13.11.2020, Friday, 10.30,

CMSE491 Seminar 2 “NTRU for polynomials” task

1. Let $N=4$. Define private and public keys, and message to be encrypted. Give necessary explanations
2. Encrypt your message getting a ciphertext. Give necessary explanations
3. Decrypt the ciphertext getting back your original message. Give necessary explanations
4. Your calculations shall be done manually or in Maple
5. Your homework and participation in the seminar will be graded (50% +50%)