LAPORAN TUGAS KRIPTOGRAFI

DOKUMENTASI ENKRIPSI DAN DEKRIPSI
RSA, ECC, NTRU

Oleh:

M0519061 Muhammad Fadhli Putra Mulyana

M0519081 Vigo Agmel Sadewa

M0519088 Fathoni Satrio Utomo

PROGRAM STUDI INFORMATIKA

FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM

UNIVERSITAS SEBELAS MARET

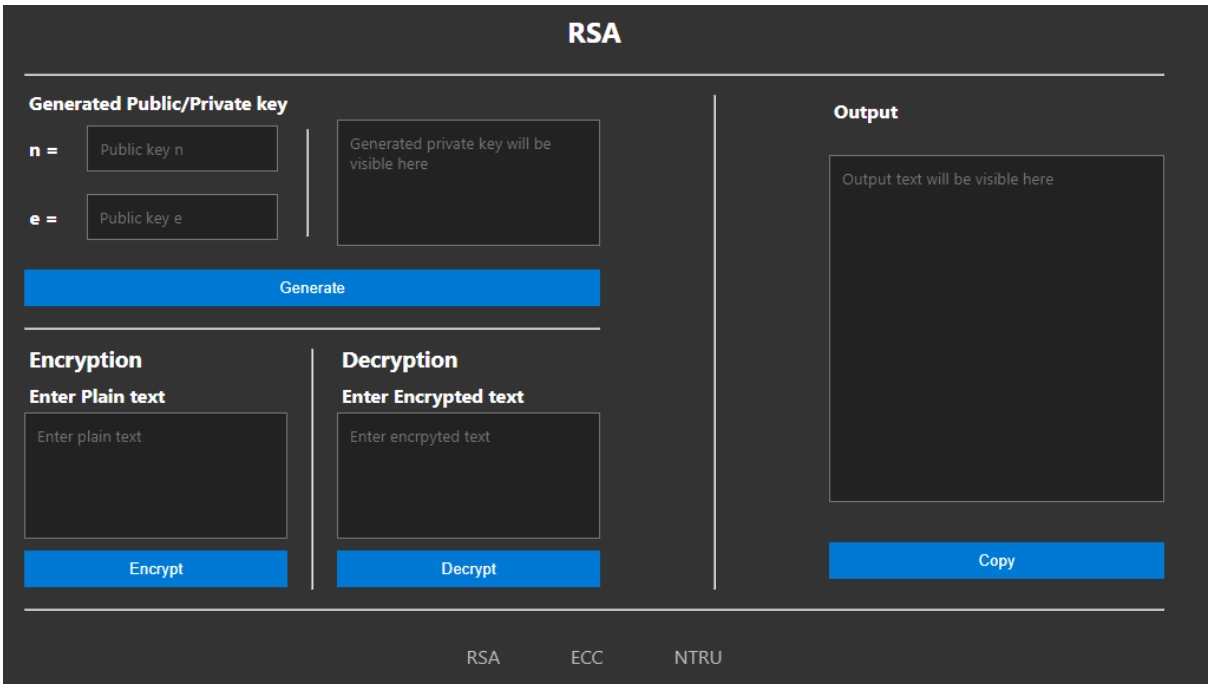
SURAKARTA

2021

Link Github : https://github.com/fadhlimulyana20/cryptohraphy

RSA

1. Screenshot Antarmuka



2. Contoh Hasil Enkripsi dan Dekripsi

Dengan public key yang dibangkitkan secara acak, didapat:

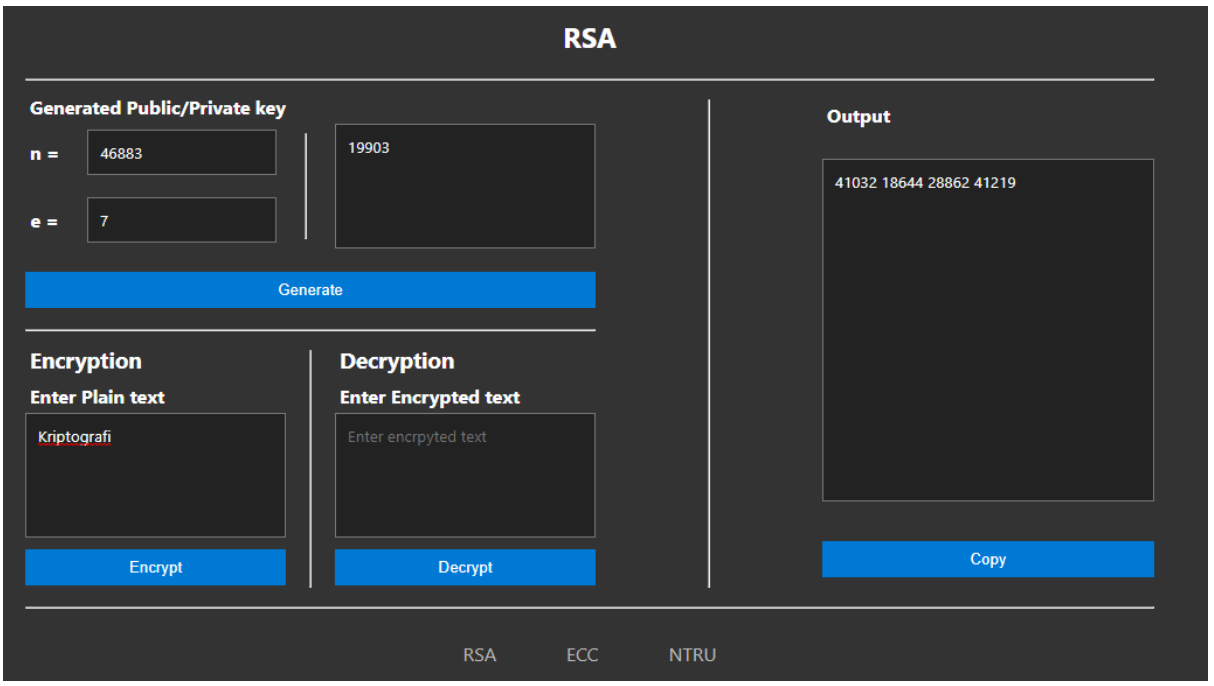
n = 46883

e = 7, dihasilkan :

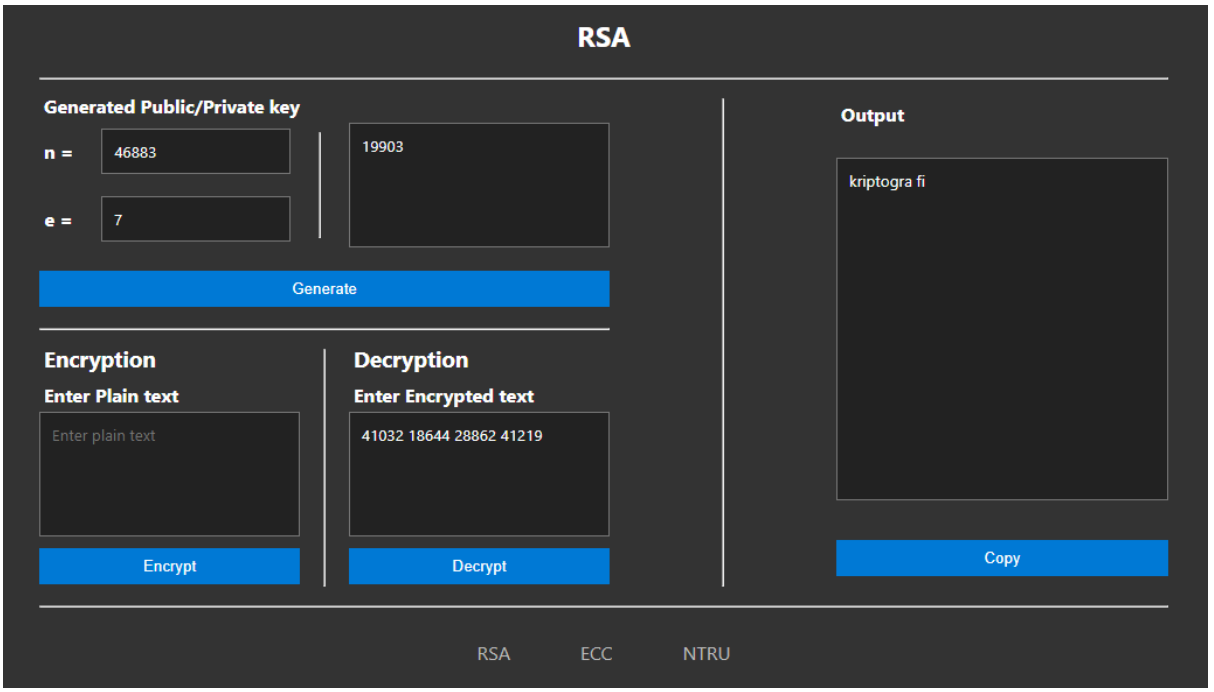
private key = 19903.

Key tersebut akan digunakan untuk enkripsi dan dekripsi menggunakan algoritma RSA.

a. Enkripsi

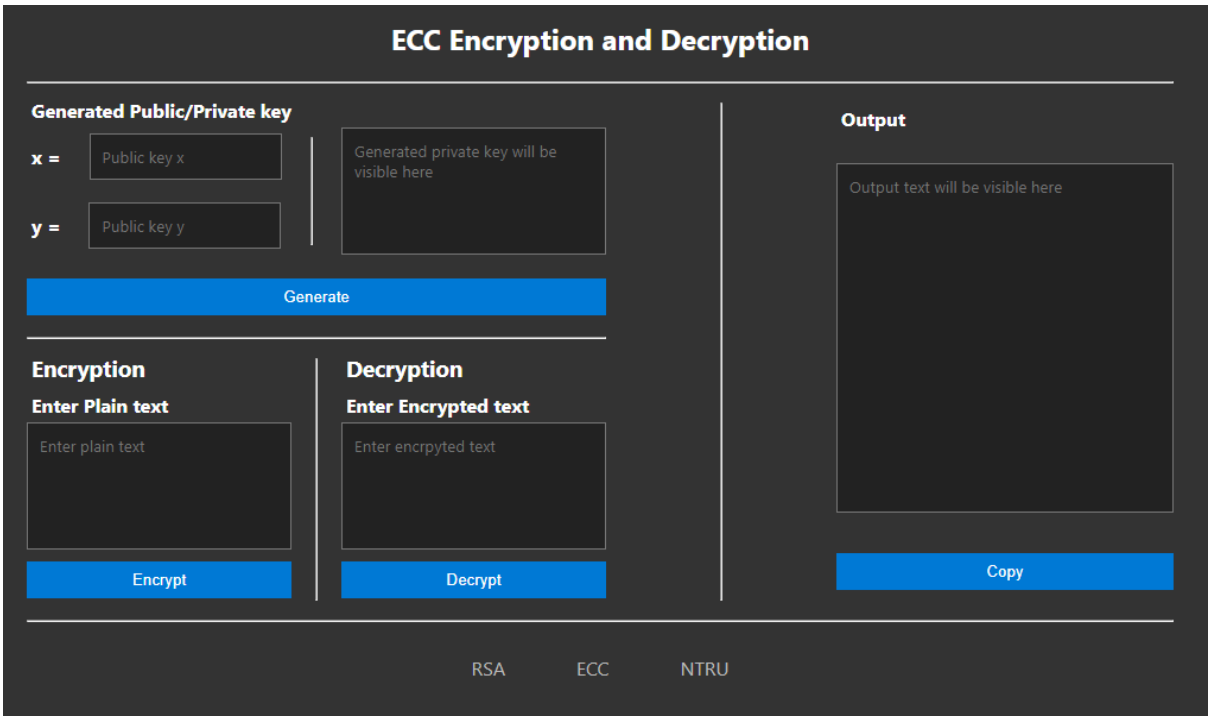

RSA
Generated Public/Private key
n =
46883
e =
7
19903
Generate
Encryption
Enter Plain text
Kriptografi
Encrypt
Decryption
Enter Encrypted text
Enter encrpyted text
Decrypt
Output
41032 18644 28862 41219
Copy
RSA
ECC
NTRU

b. Dekripsi


RSA
Generated Public/Private key
n =
46883
e =
7
19903
Generate
Encryption
Enter Plain text
Enter plain text
Encrypt
Decryption
Enter Encrypted text
41032 18644 28862 41219
Decrypt
Output
kriptogra fi
Copy
RSA
ECC
NTRU

ECC

1. Screenshot Antarmuka



2. Contoh Hasil Enkripsi dan Dekripsi

Digunakan public key yang dibangkitkan secara acak, didapat

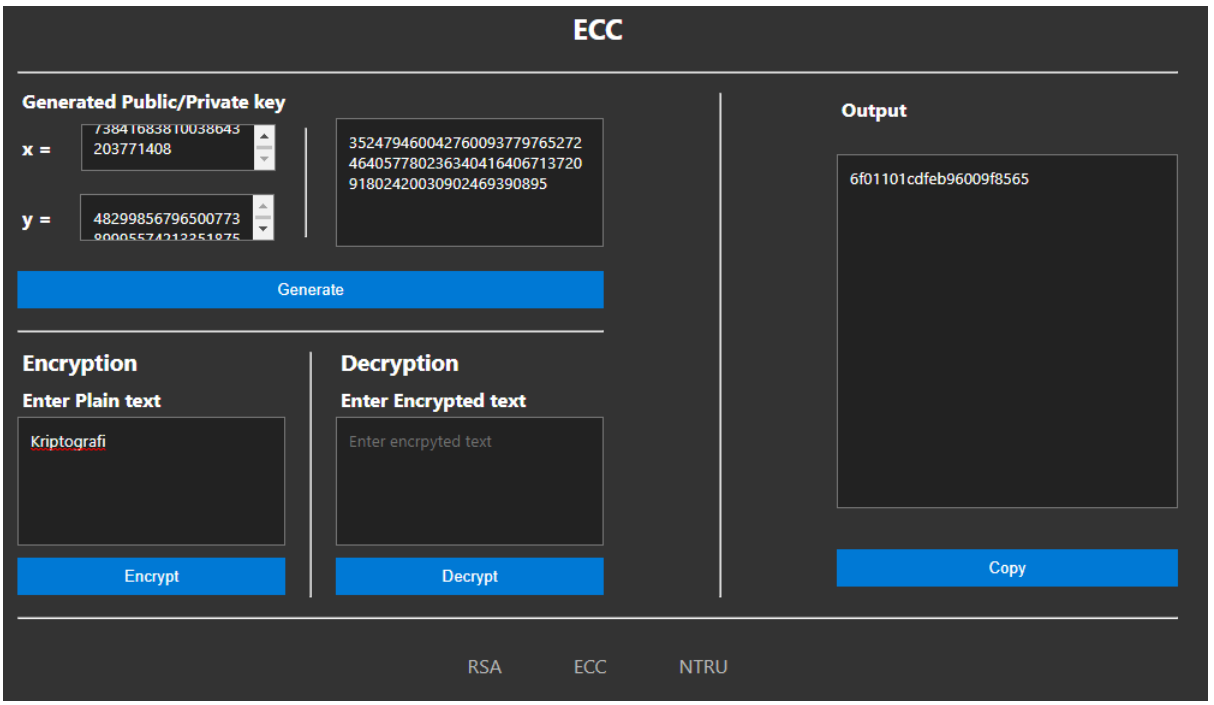
x = 46525421158038139626076142332583845319587825744737973841683810038643203771408.

y = 48299856796500773899955742133518751507216638784346117216456704628936422295698. Kemudian, didapat

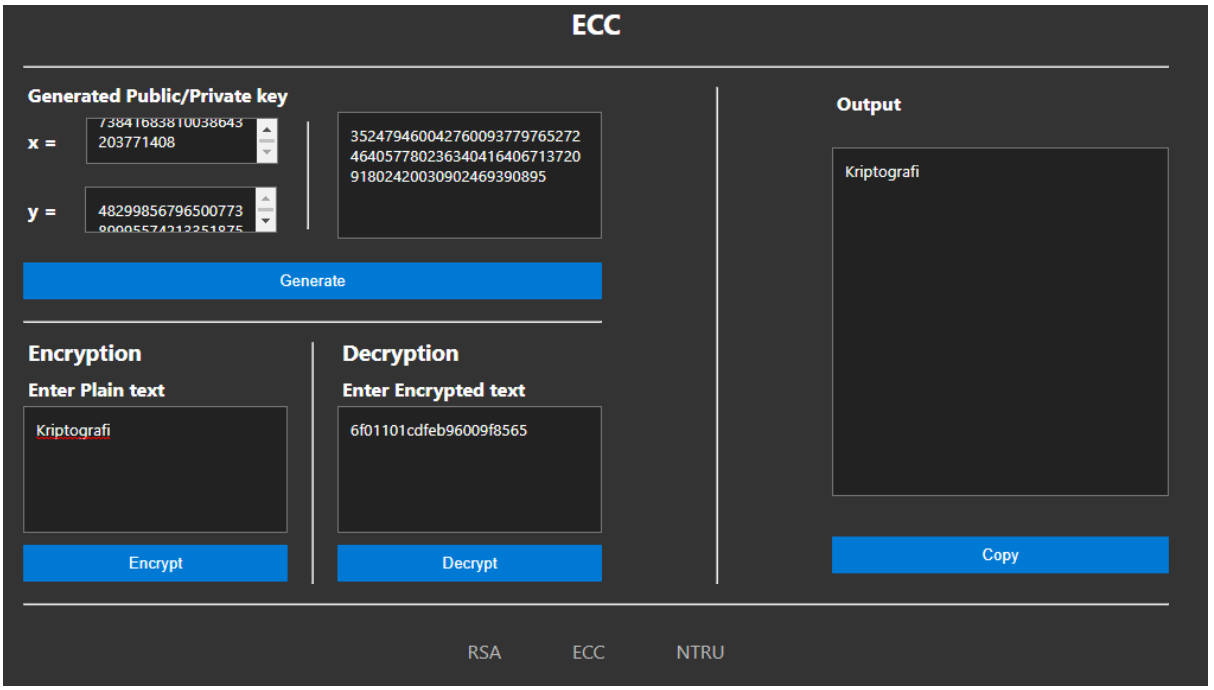
private key = 35247946004276009377976527246405778023634041640671372091802420030902469390895.

Key tersebut akan digunakan untuk enkripsi dan dekripsi menggunakan algoritma ECC

a. Enkripsi

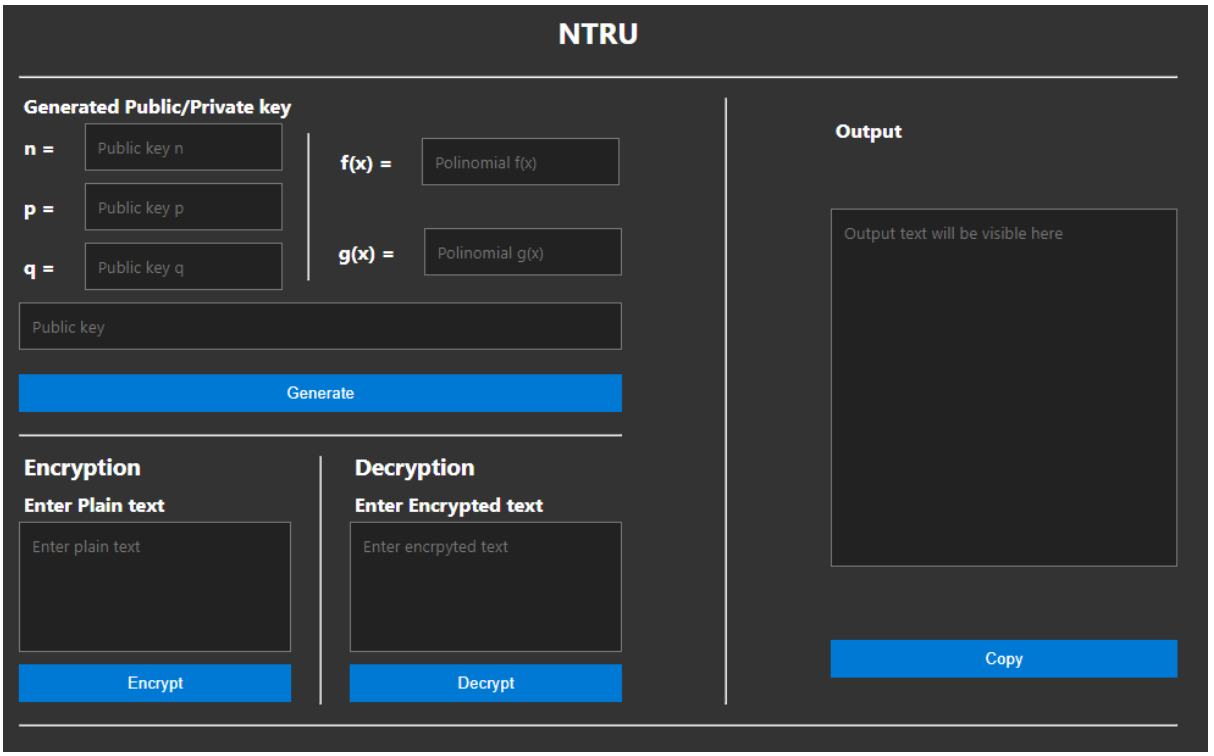

ECC
Generated Public/Private key
x =
203771408
y =
48299856796500773
352479460042760093779765272
464057780236340416406713720
918024200309024693908 95
Generate
Encryption
Enter Plain text
Kriptografi
Encrypt
Decryption
Enter Encrypted text
Enter encrpyted text
Decrypt
Output
6f01101cdfeb96009f8565
Copy
RSA
ECC
NTRU

b. Dekripsi


ECC
Generated Public/Private key
x =
203771408
y =
48299856796500773
352479460042760093779765272
464057780236340416406713720
918024200309024693908 95
Generate
Encryption
Enter Plain text
Kriptografi
Encrypt
Decryption
Enter Encrypted text
6f01101cdfeb96009f8565
Decrypt
Output
Kriptografi
Copy
RSA
ECC
NTRU

NTRU

1. Screenshot Antarmuka



2. Contoh Hasil Enkripsi dan Dekripsi

Digunakan nilai

n = 7,

p = 29, dan

q = 491531,

dimana n adalah bilangan prima, p GCD q = 1. Kemudian digunakan 2 polinomial acak f(x) dan g(x) yang berupa array polinomial dengan anggota [-1 0 1], jumlahnya paling banyak adalah sebanyak n. Digunakan polinomial

f(x) = [1,1,-1,0,-1,1] dan

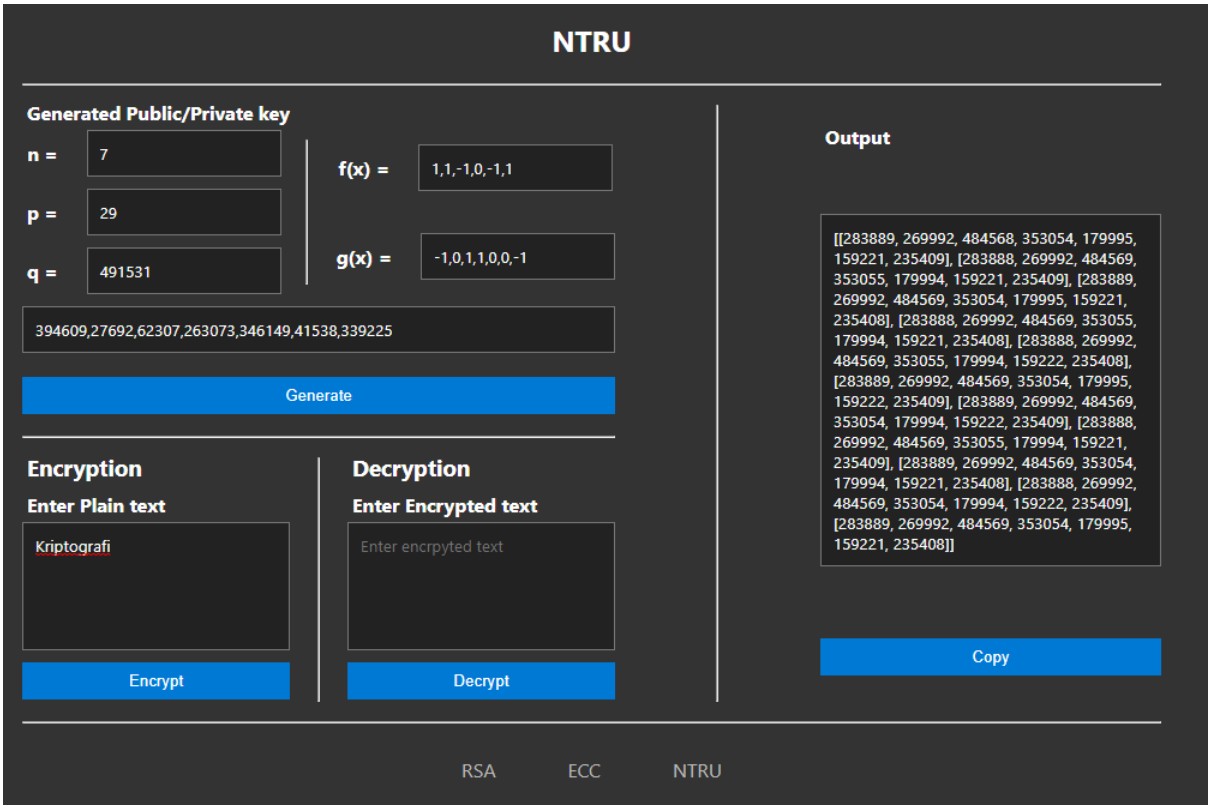
g(x) = [-1,0,1,1,0,0,-1].

Dari semua bilangan tersebut, dihasilkan

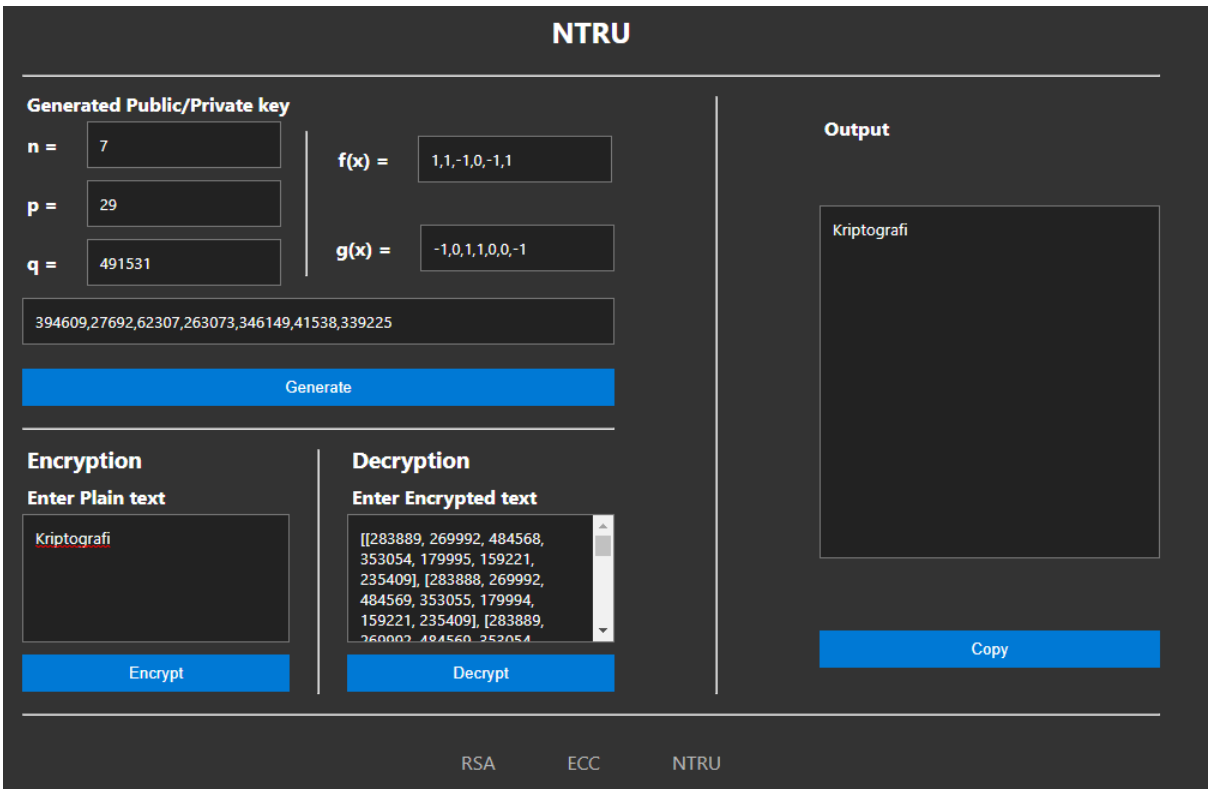
public key = [394609,27692,62307,263073,346149,41538,339225].

Key tersebut akan digunakan untuk enkripsi dan dekripsi menggunakan algoritma NTRU.

a. Enkripsi


NTRU
Generated Public/Private key
n =
7
p =
29
q =
491531
f(x) =
1,1,-1,0,-1,1
g(x) =
-1,0,1,1,0,0,-1
394609,27692,62307,263073,346149,41538,339225
Generate
Encryption
Enter Plain text
Kriptografi
Encrypt
Decryption
Enter Encrypted text
Enter encrpyted text
Decrypt
Output
[[283889, 269992, 484568, 353054, 179995, 159221, 235409], [283888, 269992, 484569, 353055, 179994, 159221, 235409], [283889, 269992, 484569, 353054, 179995, 159221, 235408], [283888, 269992, 484569, 353055, 179994, 159221, 235408], [283888, 269992, 484569, 353055, 179994, 159222, 235408], [283889, 269992, 484569, 353054, 179995, 159222, 235409], [283889, 269992, 484569, 353054, 179994, 159222, 235409], [283888, 269992, 484569, 353055, 179994, 159221, 235409], [283889, 269992, 484569, 353054, 179994, 159221, 235408], [283888, 269992, 484569, 353054, 179994, 159222, 235409], [283889, 269992, 484569, 353054, 179995, 159221, 235408]]
Copy
RSA
ECC
NTRU

b. Dekripsi


NTRU
Generated Public/Private key
n =
7
p =
29
q =
491531
f(x) =
1,1,-1,0,-1,1
g(x) =
-1,0,1,1,0,0,-1
394609,27692,62307,263073,346149,41538,339225
Generate
Encryption
Enter Plain text
Kriptografi
Encrypt
Decryption
Enter Encrypted text
[[283889, 269992, 484568, 353054, 179995, 159221, 235409], [283888, 269992, 484569, 353055, 179994, 159221, 235409], [283889,
Decrypt
Output
Kriptografi
Copy
RSA
ECC
NTRU