S T Q Q S S D

__/__/__

11Q → b) Digamos que o invasor se chama Pedro.

Supondo que todos os expoentes e são iguais a 3, podemos mostrar que Pedro pode recuperar pode recuperar M pelo fato de $K \geq e$ (de acordo com o enunciado)

Novamente pelo enunciado, temos que $mdc(N_i, N_j) = 1$ para todo $i \neq j$.

Assim, podemos notar que Pedro pode obter P_1, P_2, P_3, onde:

$$P_1 = M^3 \bmod N_1$$
$$P_2 = M^3 \bmod N_2$$
$$P_3 = M^3 \bmod N_3$$

Aplicando o Teorema Chinês do Resto para P_1, P_2, P_3 obtemos um $P' \in Z_{N_1 N_2 N_3}$ tal que $P' = M^3$ sobre os inteiros.

Assim, Pedro pode recuperar M calculando a raiz cúbica de P'. Para tal, vale salientar que Pedro só pode recuperar M porque, além dos fatores ditos no enunciado, é necessário que o expoente público e seja pequeno.