

**현대암호학기초**

약한 충돌 내성과 강한 충돌 내성 분석

2018111360이현정

[9조] 송희원, 권혜민, 윤명지, 이현정

**1. 충돌이란?** 2개의 다른 메시지가 같은 해시 값을 갖는 것

**2. 충돌 내성이란?** 충돌을 발견해 내는 것이 어려운 성질

**3. 약한 충돌 내성과 강한 충돌 내성**

약한 충돌 내성이란 어느 메시지의 해시 값이 주어졌을 때, 같은 해시 값을 갖는 다른 메시지를 발견 해 내는 것이 어려워야한다.

즉, 이 주어진 상태에서이고 h(=y, h(=y 일 때, 발견이 어려워야함

강한 충돌 내성이란 해시 값이 일치할 것 같은 서로 다른 2개의 메시지를 발견하는 것이 매우 어려워야한다.

즉, h(=y, h(=y 일 때, 발견이 어려워야한다.

(여기서 약한 충돌 내성이란 강한 충돌 내성과 대비되는 것으로 충돌 내성이 약하다는 의미는 아님)

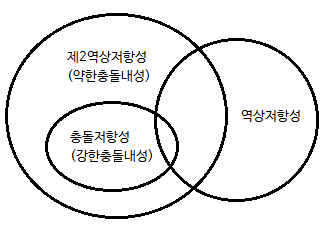
∴ 두가지 충돌 내성은 발견하기 어려워야한다는 공통점이 있지만, 값이 하나 주어짐, 주어지지 않음이 차이점이다.

**4. SHA-512의 약한 충돌 내성과 강한 충돌 내성**

-SHA-512의 약한 충돌 내성 ☞ 주어진 다이제스트와 동일한 다이제스트를 갖는 메시지를 찾는 연산 수행 수는

-SHA-512의 강한 충돌 내성 ☞ 동일한 메시지 다이제스트를 갖는 두 개의 서로 다른 메시지를 찾는 난이도 연산 수행 수는

약한 충돌 내성 속에 강한 충돌 내성이 포함되기 때문에 으로 난이도 연산 수행 횟수가 강한 충돌 내성이 더 적게 수행된다.

https://m.blog.naver.com/furtherme/220787745958 -그림출처