Домашнее задание №1

Виталий Емельянов

11 мая 2016 г.

Описание алгоритма

- существует зашитый в коде словарь subDict с допустимыми подстановками символов
- в функции findCollision:
  - с помощью функции generateSubstitution()генерируется 2^{24} случайных допустимых подстановок для строки с данными пользователя user_data
  - каждая из подстановок сохраняется в словаре userHashes, где в качестве ключа находится sha48 от подстановки, а в качестве значения mask - закодированная в int подстановка (если хранить в качестве значения саму подстановку, то оперативной памяти в 4Гб не хватает)
  - генерируется допустимая случайная подстановка над строкой attacker_data, пока sha48 от нее не будет найден в словаре userHashes
  - в случае совпадения хешей на предыдущем шаге, вызывается функцию recoverData(), от userHashes[attacker_hash], которая восстанавливает подстановку из целого числа mask
- время нахождения коллизии для sha48 заняло около 122 минут (утилита time)