정수론 18강 공개키 암호 예제

① 암호화

- 큰 소수 2개, $p=7$, $q=13$ $\quad m = 7\cdot 13 = 91$
- $\phi(m)$과 서로소인 k를 선택

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

$k = 5$

- 메세지 $a = 9$ (평문)
- $a^k \pmod m$ → 연속제곱법

$9^5 \pmod{91}$ $\quad 5 = 101_{(2)} = 2^2\cdot 1 + 2^1\cdot 0 + 2^0\cdot 1 = 2^2 + 2^0$

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

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

$\equiv 9\cdot 9 \equiv 81 \pmod{91}$

81 (암호문)

공개키 : 5, 91

② 복호화

$x^5 \equiv 81 \pmod{91}$ (소인수 분해가 어렵다.) $\quad 91 = 7\cdot 13$

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

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

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

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

u	v	$5u - 72v$
0	-1	72
1	0	5
-14	-1	2
29	2	1

$\times -2$ $\quad 72 \pmod 5$, $5 \pmod 2$

↳ gcd(5, 72)

$72 = 14\cdot 5 + 2$ (몫, 나머지)

$5 = 2\cdot 2 + 1$

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

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

* 연속제곱법 이용

$29 = 11101_{(2)} = 2^4 + 2^3 + 2^2 + 2^0$

2 | 29	1
2 | 14	0
2 | 7	1
2 | 3	1

$81^2 \equiv 9 \pmod{91}$
$81^4 \equiv 9^2 \equiv 81 \pmod{91}$
$81^8 \equiv 81^2 \equiv 9 \pmod{91}$
$81^{16} \equiv 9^2 \equiv 81 \pmod{91}$

$81^{29} \equiv 81^{24+2^3+2^2+2^0}$
$\equiv 81^{24} \cdot 81^{2^3} \cdot 81^{2^2} \cdot 81^{2^0}$
$\equiv 81^{16} \cdot 81^8 \cdot 81^4 \cdot 81^1$
$\equiv 81 \cdot 9 \cdot 81 \cdot 81$
$\equiv 81 \cdot 9 \cdot 9 \equiv 81 \cdot 81 \equiv 9 \pmod{91}$

* 중국인 나머지 정리 이용

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

$x \pmod{p} \Rightarrow 81^{29} \pmod{7}$ $\quad \phi(7)=6$ $\quad 81^{24+5} \equiv 81^{6\cdot4} \cdot 81^5$
$81^{29} \equiv 81^5 \equiv 4^5 \equiv 16 \cdot 16 \cdot 4 \equiv 2 \cdot 2 \cdot 4 \equiv 4 \cdot 4 \equiv 16 \equiv 2 \pmod{7}$

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

$81^{29} \equiv 2 \pmod{7}$
$81^{29} \equiv 9 \pmod{13}$

$81^{29} \equiv \pmod{91}$
↳ 해를 가진다. (중국인 나머지 정리)
↳ $\equiv 7 \cdot A + 13 \cdot B \pmod{91}$

7	14	21	28	35
8	15	22	29	36

$6 \cdot 6 \equiv 36 \equiv 1 \pmod{7}$
확장된 유클리드 알고리즘

↳ $\pmod{7}$ $\quad 13 \cdot B \equiv 2 \pmod{7} \Rightarrow 6 \cdot B \equiv 2 \pmod{7}$ $\quad B \equiv 5 \pmod{7}$
↳ $\pmod{13}$ $\quad 7 \cdot A \equiv 9 \pmod{13} \Rightarrow A \equiv 5 \pmod{13}$
↳ $2 \cdot 7 = 14 \equiv 1 \pmod{13}$

$81^{29} \equiv 7 \cdot 5 + 13 \cdot 5 \pmod{91}$
$\equiv 35 + 65 \equiv 100 \equiv 9 \pmod{91}$