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

M^1000000 =>1000000 multiplications

Log2(1000)=20 multiplications; 100 times faster

1. 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

V1=(v11, v12)=(1,2), v2=(v21,v22) =(3,4)

Basis?

detV<>0

detV=1\*4-3\*2=4-6=-2<>0

w=(5,6)=t1\*v1+t2\*v2; t1, t2??

W=(W1,w2)=(5,6)=t1\*(v11, v12)+t2\*(v21, v22)=t1\*(1,2)+t2\*(3,4)=(t1\*1, t1\*2)+(t2\*3,t2\*4)=(t1+3\*t2, 2\*t1+4\*t2)

W1=5=t1+3\*t2;

W2=6=2\*t1+4\*t2

T1=5-3\*t2

6=2\*(5-3\*t2)+4\*t2=10-6\*t2+4\*t2=10-2\*t2

3=5-t2=>t2=5-3=2

T1=5-3\*t2=5-3\*2=-1

T1=-1, t2=2

T1\*v1+t2\*v2=-(1,2)+2\*(3,4)=(-1,-2)+(6,8)=(-1+6, -2+8)=(5,6)=w

E1=(1,0), E2=(0,1)

Norm(e1,2)= Norm(e2,2)=1

Norm(v1,2)=sqrt(1+4)=sqrt(5)=2.24

Norm(v2,2)=sqrt(9+16)=sqrt(25)=5

H(V)=sqrt (abs(det(V))/(||v1||\*||v2||))=sqrt(abs(-2)/(2.24\*5)=sqrt(2/11.2)=sqrt(0.179)=0.42<0.5

1. LLL algorithm