords: HASH FUNCTION, MD5, COLLISION, SHA-1, DIFFERENTIAL ATTACK, TUNNELING, SHATTERED ATTACK, COLLISION DIFFERENTIAL, CRYPTOGRAPHIC STABILITY, DIFFERENTIAL CHARACTERISTIC.

Object of research: cryptographic hashing functions.

The subject of the study is the collisions of hashing functions.

The purpose of the master's thesis is to develop algorithms for constructing collisions of cryptographic hashing functions.

Cryptographic hashing functions are used: for authorization, for storing a password, for encryption, for forming an electronic digital signature, and in other areas that require confirmation of the originality of the data. Since cryptographic hash functions are used to confirm the immutability of the original information, the possibility of quickly finding a collision for them is usually tantamount to discrediting. If a hash function is used to create a digital signature, then the ability to find collisions for it is actually equivalent to the ability to forge a digital signature. Therefore, the study of the cryptographic strength of cryptographic hashing functions is a very urgent task.

In the master's thesis, the following results were obtained:

- Some existing methods of finding collisions are studied, in particular, differential attack and tunneling on the example of the MD5 function. Sufficient conditions for constructing collision messages are also described in detail.
- A practical hacking of the SHA-1 algorithm called SHAttered is considered. And the implementation of this attack to build pdf files with the same hash
- Some ways of developing the algorithm for constructing collisions are analyzed.