**CMSE-491 Final Exam 10.01.2020 (150 min, 30 points)**

St. **Name, Surname**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_St.Id#\_\_\_\_\_\_\_\_\_\_\_\_\_

**Instructor Alexander Chefranov**

Totally 7 questions, 14 pages

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Question | 1 | 2 | 3 | 4 | 5 | 6 | 7 | Total |
| Point | 4 | 3 | 3 | 5 | 5 | 5 | 5 | 30 |
| Grade |  |  |  |  |  |  |  |  |

**Task 1. (4 points)** Using NTRU for integers with , define secret keys, , public key, , and encrypt a message, . Show details of your calculations, give necessary explanations.

**Hints: NTRU for integers description**

****

****

EXTENDED EUCLID(m,b)

1. (A1,A2,A3):=(1,0,m); (B1,B2,B3):=(0,1,b);
2. if B3=0 return A3=gcd(m,b); no inverse
3. if B3=1 return B3 = gcd(m,b); B2= b-1 mod m
4. Q=
5. (T1,T2,T3):=(A1-QB1, A2-QB2, A3-QB3)
6. (A1,A2,A3):= (B1,B2,B3)
7. (B1,B2,B3):= (T1,T2,T3)
8. goto 2

:

A=(1,0,500), B=(0,1,11)

T=A-QB=(1,-45,5)

A=(0,1,11), B=(1,-45,5)

T=A-QB=(-2,91,1)

Hence . Check it: .

.

**Task 2. (3 points)** For , apply **one** iteration of Gaussian Lattice Reduction (GLR) algorithm. Show details of your calculations, give necessary explanations.

**Hint:** GLR algorithm:



.

**Task 3. (3 points)** For NTRU for polynomials with parameters, , define secret keys, , public key, and encrypt a message, . Show details of your calculations, give necessary explanations.

**Hints:**

****

****



EXTENDED EUCLID[m(x),b(x)]

1. [A1(x), A2(x), A3(x)]:=[1,0,m(x)]; [B1(x), B2(x), B3(x)]:=[0,1,b(x)];
2. if B3(x)=0 return A3(x)= gcd[m(x),b(x)]; no inverse
3. if B3(x)=1 return B3(x)= gcd[m(x),b(x)]; B2(x)=b(x)-1 mod m(x)
4. Q(x):= quotient of A3(x)/B3(x)
5. [T1(x), T2(x), T3(x)]:= [A1(x)-QB1(x), A2(x) –QB2(x), A3(x) –QB3(x)]
6. [A1(x), A2(x), A3(x)]:= [B1(x), B2(x), B3(x)]
7. [B1(x), B2(x), B3(x)]:= [T1(x), T2(x), T3(x)]
8. goto 2

A=(1,0,), B=(0,1,)

T=A-QB=(1,-x+1, 2x-2)

A=(0,1, x2+x-1), B=(1,1-x, 2x-2)

Q=(x2+x-1)/( 2x-2)=12x+1

T=A-QB=(-1-12x, 1-(12x+1)(1-x), 1)=(12x+1, 12x2-11x, 1)

Hence,

Check it: .

.

**Task 4. (5 points)** For the basis vectors, , apply one iteration of the loop on of LLL algorithm below:



Show your calculations. Give necessary explanations.

Hint:



[2] =>k=2

[3] =>

[4]=>k<=3? Yes

[5]=> j=1, ;

[6]

[7]=>j=0, end loop

[8]=>

[11]=>

[12]=> k=max(1,2) = 2

[14] => end of the 1st iteration

**Task 5. (5 points)** Explain how LLL attack on NTRU is conducted. Explain why the attack might be successful.

Attack on NTRU is conducted by constructing NTRU lattice from the equation defining the public key, , that is

where is some polynomial and extended by trivial equation, . The attack might be successful since, by construction, are polynomials with coefficients from , hence, representing them vectors have small norm and belong to the NTRU lattice, and LLL algorithm also returns shortest vectors from the lattice.

**Task 6. (5 points)** For , define RSA keys and encrypt M=3. Show your calculations. Give necessary explanations.

Hints:

****

****

****

A=(1,0,180), B=(0,1,7)

T=A-Q\*B=(1,-25,5)

A=(0,1,7), B=(1,-25,5)

T=A-Q\*B=(-1,26,2)

A=(1,-25,5), B=(-1,26,2)

T=A-Q\*B=(3,-77,1)

A=(-1,26,2), B=(3,-77,1)

Check it:

Encrypt:

**Task 7. (5 points)** For the Boneh attack on RSA lattice with below

****

prove that the element (3,3) of the lattice matrix is actually .

Hints:









In the row 3, we have a polynomial

Substituting in the last expression

,

we have

In the resulting expression, the coefficient near , that is the 3rd element in the 3rd row of the matrix, is , QED.