A common implementation of RSA decryption: $x = c^d$ in Z_N

decrypt mod p: $x_p = c^d$ in Z_p

decrypt mod q: $x_q = c^d$ in Z_q

} combine to get $x = c^d$ in Z_N

Suppose error occurs when computing x_q, but no error in x_p

Then: output is x' where $x' = c^d$ in Z_p but $x' \neq c^d$ in Z_q

$\Rightarrow$ $(x')^e = c$ in Z_p but $(x')^e \neq c$ in Z_q $\Rightarrow$ $\gcd\left((x')^e - c, N\right) = p$