

Tugas Kriptografi Invers Matrix Modular

Nama : Kevin Darmawan

NPM : 1806148744

Dalam prinsip kriptografi, menggunakan inverse dan residue matrix dimana seluruh elemen pada residue matrix ada dalam Z_n . Residue matrix akan memiliki multiplicative inverse apabila determinan matrix memiliki multiplicative inverse dalam Z_n . Kesimpulannya, residue matrix akan memiliki invers bila syarat gcd dari $\det(A)$, $n = 1$ terpenuhi.

Lalu invers didapatkan dengan membulatkan $t \times \det(A) \times \text{inv}(A)$ dengan modulus n .

```
function [ A1 ] = inversMatrix( A, n )
%inversMatrix merupakan fungsi untuk menghitung matrix Zn
dalam modulo n

r = round(mod(det(A),n));
if (gcd(n,r)==1)
    [d, s, t] = gcd(n,r);
    A1 = mod(round(t*det(A)*inv(A)),n);
else
    print('Matrix tidak memiliki determinan')
end
```