Problem 3

In the **RSA cryptosystem** with **N=65**, encryption (public) key **E=11**, what is the **decryption key D**?

- RSA is an **asymmetric** cyptosystem.
- When N is large, people believe it is difficult to calculate D from N and E.
- Known attacks require to find P, Q satisfying **N=P×Q**. (**Integer Factorization Problem**)

Problem 3

Factorization of N=65 is easy.

$N = 5 \times 13$

- The **decryption key D** satisfies
  - $1 < D < (P-1)(Q-1) = 48$
  - $ED \equiv 1 \pmod{48}$
- Since **E=11 and 48 are relatively prime**, it is easy to calculate its **mult inverse** by **Euclidean Algorithm**.

Problem 3

$48 = 4\times11 + 4 \Rightarrow 4 = 48 - 4\times11$

$11 = 2\times4 + 3 \Rightarrow 3 = 11 - 2\times4$

$4 = 1\times3 + 1 \Rightarrow 1 = 4 - 1\times3$

$1 = \cdots = 3\times48 - 13\times11$

Taking (mod 48),

$$1 \equiv -13\times11 \equiv 35\times11 \pmod{48}.$$

Answer D = 35