__/__/__ S T Q Q S S D

QQ • Seja o sistema:

$$\begin{cases} N = pq \\ \phi(N) = (p-1)(q-1) \end{cases}$$

O Nosso objetivo é encontrar os primos p e q apartir disso.

Porém:

$$\phi(N) = (p-1)(q-1) = pq - (p+q) + 1 \Rightarrow$$

$$\Rightarrow N - (p+q) + 1$$

de forma que $p+q = N - \phi(N) + 1$ é conhecido. Mas temos que:

$$(p+q)^2 - 4N = (p^2 + q^2 + 2pq) - 4pq = (p-q)^2$$

Assim, podemos concluir que:

$$p-q = \sqrt{(p+q)^2 - 4N}$$

também é conhecido. Entretanto, conhecendo $p+q$ e $p-q$, podemos obter "facilmente" p e q.

Para tal, é Necessário sabermos $\phi(N)$, mas pelo enunciado, só Sabemos N, E e D.