$n = 247$ $\quad m = 216 = \varphi(247)$

$E = 35$ $\quad \gcd(E, m) = 1$ $\quad a^{\varphi(n)} \equiv 1 \mod n$

$D = 179$

$$\left.\begin{aligned} (x^E)^D &\equiv x \mod 247 \\ x^{ED} &\equiv x \mod 247 \\ x^{ED-1} &\equiv 1 \mod 247 \end{aligned}\right\} \text{ want } \begin{aligned} ED - 1 &= \varphi(n) \\ ED &= K\varphi(n) + 1 \\ ED &\equiv 1 \mod \varphi(n) \end{aligned}$$

m

In $U(216)$ what is the inverse of 35?

Use Euclidean algorithm.

$216 = 6 \cdot 35 + 6$

$35 = 5 \cdot 6 + 5$

$6 = 1 \cdot 5 + 1$

$1 = 6 - 1 \cdot 5 = 6 - 1(35 - 5 \cdot 6)$

$1 = -1 \cdot 35 + 6 \cdot 6 = -1 \cdot 35 + 6 \cdot (216 - 6 \cdot 35)$

$1 = 6 \cdot 216 - 37 \cdot 35$

$D = -37 \equiv 179 \mod 216$

---

where did 247 come from?

Need: I must find $\varphi(247) = 216 = m$

"You" can't find $\varphi(247)$

$\varphi(n) = ??$

$\varphi(p^K) = p^K - p^{K-1}$

$\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$

if $\gcd(a, b) = 1$

$247 = 13 \cdot 19$

$\varphi(247) = \varphi(13)\varphi(19)$

$= 12 \cdot 18$

$$a^{\varphi(n)} \equiv 1 \mod n$$

when $\gcd(a,n) = 1$

$n = p \cdot q$ $\quad$ p, q prime

Need:

$$X^{k\varphi(n)} \equiv 1 \mod n$$

what if x is a multiple of p, but not q?

$X = r \cdot p$ $\quad$ for some $r < q$

$$X^{k\cdot\varphi(n)} = X^{k\cdot\varphi(pq)} = \left(X^{\varphi(q)}\right)^{k\varphi(p)} \equiv 1 \mod q$$

$$X^{k\varphi(pq)} = 1 + tq \quad \text{for some } t$$

$$(X^E)^D \equiv X^{k\varphi(pq)} \cdot X \equiv (1+tq)X = X + tq(rp) = X + t \cdot r \cdot n \equiv X \mod n.$$