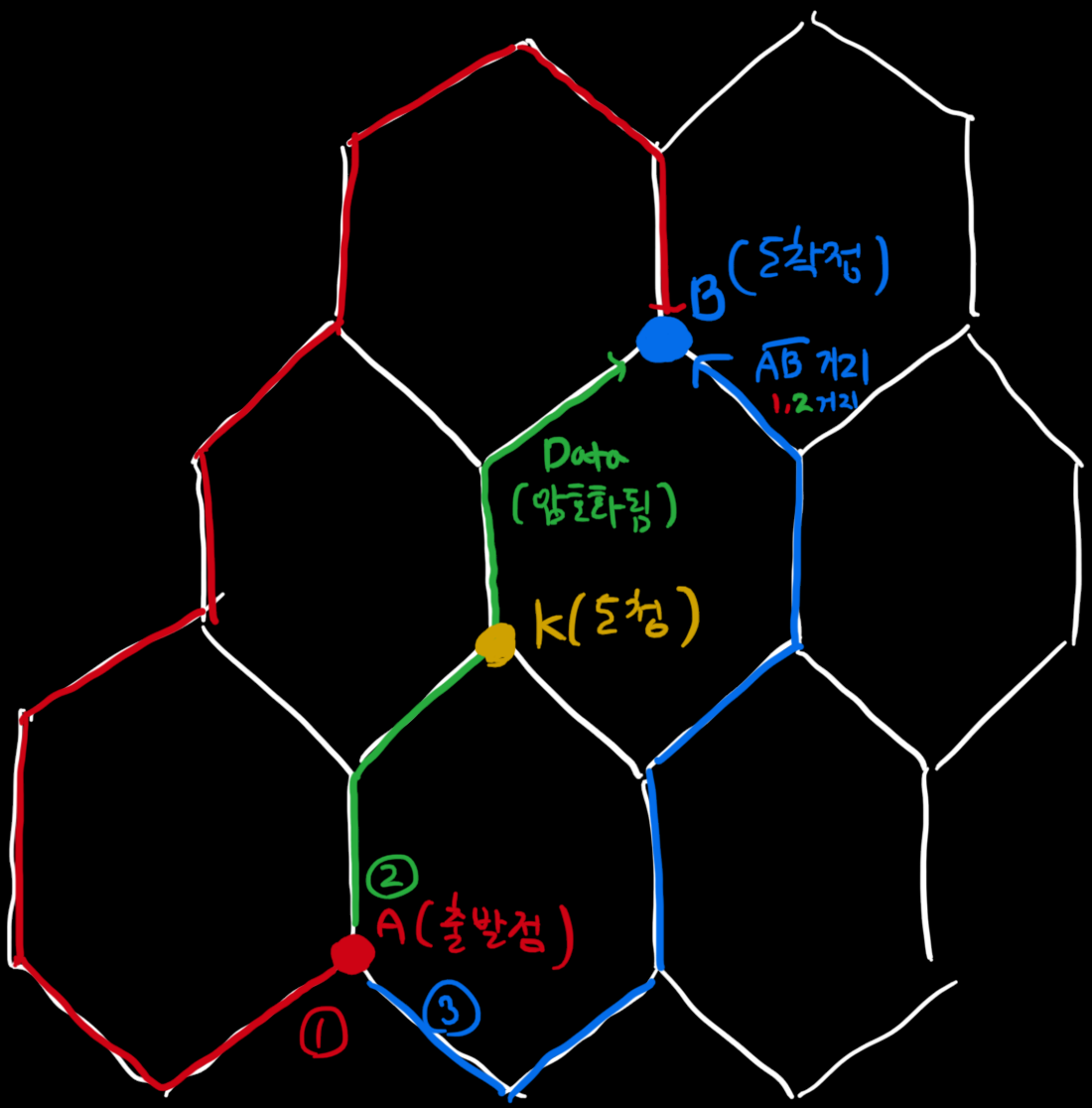
THE HONEYCOMB SEC



Part I : A

Data (정수)를 보낼 때

Data Prime = (Data^③거리) x ③거리 x ①거리

를 해서 Data Prime을 보낸다.

①에서 ③의 거리를 보낸다.

②에서는 Data Prime의 값을 보내는데,

② 를 전달하는 과정에서 각 Class 를 넘어갈 때

Data (정수) 값에서 1씩 뺀다.

③ 에서 ② 의 거리와 ① 의 거리를 B 로 보낸다.

Part II : B

받은 데이터 : Data Prime − ② 거리

- ① 거리
- ② 거리
- ③ 거리

예) DP = ①② $D^{③}$ − ②

처리 방법 :

$$D = \sqrt[③]{\frac{(DP + ②)}{①②}}$$ 로 원래 Data 복원.

Security :

①, ②, ③ 의 중간에서 데이터를 읽어낸다고 하더라도

출발점을 알 수 없으므로 (Data Prime 에서 뭘 빼야 하는지 모르므로)

결론적으로 Data 의 원래 값을 알 수 없다.

Example) 8 이라는 숫자를 보내는 경우.

A :

① = 10

② = 4

③ = 6

$DP = 10 \times 4 \times 8^6 - 4$

$= 2^{18} \times 2^2 \times 2 \times 5 - 2^2$

$= 2^{21} \times 5 - 2^2$

B:

$$D = \sqrt{\frac{(2^{21} \times 5 - 2^2 + 2^2)}{10 \times 4}} = \sqrt{\frac{2^{21} \times 5}{10 \times 4}}$$

$$= \sqrt{\frac{2^{21} \times 5}{2^3 \times 5}} = 8$$

만약 누군가가 k 점에서 도청하여 Data Prime을 읽어내고, 운이 (매우) 좋아 ① ② ③을 모두 읽어 냈다고 하더라도, Data Prime을 읽어낸 k 점이 A로부터 얼마나 먼지 모르므로 절대 Data의 값을 얻을 수 없다.