Хешування рядків. Хеш-функції

Лаворик Ольга, 1к. маг., ФВЕ

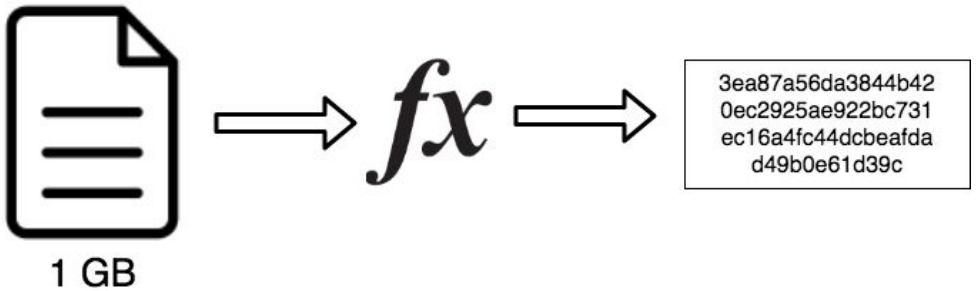
Що таке хешування

Ввід інформації будь-якої довжини та розміру та отримання на виході результату фіксованої довжини, заданого функцією хешування.

INPUT	HASH
Hi	639EFCD08ABB273B1619E82E78C29A7DF02C1051B1820E99FC395DCAA3326B8
Welcome	53A53FC9E2A03F9B6E66D84BA701574CD9CF5F01FB498C41731881BCDC68A7C8

Властивості хеш-функції

- **Детермінізм** - скільки б разів не аналізувати один і той же результат через хеш-функцію, на виході один і той же результат
- **Швидке обчислення -** висока обчислювальна швидкість
- **Складність зворотнього обчислення** F(x) -> Y, !=F^{-1} ,Y -?
- **Стійкість до колізій** якщо H(A) = H(B), то A = B.



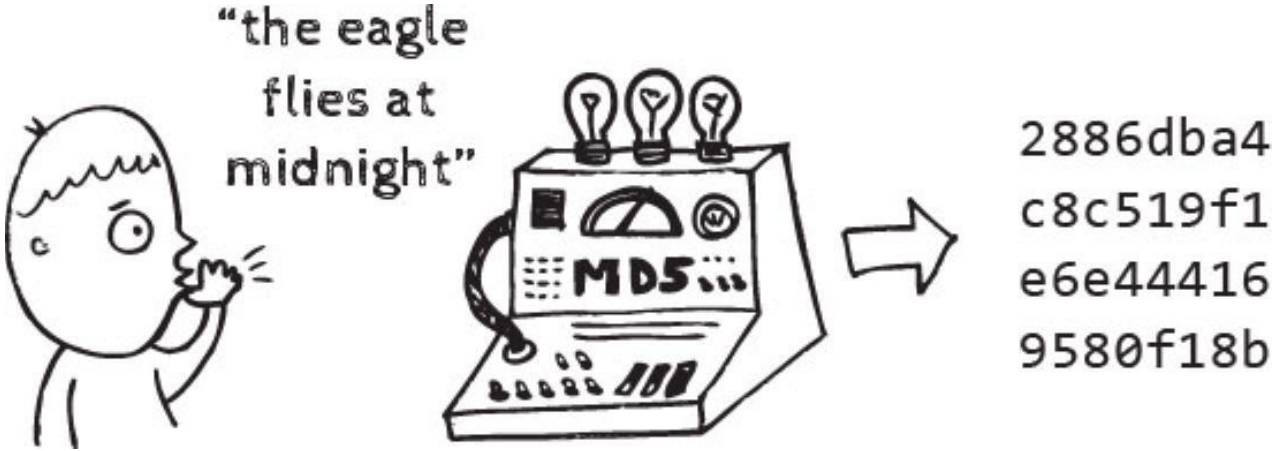
Алгоритми хешування

- SHA-256
- SHA-1, SHA-2, SHA-3
- MD5

Застосування

- Перевірка цілісності файлів
- Верифікація паролів
- Цифровий підпис
- Блокчейн

Одним із найбільш очевидних та дієвих методів вгадати хеш є метод “грубої сили”

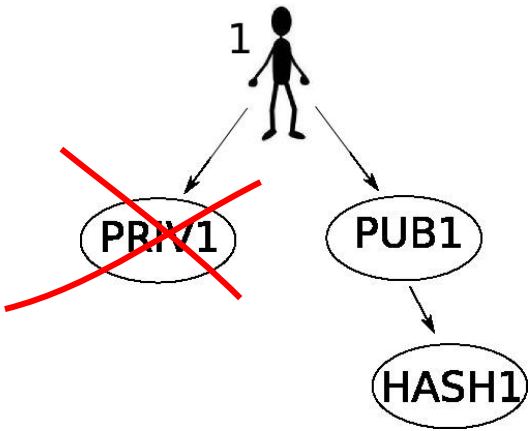


Додаткові параметри

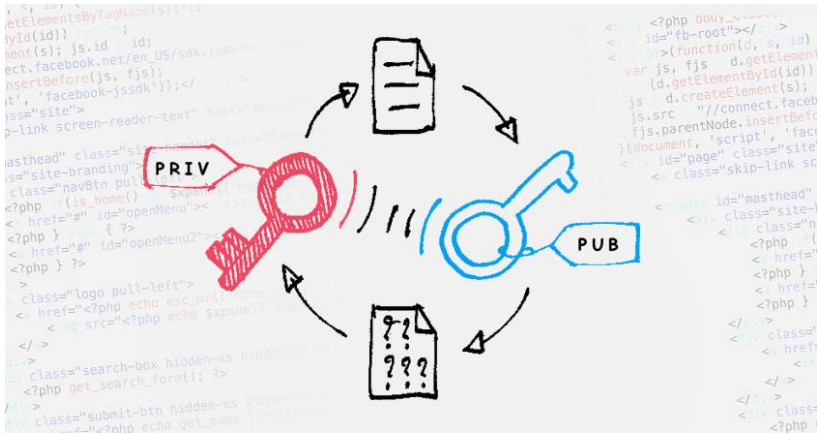
- **myString+some_random_string,**
  але не
  some_random_string+myString
- **myString+some_random_string+ano**
  ther_random_string,
  another_random_string не
  зберігається у базі даних

Види хешування за типом ключа

Симетричне (один ключ)



Асиметричне(два ключі - приватний та публічний)



Хешування та майнінг Bitcoin

Використовується double SHA-256

version	02000000
previous block hash (reversed)	17975b97c18ed1f7e255adf297599b55 330edab87803c8170100000000000000
Merkle root (reversed)	8a97295a2747b4f1a0b3948df3990344 c0e19fa6b2b92b3a19c8e6badc141787
timestamp	358b0553
bits	535f0119
nonce	48750833
transaction count	63
coinbase transaction	
transaction	
...	

Block hash

0000000000000000 e067a478024addfe cdc93628978aa52d 91fabd4292982a50

Дякую за увагу!