

# 정수론 18강 공개키 암호 예제

## ① 암호화

- 큰 소수 2개,  $p=7, q=13$   $m=7 \cdot 13 = 91$

-  $\phi(m)$ 과 서로소인  $k$ 를 선택

$$\phi(m) = \phi(91) = \phi(7) \phi(13) = 6 \cdot 12 = 72$$

$k=5$

- 메시지  $a=9$  (평문)

-  $a^k \pmod{m} \rightarrow$  연속제곱법

$$9^5 \pmod{91} \quad 5 = \overset{2^2}{10} \overset{2^0}{1} \overset{2^0}{1} (2) = 2^2 \cdot 1 + 2^1 \cdot 0 + 2^0 \cdot 1 = \underline{2^2 + 2^0}$$

$$9^2 \equiv 81 \pmod{91}$$

$$9^4 \equiv 81^2 \equiv 9 \pmod{91} \Rightarrow 9^5 \equiv 9^{2^2+2^0} \equiv 9^{2^2} \cdot 9^{2^0} \equiv 9^4 \cdot 9^1 \equiv 9 \cdot 9 \equiv 81 \pmod{91}$$

81 (암호문)

공개키: 5, 91

## ② 복호화

$$x^5 \equiv 81 \pmod{91} \quad 91 = 7 \cdot 13$$

$$\phi(m) = \phi(p) \phi(q) = 6 \cdot 12 = 72$$

$5^{-1} \pmod{\phi(m)} \Rightarrow$  확장된 유클리드 알고리즘

$$\hookrightarrow 5 \cdot u \equiv 1 \pmod{\phi(m)} \quad 5 \cdot u = \phi(m) \cdot v + 1$$

$$5 \cdot u - \phi(m) \cdot v = 1 \quad (u, v) \text{ 를 찾자}$$

| u   | v  | 5u - 72v                |
|-----|----|-------------------------|
| 0   | -1 | 72                      |
| 1   | 0  | 5                       |
| -14 | -1 | 2 $\times -2$ 72(mod 5) |
| 29  | 2  | 1 $\times -2$ 5(mod 2)  |

$\hookrightarrow \gcd(5, 72)$

$$\left. \begin{array}{l} 72 = 14 \cdot 5 + 2 \\ 5 = 2 \cdot 2 + 1 \end{array} \right\} \begin{array}{l} \text{몫} \\ \text{나머지} \end{array}$$

$$u \equiv 29 \pmod{\phi(m)}$$

$$81^{29} \equiv ? \pmod{91} \quad \text{연속제곱법 (중국인 나머지 정리)}$$

\* 연속제곱법 이용

$$\begin{array}{r} 2 \overline{) 29} \\ 2 \overline{) 14} \quad 1 \\ 2 \overline{) 7} \quad 0 \\ 2 \overline{) 3} \quad 1 \end{array} \quad \begin{array}{l} = 11101 (2) \\ = 2^4 + 2^3 + 2^2 + 2^0 \end{array}$$

$$\begin{aligned}
 81^2 &\equiv 9 \pmod{91} \\
 81^4 &\equiv 9^2 \equiv 81 \pmod{91} \\
 81^8 &\equiv 81^2 \equiv 9 \pmod{91} \\
 81^{16} &\equiv 9^2 \equiv 81 \pmod{91}
 \end{aligned}$$

$$\begin{aligned}
 81^{29} &\equiv 81^{2^4 + 2^3 + 2^2 + 2^0} \\
 &\equiv 81^{2^4} \cdot 81^{2^3} \cdot 81^{2^2} \cdot 81^{2^0} \\
 &\equiv 81^{16} \cdot 81^8 \cdot 81^4 \cdot 81^1 \\
 &\equiv 81 \cdot 9 \cdot 81 \cdot 81 \\
 &\equiv 81 \cdot 9 \cdot 9 \equiv 81 \cdot 81 \equiv 9 \pmod{91}
 \end{aligned}$$

\* 중국인 나머지 정리 이용

$$81^{29} \pmod{91} \equiv x \quad p=7, q=13$$

$$\begin{aligned}
 x \pmod{p} &\Rightarrow 81^{29} \pmod{7} \quad \phi(7)=6 \quad 81^{24+5} \equiv 81^5 \pmod{7} \\
 81^{29} &\equiv 81^5 \equiv 4^5 \equiv 16 \cdot 16 \cdot 4 \equiv 2 \cdot 2 \cdot 4 \equiv 4 \cdot 4 \equiv 16 \equiv 2 \pmod{7}
 \end{aligned}$$

$$\begin{aligned}
 x \pmod{q} &\Rightarrow 81^{29} \pmod{13} \quad \phi(13)=12 \\
 &\Rightarrow 81^{29} \equiv 9 \pmod{13}
 \end{aligned}$$

$$\begin{aligned}
 81^{29} &\equiv 2 \pmod{7} \\
 81^{29} &\equiv 9 \pmod{13}
 \end{aligned}$$

$$81^{29} \equiv \text{?} \pmod{91}$$

해를 가진다. (중국인 나머지 정리)

$$\Rightarrow \equiv 7 \cdot A + 13 \cdot B \pmod{91}$$

$$\hookrightarrow \pmod{7} \quad 13 \cdot B \equiv 2 \pmod{7} \Rightarrow 6 \cdot B \equiv 2 \pmod{7} \quad B \equiv 5 \pmod{7}$$

$$\begin{aligned}
 \hookrightarrow \pmod{13} \quad 7 \cdot A &\equiv 9 \pmod{13} \Rightarrow A \equiv 5 \pmod{13} \\
 &\hookrightarrow 2 \cdot 7 = 14 \equiv 1 \pmod{13}
 \end{aligned}$$

$$81^{29} \equiv 7 \cdot 5 + 13 \cdot 5 \pmod{91}$$

$$\equiv 35 + 65 \equiv 100 \equiv 9 \pmod{91}$$

$$\begin{array}{ccccc}
 7 & 14 & 21 & 28 & 35 \\
 8 & 15 & 22 & 29 & 36
 \end{array}$$

$$6 \cdot 6 \equiv 36 \equiv 1 \pmod{7}$$

확장된 유클리드 알고리즘