17.12.2019, Thursday, 10.30,

CMSE491 Seminar 4 and Lab 4 “LLL attack on NTRU for polynomials” task

1. Using Maple code as in [1] and public key defined in Seminar 3 “NTRU for polynomials”: “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”, conduct LLL attack on the secret keys as in [2], [3]. Give necessary explanations, show your calculations.
2. Report on the work shall have
	1. Maple screenshots with the attack preparing and results,
	2. Analysis of the results: whether secret keys or their rotations are obtained (as in [3]).
3. Your homework and participation in the seminar will be graded (50% +50%)

References

1. [Maple LLL code](https://staff.emu.edu.tr/alexanderchefranov/Documents/CMSE491/Fall2019/LLL%20example%203x3%2013092019.mw)
2. [LLL attack on NTRU](https://staff.emu.edu.tr/alexanderchefranov/Documents/CMSE491/Fall2019/Hoffstein2015%20Introduction%20to%20Mathematical%20Cryptography%20425-428.pdf)
3. [Example of LLL attack on NTRU](https://staff.emu.edu.tr/alexanderchefranov/Documents/CMSE491/Fall2019/Hoffstein2015%20Introduction%20to%20Mathematical%20Cryptography%20453-454.pdf)