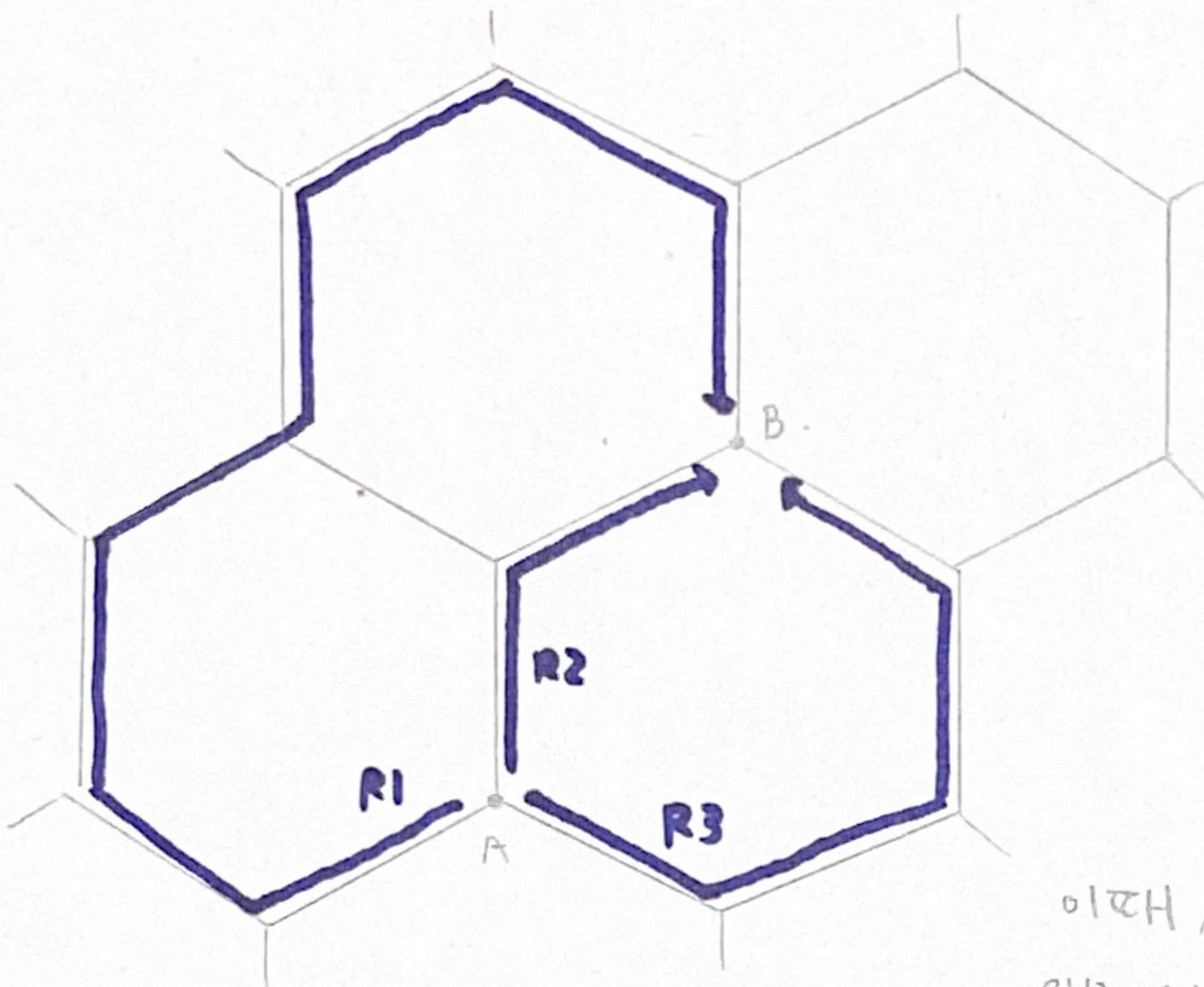


HONEYCOMB ENCRYPTION MODEL III

By. JOENSUNG KIM.



A 지점에서 B 지점으로 연결되는 통로가
R₁, R₂, R₃ 3개이다.

$$\begin{cases} r_1 = (R_1 \text{의 길이}) \\ r_2 = (R_2 \text{의 길이}) \\ r_3 = (R_3 \text{의 길이}) \text{라고 정하자.} \end{cases}$$

A는 B에게 D라는 암호를 보내려고 하고,
중간에서 이를 가로채도 알 수 없도록
암호화를 해서 보낸다.

이때, A와 B는 모두 r₁, r₂, r₃의 값을 알고 있으며,
이부에서는 이를 몰랐다고 가정하자.

1. k = r₁ + r₂ + r₃라고 하자.

k±1, k±2...를 하여 k에 가장 가까운 소수(Prime number)를 찾아
P_r이라고 하자.

2. D = d₁ + d₂ + d₃가 되도록 임의의 정수 d₁, d₂, d₃를 정한다.

이들을 d_n이라고 부르도록 한다.

3. 소인수분해했을 때 P_r의 지수가 d_n인, 가장 작은 h! (factorial)를 구한다.

경로 R_n을 통해 h!를 보내는데,

한 번을 이동할 때마다 10000 쪽을 뺀다.

4. B는 결과적으로 h! - r_n × 10⁴의 값을 받게 된다.

이를 f라고 정의하자, 여기에 수를 더해 h의 값을 구한다.

르장드르 공식을 통해 d_n의 값을 알아낼 수 있다.

$$d_n = \sqrt[p]{h!} = \sum_{k=1}^{\infty} \left[\frac{h}{p^k} \right]$$

5. 위의 공식을 통해 d₁, d₂, d₃를 모두 찾아 더하면

A가 원래 보내려고 했던 D의 값을 알 수 있다.

* 르장드르 공식 (Legendre's formula)

$$\sqrt[p]{n!} = (n! \text{을 소인수분해 시 } p \text{의 지수})$$

$$\text{ex) } \sqrt[3]{10!} = 4$$

이를 공식을 적용했을 때

$$\sqrt[p]{n!} = \sum_{k=1}^{\infty} \left[\frac{n}{p^k} \right] \text{이 나온다}$$