28.12.2020, Monday, 12.30,

CMSE491 Seminar 3 “LLL” task

1. Reduce the basis $v\_{1}=\left(\begin{matrix}1&2&3\end{matrix}\right),v\_{2}=(\begin{matrix}4&5&6\end{matrix}),v\_{3}=\left(\begin{matrix}7&8&8\end{matrix}\right)$,

by LLL manually similar to how it is made in [LLL numerical example](https://staff.emu.edu.tr/alexanderchefranov/Documents/CMSE491/Fall2019/LLL%20example%20according%20to%20method%20in%20Hofstein%2016092019.docx) (click Cancel if asked for a password). Give necessary explanations.

1. Check correctness of your calculations with the help of the Maple code ([LLL example](https://staff.emu.edu.tr/alexanderchefranov/Documents/CMSE491/Fall2019/LLL%20example%203x3%2013092019.mw)). Explain LLL implementation in the code by establishing correspondence between its lines and LLL definition in [LLL](https://staff.emu.edu.tr/alexanderchefranov/Documents/CMSE491/Fall2019/Hoffstein2015%20Introduction%20to%20Mathematical%20Cryptography%20436-448.pdf), Figure 7.8.
2. Arrange your homework as a pdf file with all related materials (calculations, Maple code runs, Maple code implementing LLL annotated with your explanations). The place for uploading will be specified later.

Note: all referred above materials are available in Lecture Notes web page (weeks of 16.11.2020, LLL; 14.12.2020, the rest two)

Your homework and participation in the seminar will be graded (50% +50%)