Bitcoin 주소 숙제

1. 개인키를 입력받아 Bitcoin 주소를 생성하는 프로그램을 작성하라. 단, 공개키의 크기를 줄이기 위하여 아래와 같은 압축방식으로 생성한다.
   - 개인 키 = k라고 할 때, 공개키 = k * G를 계산 → (x, y) 좌표: 256bit * 2
   - 타원 곡선의 식이 $y^2 = x^3 + 7$ % p. x값을 이용하여 y 값을 계산할 수 있으므로, 공개키에 x 좌표만 포함한다. 단, 하나의 x 값에 두 개의 y 값이 대응되므로, 짝수(양수)와 홀수(음수)를 구분할 필요가 있다.
   - 따라서 public key hash에 사용하는 공개키는 짝수일 경우 0x02 + x 좌표, 홀수일 경우 0x03 + x 좌표를 사용한다.

   압축 공개키를 이용하여 Public Key Hash를 생성한 후, 강의노트의 6페이지와 8페이지에 설명한 알고리즘을 이용하여 Base58Check 인코딩 방식의 주소를 출력한다. (Step-by-step 알고리즘은 첨부한 문서 참조) 실행의 예는 다음과 같다.

```
개인키 입력? 18e14a7b6a307f426a94f8114701e7c8e774e7f9a47e2c2035db29a206321725
공개키 hash = 00f54a5851e9372b87810a8e60cdd2e7cfd80b6e31
비트코인 주소 = 1PMycacnJaSqwwJqjawXBErnLsZ7RkXUAs
```

   RIPEMD160은 Crypto.Hash 모듈을 사용하며, Base58Check 인코딩은 base58check 모듈을 사용한다.

2. 사용자가 특정 문자열로 시작되는 비트코인 주소를 원할 경우가 있다. 공개키 Hash가 00으로 시작되므로, Base58Check 인코딩의 결과로 P2PKH 비트코인 주소는 항상 1로 시작된다. 따라서 주소의 두 번째 문자부터 원하는 문자열을 입력하면, 이 주소를 생성하는 개인키를 찾아서 공개키와 함께 출력하라. 단, 개인키는 random으로 만들고 생성된 주소가 사용자가 원하는 문자열과 같은지 확인하므로, 사용자의 문자열이 길어질수록 많은 검사가 필요하고 시간이 길어진다. 확률적으로는 문자열의 길이가 x이면, 58^x만큼의 검사가 필요하다.

```
희망하는 주소의 문자열? LG
개인 키 = ddad6ba2ceef0bbb1404e7a9bc33ddab098885678be0a79a14e9a802844674f9
주소 = 1LGy3W4rhPAY3HzmzVqq38GTgLhCuQKNM9
```