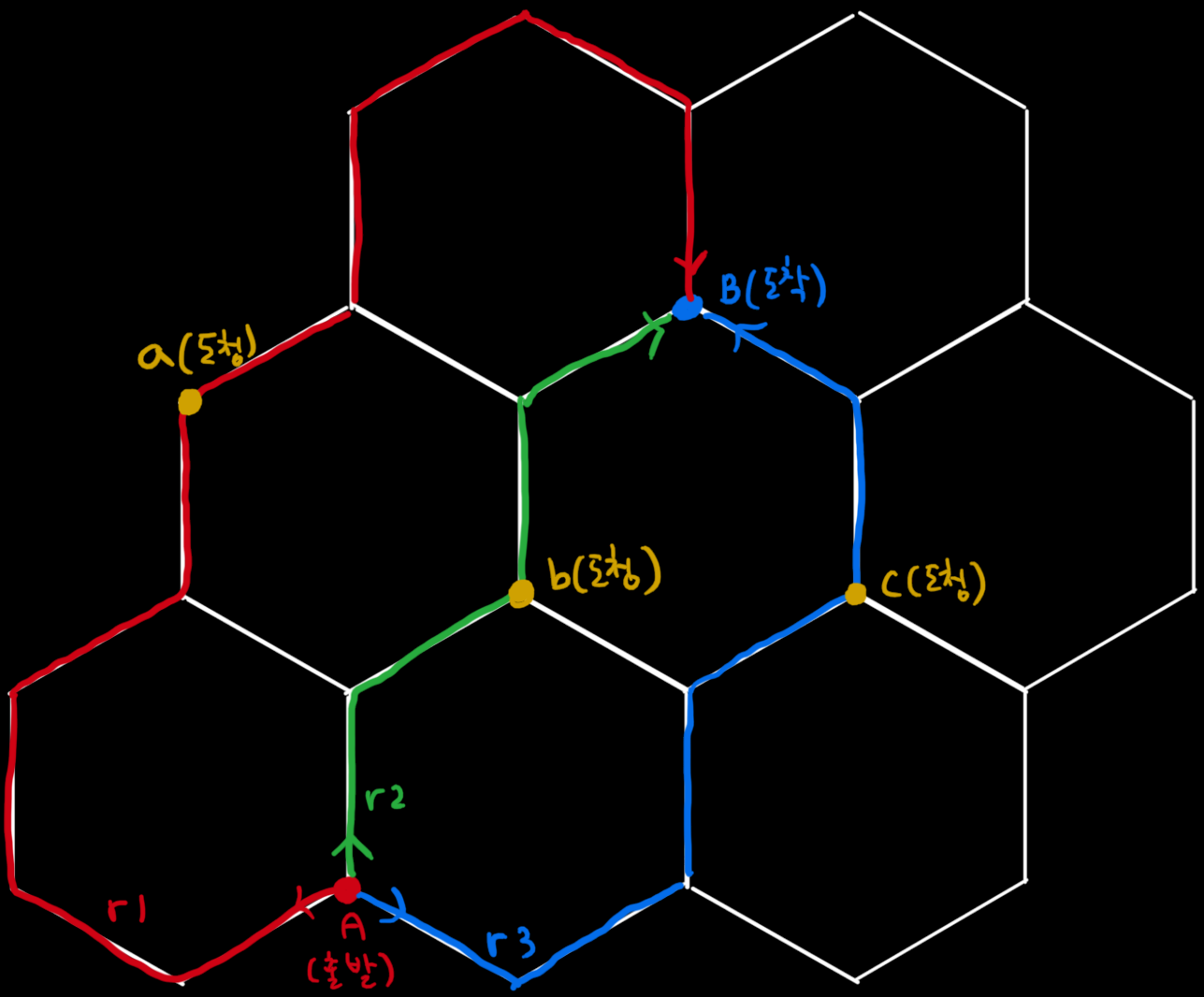
The Honeycomb Sec II



Part I : A

D라는 정보를 보낼 때,

r1 = (r1의 거리)

r2 = (r2의 거리)

r3 = (r3의 거리)라고 정한다.

D_p 에 암호화된 데이터 D를 보낸다.

$D_p = r1\, r2\, r3\, D^{r3}$ 를 정의하자.

다음과 같이 신호를 보낸다.

Route 1 : r3 의 값을 보내는데, 육각형의 한 꼭짓점을 지날 때마다 1씩을 뺀다.

Route 2 : D_p의 값을 보내는데, 육각형의 한 꼭짓점을 지날 때마다 $r2^{r2}$씩을 뺀다.

Route 3 : r1의 값을 그대로 보낸다.
r2의 값을 보내는데, 육각형의 한 꼭짓점을 지날 때마다 1씩을 뺀다.

Part Ⅱ : B

다음과 같이 신호를 받는다.

Route 1 : (r3 − r1)의 값을 받는다. ⇒ R1

Route 2 : $(D_p - r2^{r2})$의 값을 받는다. ⇒ R2

Route 3 : r1의 값과 (r2 − r3)의 값을 받는다. ⇒ R3a ⇒ R3b 라 놓자.

위의 데이터들을 조합해

$$\begin{cases} r1 = R3a \\ r2 = R3b + R1 + R3a \end{cases}$$

$$\begin{cases} r3 = R1 + R3a \\ Dp = R2 + (R3b + R1 + R3a)^{2\times(R3b+R1+R3a)} \end{cases}$$

의 값들을 얻을 수 있다.

$Dp = r1\,r2\,r3\,D^{r3} - r2^{2\,r2}$ 였으므로

$$Dp + r2^{2\,r2} = r1\,r2\,r3\,D^{r3}$$

$$\frac{Dp + r2^{2r2}}{r1\,r2\,r3} = D^{r3}$$

$$\therefore D = \sqrt[r3]{\frac{Dp + r2^{2r2}}{r1\,r2\,r3}}$$ 를 기준에 A가 암호화한 데이터를 얻을 수 있다.

Example)

8이라는 Data를 보내는데,

$r1 = 10$, $r2 = 4$, $r3 = 6$ (맨 위 그림과 같음)

$Dp = 10\times4\times6\times8^6$

$= 62914560$

B는 다음을 수신함.

r1에서.. -4

r2에서.. 62849024

r3에서.. 10, -2

이를 조합해서 기존 데이터를 모두 얻음.

$$\therefore D = \sqrt[6]{\frac{62849024+65536}{10\times4\times6}}$$

$$= 8.$$

Security:

도청자의 입장을 보자.

도청자는 위 그림에서 a, b, c에서 정보를 듣고 있다.

그러나, r1과 r2를 구별할 수 없기 때문에

2가지의 경우를 나누어 생각해야 한다.

다음과 같은 데이터를 받는다.

- $r3 - a$
- $Dp - b r2^{r3}$
- $r1$
- $r2 - c$

이때, 각 데이터가 무슨 데이터를 의미하는지 알고 있다고 가정할 때,

a, b, c 세 가지의 미지수가 있기 때문에

무수히 많은 경우의 수가 생긴다.

또한, 이 무수히 많은 경우의 수를 일일이 대입해 보며

Data의 값이 나온다고 하더라도

이중 어떤 것이 Data 인지를 알 수 없을 것이다.