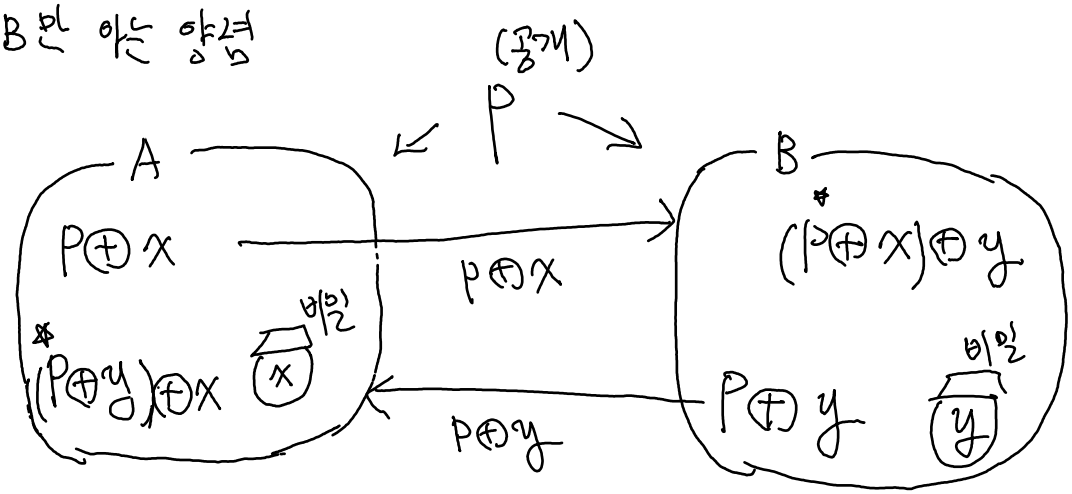
Diffie-Hellman key exchange

- 중요한 데이터를 공개된 통신망을 이용하여 공유하는 방법.
- Operation s.t 정방향 계산은 빠르고, 역방향계산은 매우 느림.
  그리고 교환법칙이 성립함. (그런 Operation이 필요하다)

- 예 ⊕
  - 양변에 operation은 역방향(양변분리)은 불가능,
    양변 x, 양변 y를 섞는것은 양변 y, 양변 x 섞는것과 같다 (교환법칙)

  - A와 B는 서로 양변비법을 (공개된 공간에서) 비밀리에 공유하고 싶다.

    P : 모두에게 공개된 양변
    x : A만 아는 양변
    y : B만 아는 양변



P⊕x를 P와 x로 분리불가능

P⊕y⊕x 가 공유되었다. ∎

(SNU, 이광근교수)

- 실제 Operation

- P: 소수 (공개), x, y는 각각 비밀

- ⊕ : $P \oplus x = 2^x \bmod P$

P⊕x 값은 공개

2^x 실수일지라도 (P, x 모두 비밀키)

- $(P \oplus x) \oplus y = (2^x \bmod P)^y \bmod P$ ... ①

서로 공유되는 key

$(P \oplus y) \oplus x = (2^y \bmod P)^x \bmod P$ ... ②

①

Let $2^x = Pk + r \quad (0 \le r < P)$

$2^x \bmod P = 2^x - Pk$

$(2^x \bmod P)^y = (2^x - Pk)^y = (2^x)^y \cdot (Pk)^0$

$+ C_1 (2^x)^{y-1} \cdot (Pk)^1 + \cdots + C (2^x)^0 \cdot (Pk)^y$

↳ ($\bmod P = 0$)

$\therefore (2^x \bmod P)^y \bmod P = 2^{xy} \bmod P$ ⇒ 비밀리 공유되는 key

②도 $2^{yx} \bmod P$

교환법칙 성립 ⇒ 그런 operation 찾는 것