**Ethical Hacking and Network Security**

* Cryptography & Steganography

**Hash algorithms**

1. Determinism

→ 같은 input일 경우 같은 output이 나와야 한다.

2. Unique

→ 서로 다른 input은 다른 hash 결과가 나와야 한다.

3. One-way

→ hash 결과로부터 원래 값을 역산할 수 없어야 한다.

4. Fixed length

→ hash 종류에 따른 고정된 output 길이를 가진다.

5. Avalanche effect

→ input의 한 bit만 변경되어도 다른 hash 결과가 생성된다.

Attack on Hash

1. Collision attack

→ 같은 hash 결과를 가지는 다른 두 개의 message를 찾는 것.

2. First preimage attack

→ hash 값이 주어졌을 경우 해당 hash 값을 출력하는 input을 찾는 것.

3. Second preimage attack

→ input이 주어졌을 때 해당 input과 공통된 hash 결과를 갖는 다른 input을 찾는 것.

**Steganography**

secret file을 image, video와 같은 cover file에 삽입하여(embedded) 송/수신 하는 기법

**/etc/shadow**

shadow 파일은 총 7개의 account와 관련된 정보가 저장되어 있는 파일이다.

1. username

2. hashing password

- password 항목은 총 세 개의 항목이 $로 구분되어 있는데 $(hash type)$(salt)$(password) 형식을 가지고 있다.

- type의 경우 1은 MD5, 2a는 blowfish, 2y는 eksblowfish, 5는 sha-256, 6은 sha-512를 의미한다.