Cryptographic hash 101

그 패스워드 해싱은 틀렸다.

P-NP Problem

결정문제 (답이 **true or false**인 것)

P : 결정 문제중, 다항시간 안에 풀 수 있는가?

NP : 결정 문제중, 다항시간 안에 검산 할 수 있는가?

P-NP Problem

{ -3, 5, 7, 2, 1, 0 } 에서 합이 **0**이 되는 부분집합이 존재하는가?

{ -3, 2, 1 }은 합이 **0**이되는 부분집합인가**?**

Hash

Hash vs Cryptographic Hash

- **Hash**를 보고 입력값을 찾기 어려워야함
- 입력의 **Hash**를 유지하면서 입력을 변경하기 어려워야함

HashDos

해시 충돌을 의도적으로 발생시키는 **DDoS** 공격

Java HashMap, javascript Map, python dict ...

입력이 같으면, 출력이 같다.

해시충돌을 무수히 많이 발생시킨다면?

Hash

Hash vs Cryptographic Hash

- **Hash**를 보고 입력값을 찾기 어려워야함
- 입력의 **Hash**를 유지하면서 입력을 변경하기 어려워야함
- **(new!) Hash**가 같은 두 입력을 찾기 어려워야함 **(**심지어는 같은 입력이라도**, prefix**가 같으면 안됨**)**

md5

입력에 대해 **128**비트 **(**보통 **16**진수 **32**자리**)** 의 출력을 만듬

Hash Collision 공격에 취약함
일부 고속연산이 필요한 경우, 사용되는곳들이 있음 **(**물리장비 등**)**

https://shattered.io

sha-1

입력에 대해 **160**비트 (보통 **16**진수 **40**자리) 의 출력을 만듬

무려 **05**년부터 위험성을 알고있었음

현재 쓰는곳이 있다면, 당장 바꿔야함

https://shattered.io

틀렸다.

salt와 **password**를 복잡하게 만들었으니

안전하다고 생각하면

틀렸다.

DB가 침해당해도 암호화 되어있으니 괜찮다는 생각은

틀렸다.

sha-256을 **password hash** 로 사용하는 것은

틀렸다.

sha-256에 **salt**를 붙였으니 안전하다고 생각하면

Hash Performance

Hash-Mode 1400 (SHA2–256 / RTX 4090)

- Speed.#1.....: 13567.2 MH/s (51.56ms)
- Speed.#2.....: 605.4 MH/s (81.58ms)
- Speed.#*.....: 14172.6 MH/s

비트코인 채굴과의 관계

비트코인 채굴 : 해당 **sha-256 hash**를 깨는 과정

비트코인 채굴 초창기 **(2010**년대 기준**) :** 그래픽 카드

현재 **: ASIC, FPGA**

H/W 의 발전

저장장치는 매우 저렴해짐 (8TB 하드디스크가 단돈 20만원)

메모리는 별로 저렴해지지 않았다. (램 가격을 보면 됨)

-> 메모리를 많이 쓰도록 강제하면 된다 !

Password Hash!

argon2 (blake2 를 반복한 hash)

Balloon (sha-3 를 여러번)

yescrypt

Reference.

password-hashing.net

hashcat.net

NIST.SP.800-63B-4.2pd.pdf

https://github.com/veorq/SipHash