**제목 : 알고리즘 적용 기획서 #2 (회원정보 보호)**

**내용 :** 해싱 알고리즘을 이용한 회원정보 보호 서비스

**적용 알고리즘** : 해싱

**알고리즘 개요**

해시 알고리즘은 작성된 임의의 값을 해시 함수를 통해, 역이 성립하지 않는 특징을 통해, 로그인 등 비밀번호 보안에 활용하고 있습니다.

**[해시 알고리즘의 장점]** **첫 번째**로 **출력 값을 토대로 입력 값을 예측할 수 없**는 비가역적인 성질을 가지는 것입니다. 이러한 특징은 해시 결과값을 보더라도 그 원본 값이 무엇인지 알 수 없기에 비밀번호 등의 정보 보안에 장점을 가지고 있습니다.  
 **두 번째**로는 입력 값의 아주 일부만 변경되어도 전혀 다른 결과 값을 출력한다는 것입니다. 이로써 **결과값을 통해서 입력 값을 추측할 수 없다**는 특징을 가집니다. 이는 첫번째 장점과 마찬가지로 정보 보안에 장점을 가지고 있습니다.  
 **세 번째**로는 어떤 입력 값에도 **항상 고정된 길이의 해시 값을 출력**한다는 것 입니다. 이는 아무리 긴 문장일 입력하더라도 고정된 길이(SHA-256 : 64비트)로 변경된다는 것입니다.

**[해시 알고리즘의 단점]**  
해시 결과가 겹쳐 해시 **충돌이 일어나는 경우가 발생할 수 있다**는 것입니다. 일반적으로 해시 함수로 표현 가능한 개수보다 해시 함수의 입력으로 들어오는 값들이 더 클 수 있기 때문에 모든 값들에 1:1 대응이 가능하다는 보장이 없습니다. 일반적으로 이런 해시 충돌이 발생할 가능성을 염두에 두고 다양한 충돌 방지 알고리즘을 통해서 해결하고 있습니다.

그리고 과거에 사용하던 해시 함수는 동일한 입력 값이 주어진다면 동일한 결과를 받을 수 있기 때문에 쉬운 암호를 사용하는 경우 (1234,9999 등) 다른 사람들과 **해시 결과값이 겹쳐서 예측하기 쉽다**는 것입니다.

**적용 서비스** : 로그인, 회원가입 등 회원정보 관리 적용 서비스 개발 개요

**적용 서비스 개발 개요**

데이터를 입력할 시에는 개인이 확인 가능하도록 하지만 서버와의 통신을 진행할 때에는 해싱 알고리즘을 통해, 개인정보가 보호될 수 있도록 해싱 함수를 적용하였고 적용된 해시 코드는 SHA-256입니다.

해시 코드는 통신을 진행하기 위해서 login, update, regist을 사용할 때 적용시켰으며, 받아진 값 중 동일한 비밀번호에 대해서 같은 결과를 도출하는 것을 막기 위해서 hash 함수를 적용할 때 “ID + Password” 문자열에 대해서 적용시켰으며, 그 값을 DB에 전송 및 저장하는 형태로 진행하였습니다.

[아이디 : a, 비밀번호 : 1234]  
[아이디 : a!, 비밀번호 : 1234]

**비밀번호만 사용 시**

03ac674216f3e15c761ee1a5e255f067953623c8b388b4459e13f978d7c846f4  
03ac674216f3e15c761ee1a5e255f067953623c8b388b4459e13f978d7c846f4

**이이디+비밀번호 사용 시**

3e0a3501a65b4a7bf889c6f180cc6e35747e5aaff931cc90b760671efa09aeac  
7d59015e552b0e88985e1adc16c9eddee4dde7006fcf50074978e140674ebbc2

이 때, DB의 password 필드는 hash결과를 저장하기 위해서 64비트(혹은 그 이상)로 변경해 주었고, 별도의 hash함수를 만들어 적용하도록 하였습니다.