**Cryptography and Coding Homework**

**Vedasagar Karthykeyan (vkarthy1)**

**Question 1:**

function [ gcd, X, Y ] = extendedEuclideanAlgo( a, b )

%UNTITLED Summary of this function goes here

%   Detailed explanation goes here

x=[]; y=[]; q=[]; arr=[];

x(1)=1; x(2)=0;

y(1)=0; y(2)=1;

arr(1)=a; arr(2)=b;

q(2)=floor(arr(1)/arr(2));

j=2;

while arr(j)~=0

    x(j+1) = x(j-1) + q(j)\*x(j);

    y(j+1) = y(j-1) + q(j)\*y(j);

    arr(j+1) = (power(-1, j) \* x(j+1) \* a) + (power(-1, j+1) \* y(j+1) \* b);

    q(j+1) = floor(arr(j)/arr(j+1));

    j=j+1;

end

gcd = arr(j-1);

X = power(-1, j) \* x(j-1);

Y = power(-1, j+1) \* y(j-1);

[gcd, X, Y] = extendedEuclideanAlgo(2501, 1002)

gcd =

1

X =

125

Y =

-312

[gcd, X, Y] = extendedEuclideanAlgo(19, 7)

gcd =

1

X =

3

Y =

-8

[gcd, X, Y] = extendedEuclideanAlgo(114, 76)

gcd =

38

X =

1

Y =

-1

**Question 2:**

function [ x ] = inversemodn( a, n )

%UNTITLED2 Summary of this function goes here

%   Detailed explanation goes here

[gcd, X, Y] = extendedEuclideanAlgo(a, n);

if gcd ~=1

   disp('No inverse');

else

   x = mod(X, n);

end

x = inversemodn(3, 26)

x =

9

x = inversemodn(5, 26)

x =

21

x = inversemodn(7, 26)

x =

15

**HW\_6\_a)**

for x=1:61

p(x) = 8\*power(x,2) - 488\*(x) + 7243

end

isprime(abs(p))

ans =

Columns 1 through 25

1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1

Columns 26 through 50

1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1

Columns 51 through 61

1 1 1 1 1 1 1 1 1 1 1

**HW\_6\_b)**

for y=1:19

q(y) = power(y,4)+ 29\*power(y,2) + 101;

end

isprime(q)

ans =

1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1

diary off