

정수를 17장 공개키 암호

「HELLO」 문자열 아스키코드

104 101 108 111

104 101 108 111 char  
암호화 암호화  
복호화(해독)

\* 공개키 암호

$a$ : 메시지 (평문),  $b$ : 암호문

큰 소수 2개를 뽑아서  $p, q$  하자.  $m = pq$ .

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

$\phi(m)$ 과 서로소인  $k$ 를 뽑자.

$a^k \pmod{m} \rightarrow$  연속제곱법을 이용

$$a^k \equiv b \pmod{m}$$

$k, m, b$

$$a^k \equiv b \pmod{m} \rightarrow \text{방정식} \quad \gcd(b, m) = 1, \gcd(k, \phi(m)) = 1$$

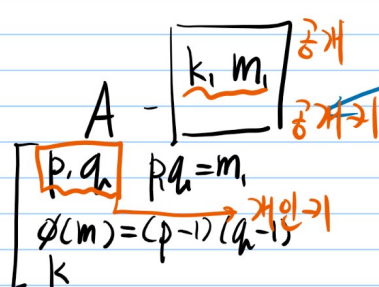
$m = p \cdot q \Rightarrow$  시간이 오래 걸린다.

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

$k$ 의  $\text{mod } \phi(m)$ 에 대한 역원을 구한다. (확장된 유클리드 알고리즘)

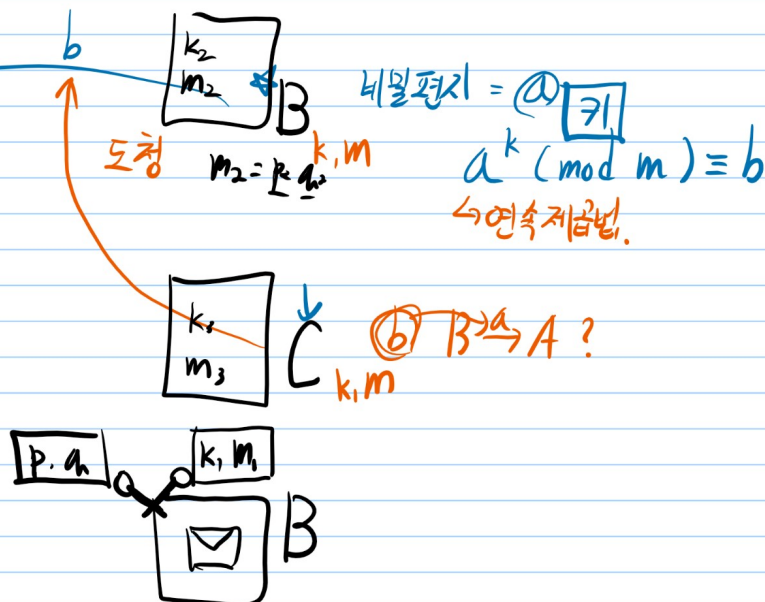
$$ku \equiv 1 \pmod{\phi(m)} \Rightarrow ku - \phi(m)v = 1 \quad (u, v) \text{를 찾자.}$$

$$b^u \pmod{m} \Rightarrow a \text{가 된다.}$$



$$b \equiv a^k \pmod{m}$$

속도



\* 대칭키 암호

