

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

The screenshot shows a web application titled "RSA" with a dark theme. It is divided into three main sections: "Generated Public/Private key", "Encryption", and "Decryption".

- Generated Public/Private key:** Contains input fields for "n =" (Public key n) and "e =" (Public key e). A "Generate" button is below these fields. To the right, a box indicates "Generated private key will be visible here".
- Encryption:** Contains an "Enter Plain text" input field and an "Encrypt" button.
- Decryption:** Contains an "Enter Encrypted text" input field and a "Decrypt" button.
- Output:** A large box on the right labeled "Output" with the text "Output text will be visible here" and a "Copy" button at the bottom.

At the bottom of the interface, there are three tabs: "RSA", "ECC", and "NTRU", with "RSA" currently selected.

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 encrypyted 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

The screenshot shows a web application titled "ECC Encryption and Decryption". It features a dark theme with blue buttons. The interface is divided into several sections:

- Generated Public/Private key:** This section contains input fields for "x =" (Public key x) and "y =" (Public key y). To the right is a box labeled "Generated private key will be visible here". A blue "Generate" button is positioned below these inputs.
- Encryption:** This section has a label "Enter Plain text" above a text input field. A blue "Encrypt" button is located below the input field.
- Decryption:** This section has a label "Enter Encrypted text" above a text input field. A blue "Decrypt" button is located below the input field.
- Output:** A large text area on the right side is labeled "Output text will be visible here". A blue "Copy" button is located below this area.

At the bottom of the application, there are three radio buttons labeled "RSA", "ECC", and "NTRU", with "ECC" currently selected.

2. Contoh Hasil Enkripsi dan Dekripsi

Digunakan public key yang dibangkitkan secara acak, didapat

x =

465254211580381396260761423325838453195878257447379738416838100386432
03771408.

y =

482998567965007738999557421335187515072166387843461172164567046289364
22295698. Kemudian, didapat

private key =

352479460042760093779765272464057780236340416406713720918024200309024
69390895.

Key tersebut akan digunakan untuk enkripsi dan dekripsi menggunakan algoritma ECC

a. Enkripsi

ECC

Generated Public/Private key

x =

73841683810038643

203771408

y =

48299856796500773

80005574112251875

352479460042760093779765272

464057780236340416406713720

91802420030902469390895

Generate

Encryption

Enter Plain text

Kriptografi

Encrypt

Decryption

Enter Encrypted text

Enter encrypted text

Decrypt

Output

6f01101cdf96009f8565

Copy

RSA

ECC

NTRU

b. Dekripsi

ECC

Generated Public/Private key

x =

73841683810038643

203771408

y =

48299856796500773

80005574112251875

352479460042760093779765272

464057780236340416406713720

91802420030902469390895

Generate

Encryption

Enter Plain text

Kriptografi

Encrypt

Decryption

Enter Encrypted text

6f01101cdf96009f8565

Decrypt

Output

Kriptografi

Copy

RSA

ECC

NTRU

NTRU

1. Screenshot Antarmuka

The screenshot displays the NTRU web application interface. It features a dark theme with white text and blue buttons. The interface is divided into several sections:

- Generated Public/Private key:** This section contains input fields for n (Public key n), p (Public key p), and q (Public key q). It also includes input fields for $f(x)$ (Polynomial $f(x)$) and $g(x)$ (Polynomial $g(x)$). A large input field for the Public key is located below these. A blue "Generate" button is positioned at the bottom of this section.
- Encryption:** This section has an input field for "Enter Plain text" and a blue "Encrypt" button.
- Decryption:** This section has an input field for "Enter Encrypted text" and a blue "Decrypt" button.
- Output:** A large text area on the right side where the output text will be visible. A blue "Copy" button is located at the bottom of this section.

2. Contoh Hasil Enkripsi dan Dekripsi

Digunakan nilai

$n = 7$,

$p = 29$, dan

$q = 491531$,

dimana n adalah bilangan prima, $p \text{ GCD } q = 1$. 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 encrypted 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, 159222, 235408], [283889, 269992, 484569, 353054, 179995, 159222, 235409], [283889, 269992, 484569, 353055, 179994, 159221, 235408], [283888, 269992, 484569, 353055, 179994, 159222, 235409], [283889, 269992, 484569, 353054, 179995, 159221, 235409], [283889, 269992, 484569, 353054, 179995, 159222, 235409], [283888, 269992, 484569, 353055, 179994, 159221, 235408], [283888, 269992, 484569, 353055, 179994, 159222, 235409], [283889, 269992, 484569, 353054, 179995, 159221, 235408], [283889, 269992, 484569, 353054, 179995, 159222, 235409], [283888, 269992, 484569, 353055, 179994, 159221, 235408], [283888, 269992, 484569, 353055, 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, 269992, 484569, 353054, 179995, 159222, 235408], [283888, 269992, 484569, 353055, 179994, 159222, 235409], [283889, 269992, 484569, 353054, 179995, 159221, 235408]]

Decrypt

Output

Kriptografi

Copy

RSA

ECC

NTRU