**CMSE-491 MT Exam 21.11.2019 (105 min, 20 points)**

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

**Instructor Alexander Chefranov**

Totally 3 questions, 9 pages

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Question | 1 | 2 | 3 | Total |
| Point | 7 | 5 | 8 | 20 |
| Grade |  |  |  |  |

**Task 1. (7 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

Find

1. A=(1,0,501), B=(0,1,14)

T=A-q\*B=(1-35\*0, 0-35\*1, 501-35\*14)=(1,-35,11)

1. A=(0,1,14), B=(1,-35,11)

T=A-q\*B=(0-1\*1, 1+1\*35, 14-1\*11)=(-1,36,3)

1. A=(1,-35,11), B=(-1,36,3)

T=A-q\*B=(1+3\*1, -35-3\*36, 11-3\*3)=(4,-143,2)

1. A=(-1,36,3), B=(4,-143,2)

T=A-q\*B=(-1-1\*4, 36+1\*143, 3-1\*2)=(-5,179,1)

Thus, since . Check it:

**Task 2. (5 points)** For , apply **one** iteration of Gaussian Lattice Reduction (GLR) algorithm. Show details of your calculations, give necessary explanations.

**Hint:** GLR algorithm:



, no swap

**Task 3. (8 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

Calculate

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

q=quo(A3/B3),

T=A-qB=(1,

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

q=quo(A3/B3),

T=A-qB=(

1. A=(1, , B=

q=quo(A3/B3),

T=A-qB=(6

1. A=, B=

q=quo(A3/B3),

T=A-qB=

B3=16=>

Check: