Laboratory Session 5

1. Introduction

In this lab you will use MATLAB to break a weakened form of the RSA public key encryption algorithm using a very short key and determine the plaintext from a ciphertext message.

MATLAB can be found by:

Start >MATLAB

A summary of how the RSA algorithm works is described in Section 3. You will need to understand this section in order to determine the private key from the given public key.

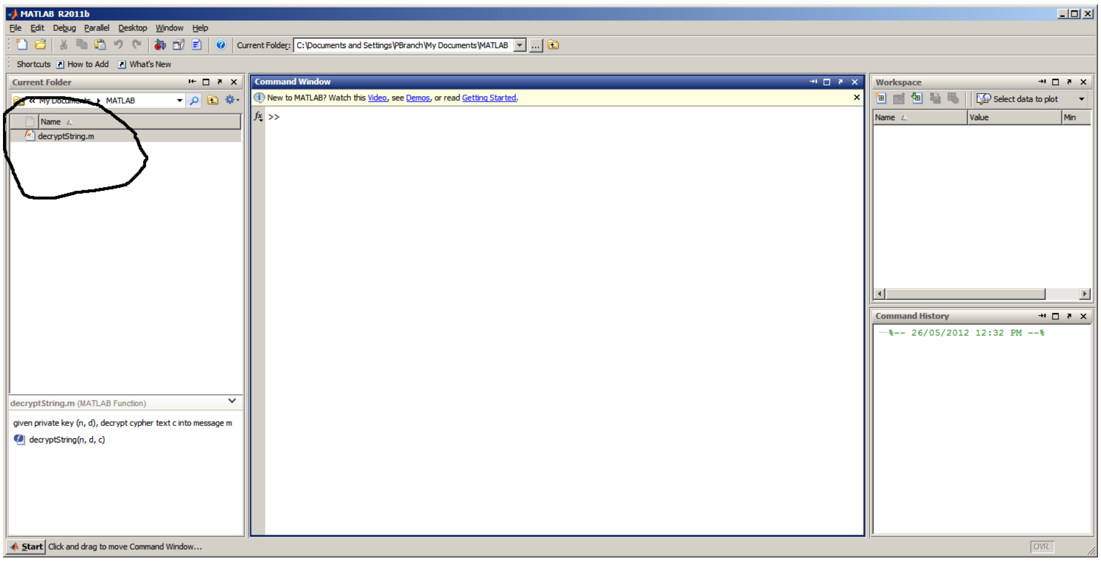
Should you need it, an introduction / revision of MATLAB is in Section 4. All the commands you need to do the lab are included in this section. If you are unfamiliar with MATLAB do this section first.

2. Method

You are to decrypt the following message c which you know was encrypted with the given public key of [n,e] = [2407,57].

```
c = [2050   2296   640    479    640    2377   1274   479    640    2377
     2395   194    476    2377   2395   602    2014   640    1205   2377
     476    1888   2377   640    1142   1421   479    602    2014   2395
     586    476    1142   749    2377   476    1142   640    2377   2395
     2296   1274   2395   2377   194    586    1285   1285   2377   2014
     479    640    1904   640    1142   2395   2377   602    476    540
     479    2377   1205   586    1205   2395   640    479    2377   1888
     479    476    2011   2377   479    640    1274   1741   586    1142
     1019   2377   602    476    540    479    2377   1741   586    1274
     479    602    2377]
```

1. Install the routine `decryptString.m` in the work directory. This can be done by dragging the file from the desktop directly into the left-hand panel as shown below:



New to MATLAB? Watch this Video, see Demos, or read Getting Started.

```
>>
```

given private key (n, d), decrypt cypher text c into message m

decryptString(n, d, c)

```
%-- 26/05/2012 12:32 PM --%
```

Click and drag to move Command Window...

This routine decrypts a string of cipher text using the appropriate key. You have to determine the private key from the public key.

2. Determine the private key [n, d] associated with the public key [n, e] = [2407, 57]. You may assume that d is less than n and is unique. You will need to construct a **for** loop to test different values of d.

3. Use the private key to decrypt the message. This can be done using the `decryptString.m` routine. Its use is

   ```
   decryptString(n, d, c)
   ```

   where n and d is the private key and c is a vector containing the cipher text.

4. To obtain the full message, repeat with the public key [n, e] = [7663, 89] and for the cipher text c below.

```
c = [2980  3647  1145  7023  4485  3647  7130  7023  6069  5363
     2980  6069  7023  3911  2971  5943  5943  7023  1889  5561
     7130  454   7130  3647  6069  7023  3243  4485  2957  5561
     7023  5465  4485  454   7130  5561  3647  1883  7130  3647
     6069  656   7023  6689  2206  5561  2957  4580  7130  7023
     6238  4580  5363  3647  7130  2971  5561  1603]
```

3. RSA Algorithm

To create the public key select two large positive prime numbers p and q

Compute $n = p*q$

Compute $x = (p-1)*(q-1)$

Choose an integer e which is relatively prime to x.

Public key is then $[e, n]$

To create the private key

compute d such that $(d*e) \bmod x = 1$

Private key is then $[d, n]$

Data to encrypt is m

To encrypt m, compute $c = (m^e) \bmod n$

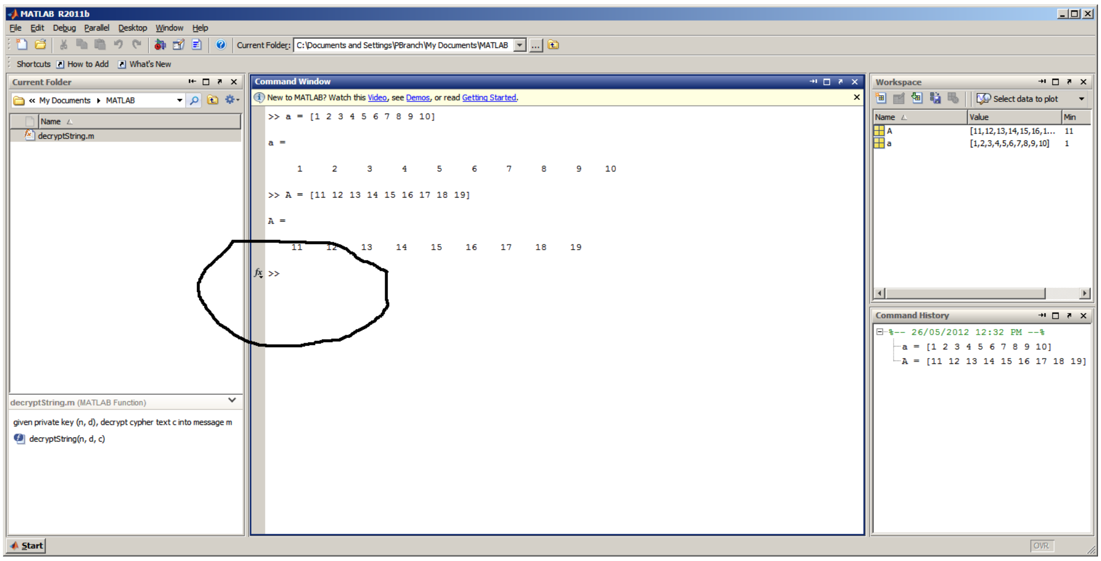
To decrypt c, compute $m = (c^d) \bmod n$

4. MATLAB Revision / Introduction

MATLAB is designed primarily to operate on matrices and vectors. We only need to deal with operations on vectors. The command window is used to run the MATLAB instructions. The Command History window keeps a record of all the instructions.

Note that all the Matlab instructions should be typed in the command window.

Laboratory Session 5



decryptString.m

decryptString.m (MATLAB Function)

given private key (n, d), decrypt cypher text c into message m

decryptString(n, d, c)

New to MATLAB? Watch this Video, see Demos, or read Getting Started.

```
>> a = [1 2 3 4 5 6 7 8 9 10]

a =

     1     2     3     4     5     6     7     8     9    10

>> A = [11 12 13 14 15 16 17 18 19]

A =

    11    12    13    14    15    16    17    18    19

fx >>
```

Name	Value	Min
A	[11,12,13,14,15,16,1...	11
a	[1,2,3,4,5,6,7,8,9,10]	1

```
%-- 26/05/2012 12:32 PM --%
  a = [1 2 3 4 5 6 7 8 9 10]
  A = [11 12 13 14 15 16 17 18 19]
```

Vector definition

The simplest way to define a matrix is to list its elements in order

Try `a = [ 1 2 3 4 5 6 7 8 9]`

Note : You can suppress the listing of the array by adding a semi-colon at the end. Also note that MATLAB is case sensitive.

Try `A = [ 11 12 13 14 15 16 17 18 19];`

Accessing vector elements

Individual elements of an array A or string S are accessed by A(i)

Try `A(7)`

Putting a semicolon after a command suppresses output.

Try `a;`

Now try `a`

Displaying values

`disp (x)` displays the value of `x`

Try `disp(A)` and `disp(A(2))`

Putting a semicolon after a command suppresses output.

Try `disp(a);`

'for' loop

for loops in MATLAB can be implemented with

```
for count = start value : end value
    statement
```

```
end
```

Try

```
for i = 1:20
  x(i)= i;
  disp(x(i))
end;
```

`disp(x)` displays the value of `x`

Strings in MATLAB

Strings of characters can be defined in MATLAB with the ' delimiter.

Try `textstring = 'a string of text'`

Individual elements of the string can be accessed with the number of the element (starting from 1) in parentheses.

Try `textstring(5)`

Useful MATLAB commands

factor(n) returns the prime factors of n

for loop for i = 1:20 x(i)= i; end

if statement if (x==1) disp(x)

mod(x, y) returns x mod y

length(x) returns the length of a vector x

break ends execution of current for loop

disp(x) displays the value of x

5. Assessment

A report is required for this lab. The report is to consist of the following sections

1. An outline of the RSA algorithm (2 marks)
2. Your MATLAB code for breaking the algorithm with explanation as to what the code does. (2 marks).
3. The results from running your code and the first decrypted message (2 marks)
4. The results from running your code and second decrypted message (2 marks)

The assignment is to be submitted via TURNITIN. Please note that **duplicated code will be treated as plagiarism**.