RSA algorithm in text and image encryption/decryption

To encrypt a message, P, compute $C = P^e \pmod{n}$. To decrypt C, compute $P = C^d \pmod{n}$.

Let P is the numerical value of message.
Encoded message, $C = P^e \pmod{n}$
Decoded message, $P = C^d \pmod{n}$

Let us consider another example:

$p = 3, q = 11$

$n = pq = 33, z = (p\text{-}1)(q\text{-}1) = 20$

$d = 7$, since 20 and 7 does not have common factor

Now $7e = 1 \bmod 20$ which provides $e = 3$

$C = P^3 \pmod{33}$ which provides encoded value C

Plaintext (P)			Ciphertext (C)		After decryption	
Symbolic	Numeric	P^3	$P^3 \pmod{33}$	C^7	$C^7 \pmod{33}$	Symbolic
S	19	6859	28	13492928512	19	S
U	21	9261	21	1801088541	21	U
Z	26	17576	20	1280000000	26	Z
A	01	1	1	1	01	A
N	14	2744	5	78125	14	N
N	14	2744	5	78125	14	N
E	05	125	26	8031810176	05	E
		Sender's computation		Receiver's computation		

Fig. An example of the RSA algorithm.

```
e = 3; n = 33; d = 7; %RSA parameters
y='JAHANGIRNAGAR'; %input string
z = double(y); %ASCII values
S=z-60; %to reduce size of the integer
for i=1:length(z)
Encrypt(i)=mod(S(i)^e, n);
end
char(Encrypt)  % encrypted string
Encrypt=double(Encrypt);
for j=1:length(z)
Decrypt(j)=mod(Encrypt(j)^d, n);
end
Recover=char(Decrypt+60) %increase the decoded value by 60
```

The value of *S* must be less than *n*

RSA In Image Encryption and Decryption

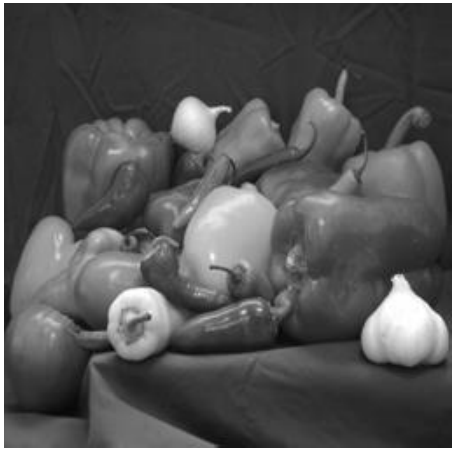
```
clear all
close all
e = 3; n = 33; d = 7; N=256;
I=imread('peppers.png');
I=rgb2gray(I);
I=imresize(I,[N, N]);
subplot(2,2,1)
imshow(I)
title('Original Image')
```

```
I=double(I);
R=mod(I,16);
%Remainder of the image
for i=1:N
for j=1:N
Q(i,j)=uint8((I(i,j)/16)-0.5);
% Quiescent of the image
end
end
```

```
Q=double(Q);
for i =1:N
for j = 1:N
Qe(i, j)=mod(Q(i,j)^e, n);
Re(i, j)=mod(R(i,j)^e, n);
%Decryption of image
Qd(i, j)=mod((Qe(i,j))^d, n);
Rd(i, j)=mod((Re(i,j))^d, n);
end
end
```

```
Rec=Qd*16+Rd;
subplot(2,2,2)
imshow(uint8(Qe))
title('Encrypted Quiescent Image')
subplot(2,2,3)
imshow(uint8(Re))
title('Encrypted Remainder Image')
subplot(2,2,4)
imshow(uint8(Rec))
title('Decrypted Image')
```

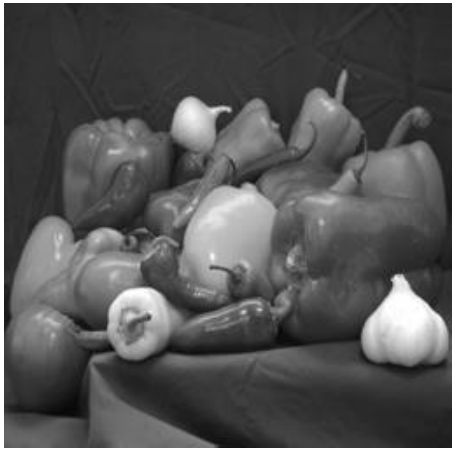
Original Image



Encrypted Quiescent Image

Encrypted Remainder Image

Decrypted Image



Try for RGB image

```
I=imread('peppers.png');
I1=I(:,:,1); %red plate
I2=I(:,:,2); %green plate
I3=I(:,:,3); %blue plate
subplot(2,2,1)
imshow(I1)
title('Red plate')
subplot(2,2,2)
imshow(I2)
title('Green plate')
subplot(2,2,3)
imshow(I3)
title('Blue plate')
Y=cat(3,I1,I2,I3);
subplot(2,2,4)
imshow(Y)
title('RGB image')
```