#10 bcrypt 라이브러리로 비밀번호 암호화

- postman을 이용해 회원가입 시 몽고디비 조회해보면 비밀번호가 입력한 값 그대로 저장되어있음 → DB 저장시 암호화 처리 필요


```
_id: ObjectId("62c6f36e50154605eb0bca81")
name: "nurikim"
email: "nuri@gmail.com"
password: "12345"
__v: 0
```


- bcrypt 라이브러리 설치

```
npm install bcrypt --save
```

- 사용법

https://www.npmjs.com/package/bcrypt usage 참고

  - salt 사용→ salt : 비밀번호를 hashing 하는 key값 같은 느낌?
  - hash는 동일한 평문에 대해서 같은 암호화 값을 출력하므로 평문에 임의의 salt 값을 추가하여 다양한 암호화 값을 생성함

  - User 모델에 정보를 저장하기 전에 암호화하는 로직을 추가

```
//boiler-plate/User.js

const bcrypt = require('bcrypt')
const saltRounds = 10 //salt 자릿수

userSchema.pre('save', function(next){
  //save함수 실행 전 pre function실행, 여기서 next는 save 함수 의미
```

```
  var user = this; //userSchema
  if(user.ismodified('password')){ //userSchema에서 password 필드가 변경된 경우만 실행
    bcrypt.genSalt(saltRounds, function(err, salt){
      if(err) return next(err) //에러나면 next 실행

      brypt.hash(user.password, salt, function(err, hash){
      //user.password 평문을 salt로 암호화-> 암호화한 텍스트= hash
      if(err) return next(err)
      user.password = hash
      next()
      })
    })
  }else{
    next()
  }
});
```

[결과]


```
_id: ObjectId("62caae934c0ad1681ea0999d")
name: "test1"
email: "test1@gmail.com"
password: "$2b$10$cK5iYNpUupvevoFqR2uW8OvpJEHfsF6G.WW9QnsMIgNlFjE8o9zrG"
__v: 0
```