Extra opgave RSA cryptografie

Op blz. 321–324 van het boek wordt het RSA cryptosysteem beschreven. Neem aan dat $P = 3$, $Q = 11$ en dat de boodschap die we willen versturen het getal $M = 13$ is.

a Bereken $N = P \times Q$ en $(P - 1) \times (Q - 1)$.

b Kies een exponent G met $1 < G < (P-1) \times (Q-1)$ die geen deler gemeen heeft met $(P-1) \times (Q-1)$.

c Bepaal het getal K (de geheime sleutel) met $1 < K < (P - 1) \times (Q - 1)$, waarvoor geldt dat

$$(G \times K) \bmod ((P - 1) \times (Q - 1)) = 1.$$

d Codeer de boodschap $M = 13$. Dat wil zeggen: bereken $M^G \bmod N$.

e Decodeer de gecodeerde boodschap. Dus als H het antwoord van het vorige onderdeel is, bereken $H^K \bmod N$.