S T Q Q S S D

__/__/__

Como sabemos, temos que:

$$ed = 1 + K \cdot \phi(n) \quad \text{ou} \quad ed \equiv 1 \pmod{\phi(n)}$$

Logo, o inteiro K serve para representar os "ciclos" que a aritmética modular é capaz de realizar.

Assim, uma vez que sabemos a chave privada D, podemos calcular a seguinte expressão:

$$x \cdot d - 1$$

Que por definição, sabemos que é um múltiplo de $\phi(n)$. Assim, podemos "quebrar" $\phi(n)$.

Como provado anteriormente, podemos descobrir p e q sabendo N e $\phi(n)$.

Logo, a questão está provada