정수론 17강 공개키 암호

「HELLO」 문자열 아스키코드

104 101 108 108 111

104 101 108 108 111 char

암호화 복호화 (해독) 암호화

* 공개키 암호

a : 메세지 (평문) , b : 암호문

큰 소수 2개를 뽑아서 p, q 라고 하자. $m = pq$.

$\phi(m) = (p-1)(q-1)$

$\phi(m)$과 서로소인 k를 뽑자.

$a^k \pmod m$ → 연속제곱법을 이용

$a^k \equiv b \pmod m$

k, m, b $x^k \equiv b \pmod m$ → 방정식 $\gcd(b, m) = 1$, $\gcd(k, \phi(m)) = 1$

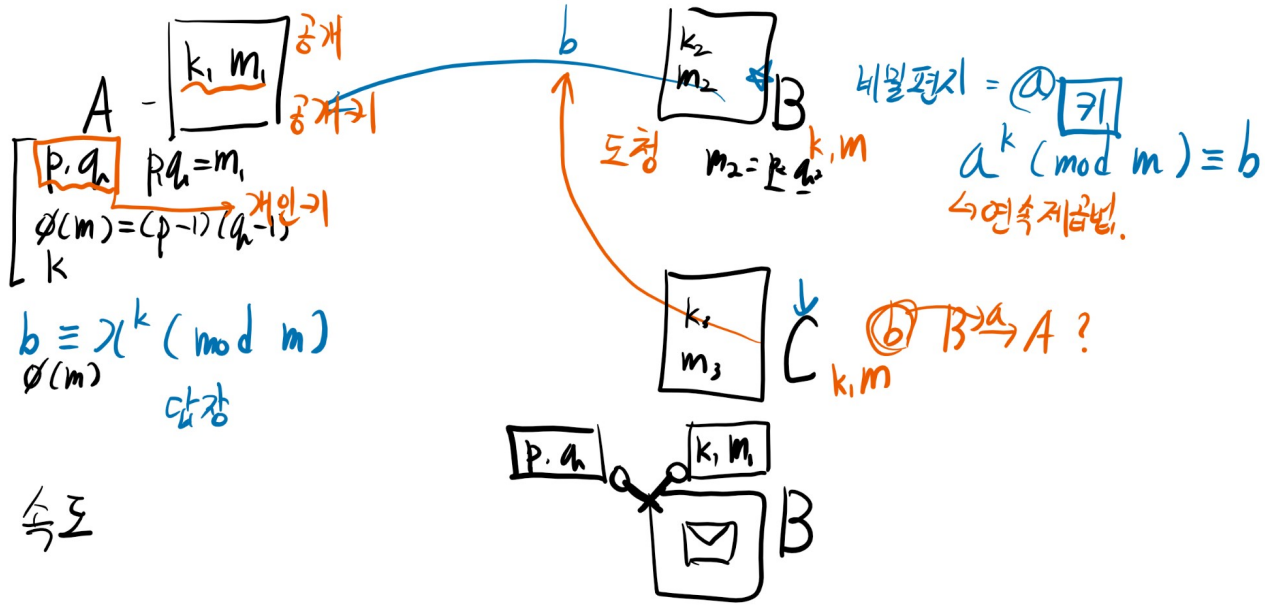
↳ a $m = p \cdot q$ ⇒ 시간이 오래 걸린다.

⇒ $\phi(m)$을 구한다. $\phi(m) = (p-1)\cdot(q-1)$

k의 mod $\phi(m)$에 대한 역원을 구한다. (확장된 유클리드 알고리즘)

$ku \equiv 1 \pmod{\phi(m)} \Rightarrow ku - \phi(m)v = 1$ (u, v)를 찾자.

$b^u \pmod m$ ⇒ a가 된다.



★ 대칭키 암호