28.11.2019, Thursday, 10.30,

CMSE491 Seminar 3 “NTRU for polynomials” task

1. Let $N=3, p=5, q=41, d=1, f=x^{2}+x-1, g=x^{2}-x$. Define public key, $h$, and encrypt and decrypt back a message, $m=2x^{2}+1$. Give necessary explanations, show your calculations.
2. Your homework and participation in the seminar will be graded (50% +50%)