Phantom example (concluded)

You are Boba Fett . You receive the message:

$$u(x) = x^3 - 8x^2 + 11x - 16 \qquad v(x) = 13x^3 + 13x^2 + 13x + 18$$

from Ahsoka Tano . Recall your private key is:

$$s(x) = x^3 - x^2 - x - 1$$

You compute

$$p'(x) = \left\lfloor \frac{(v(x) - s(x)u(x)) \,\mathrm{MOD}\, (x^4 + 1) \,\mathrm{MOD}\, 23}{\lfloor 23/2 \rceil} \right\rceil \mathrm{MOD}\, 2 = ???$$

Do you get the message that Ahsoka sent?