CMSE491 Problem Session 15.01.2021

1. RSA: key generation, Euler totient function, finding multiplicative inverse, Extended Euclid algorithm, encryption/decryption, exponentiation by squaring in-line with modular reduction
2. Lattices, basis vectors, Closest lattice vector problem (CVP), linear combination, decomposition of a vector over given basis, Babai’s algorithm to solve approximate CVP, good basis, bad basis, Hadamard ratio, GGH public-key algorithm, GGH private and public keys, GGH encryption, GGH decryption, GGH digital signature
3. LLL algorithm