SCREEN SHOTS

RSA_GEN and RSA_ENC

Editor - M:\ELEC5471M_FT16_MATLAB_Project_Oyetoke_Raghuraman\Factor_Pairs.m

Factor_Pairs.m | RSA_Dec.m | RSA_Enc.m | RSA_Gen.m | RSA_Hack.m

```
% Make sure exactly 1 argument is passed
if nargin ~= 1
  error('Factor_Pairs:Invalid_No_Of_Arguments_Passed','This function works with 1 argument N.');
end

% Make sure N is a positive integer greater than 0
```

Command Window

New to MATLAB? See resources for Getting Started.

```
>> RSA_Gen(97,67)

RSA PUBLIC AND PRIVATE KEY GENERATOR STARTED

Input validation in progress...
Input validation completed
Starting operation to generate keys...
Answer:
Public Key = (6499 , 325)
Private Key = (6499, 2125)
N = 6499
d = 2125
e = 325

ans =

        6499

>> RSA_Enc(6499,325,4000)

RSA ENCRYPTION STARTED

Input validation in progress...
Input validation completed
Starting operation to generate ciphertext...

The Cipher Text for Messgae 4000 is 3118

ans =

        3118

fx >>
```

RSA_DEC

Editor - M:\ELEC5471M_FT16_MATLAB_Project_Oyetoke_Raghuraman\Factor_Pairs.m

Factor_Pairs.m | RSA_Dec.m | RSA_Enc.m | RSA_Gen.m | RSA_Hack.m

```
% Make sure exactly 1 argument is passed
if nargin ~= 1
  error('Factor_Pairs:Invalid_No_Of_Arguments_Passed','This function works with 1 argument N.');
end

% Make sure N is a positive integer greater than 0
```

Command Window

New to MATLAB? See resources for Getting Started.

```
N = 6499
d = 2125
e = 325

ans =

        6499

>> RSA_Enc(6499,325,4000)

RSA ENCRYPTION STARTED

Input validation in progress...
Input validation completed
Starting operation to generate ciphertext...

The Cipher Text for Messgae 4000 is 3118

ans =

        3118

>> RSA_Dec(6499, 2125, 3118)

 RSA CIPHER TEXT DECIPHERER STARTED

Input validation in progress...
Input validation completed
Starting operation to generate plain text...
The Plain Text for Ciphertext 3118 is 4000

ans =

        4000

fx >>
```

RSA HACK

Editor - M:\ELEC5471M_FT16_MATLAB_Project_Oyetoke_Raghuraman\Factor_Pairs.m

Factor_Pairs.m | RSA_Dec.m | RSA_Enc.m | RSA_Gen.m | RSA_Hack.m

```
% Make sure exactly 1 argument is passed
if nargin ~= 1
  error('Factor_Pairs:Invalid_No_Of_Arguments_Passed','This function works with 1 argument N.');
end

% Make sure N is a positive integer greater than 0
```

Command Window

New to MATLAB? See resources for Getting Started.

```
>> RSA_Hack(6499,325,3118)

RSA HACK STARTED

Input validation in progress...
Input validation completed
Moving on to get all possible factors of N...

FACTOR PAIR GENERATOR STARTED

Factor pairs p, q of 6499 are listed below
           1        6499
          67          97

All possible factor pairs of N have been gotten. Each pair will be analysed to get possible ms
Factor pair analysis in progress....

Factors p, q = : 67, 97
derived z: 6336
derived d: 2125

 RSA CIPHER TEXT DECIPHERER STARTED

Input validation in progress...
Input validation completed
Starting operation to generate plain text...
The Plain Text for Ciphertext 3118 is 4000
derived d: 8461

 RSA CIPHER TEXT DECIPHERER STARTED

Input validation in progress...
Input validation completed
Starting operation to generate plain text...
```

```
 RSA CIPHER TEXT DECIPHERER STARTED

Input validation in progress...
Input validation completed
Starting operation to generate plain text...
The Plain Text for Ciphertext 3118 is 4000
derived d: 14797

 RSA CIPHER TEXT DECIPHERER STARTED

Input validation in progress...
Input validation completed
Starting operation to generate plain text...
The Plain Text for Ciphertext 3118 is 4000
derived d: 21133

 RSA CIPHER TEXT DECIPHERER STARTED

Input validation in progress...
Input validation completed
Starting operation to generate plain text...
The Plain Text for Ciphertext 3118 is 4000
derived d: 27469

 RSA CIPHER TEXT DECIPHERER STARTED

Input validation in progress...
Input validation completed
Starting operation to generate plain text...
The Plain Text for Ciphertext 3118 is 4000
derived d: 33805

 RSA CIPHER TEXT DECIPHERER STARTED

Input validation in progress
```

Command Window

New to MATLAB? See resources for Getting Started.

```
 RSA CIPHER TEXT DECIPHERER STARTED

Input validation in progress...
Input validation completed
Starting operation to generate plain text...
The Plain Text for Ciphertext 3118 is 4000
derived d: 40141

 RSA CIPHER TEXT DECIPHERER STARTED

Input validation in progress...
Input validation completed
Starting operation to generate plain text...
The Plain Text for Ciphertext 3118 is 4000
derived d: 46477

 RSA CIPHER TEXT DECIPHERER STARTED

Input validation in progress...
Input validation completed
Starting operation to generate plain text...
The Plain Text for Ciphertext 3118 is 4000
derived d: 52813

 RSA CIPHER TEXT DECIPHERER STARTED

Input validation in progress...
Input validation completed
Starting operation to generate plain text...
The Plain Text for Ciphertext 3118 is 4000
derived d: 59149

 RSA CIPHER TEXT DECIPHERER STARTED

Input validation in progress...
Input validation completed
```

```
 9 -   if nargin ~= 1
10 -     error('Factor_Pairs:Invalid_No_Of_Arguments_Passed','This function works with 1 argument N.');
11 -   end
```

Command Window

New to MATLAB? See resources for Getting Started.

```
Input validation in progress...
Input validation completed
Starting operation to generate plain text...
The Plain Text for Ciphertext 3118 is 4000
derived d: 84493

 RSA CIPHER TEXT DECIPHERER STARTED

Input validation in progress...
Input validation completed
Starting operation to generate plain text...
The Plain Text for Ciphertext 3118 is 4000
derived d: 90829

 RSA CIPHER TEXT DECIPHERER STARTED

Input validation in progress...
Input validation completed
Starting operation to generate plain text...
The Plain Text for Ciphertext 3118 is 4000
derived d: 97165

 RSA CIPHER TEXT DECIPHERER STARTED

Input validation in progress...
Input validation completed
Starting operation to generate plain text...
The Plain Text for Ciphertext 3118 is 4000

By analyzing all the copairs and limiting the generated d to between 1 and 100000, ALL
the possible message(s) from the public key 6499,325 and cipher text 3118 are/is: 4000 4000 4000 4000 4000 4000 4000 4000 4000 4000

Finally, the UNIQUE possible message(s) from the public key 6499,325 for cipher text 3118 are/is:     4000
ans =

        4000
```