

$$p=7, q=5, \phi(pq)=24, e=19, n=35, d=19$$

$$M=5$$

To encrypt, find  $5^{19} \pmod{35}$

$$5^1 = 5$$

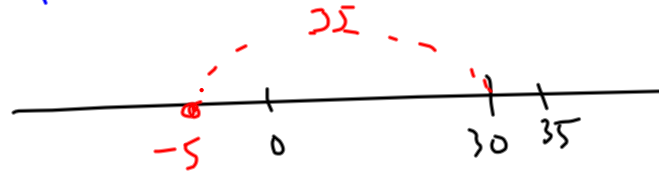
$$5^2 = 25$$

$$5^4 = 625 \rightarrow 30$$

$$5^8 = 25$$

$$5^{16} = 30$$

Write 19 as sum of powers of 2.



$$19 = 16 + 2 + 1$$

$$= 10011 \text{ (binary)}$$

$$\begin{aligned} \text{So } 5^{19} &= 5^{16} \cdot 5^2 \cdot 5^1 \\ &= 30 \cdot 25 \cdot 5 \\ &= (-5)(10) \cdot 5 \\ &= 250 \pmod{35} \\ &= \end{aligned}$$

Method for finding very large powers mod  $n$ .

Find  $M$   
 $M^2$   
 $M^4$   
 $M^8$   
 $M^{16}$   
 $M^{32}$   
 $\vdots$

mod  $n$  each time.

$$250 \% 35 = 5$$

Remainder 5

$$M^e = 5 = N$$

35

70

1

140

210

245