

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.

If you decide to use the online version of MATLAB you will need to set up a Mathworks account to access Matlab Online. To do this go to:

<https://matlab.mathworks.com>

And follow the prompts. You will need to use your Swinburne account to set up the account.

You can copy text from Matlab Online onto your desktop using CTRL-c and CTRL-v to paste it.

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.

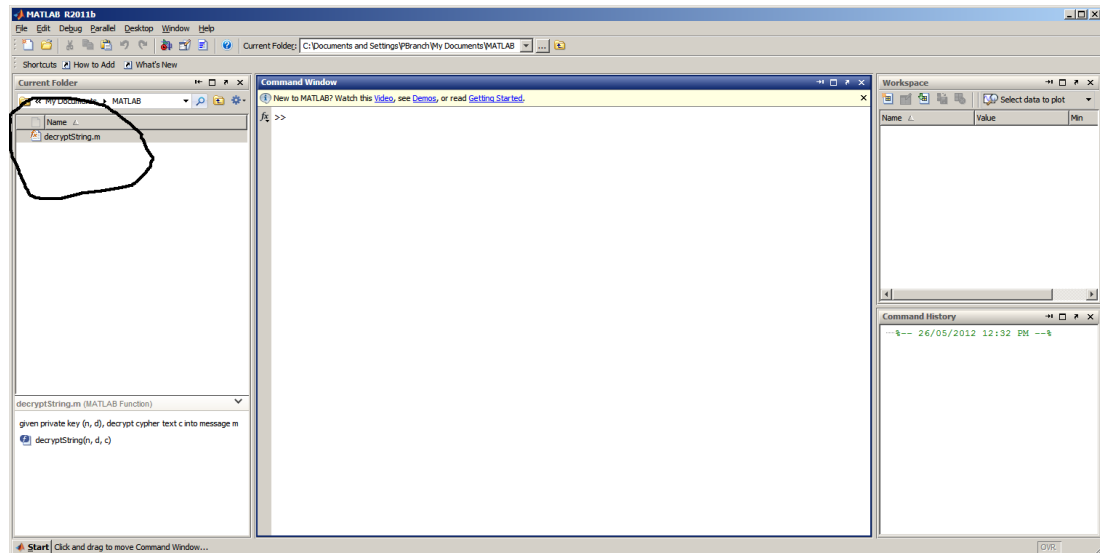
2. Method

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

```
1. c = [2377    400    2296    640    1142    1770    2014    540    1188
        1285    586    1421    1770    586    1142    2395    640    479
        640    1205    2395    1770    586    1142    1770    1421    479
        602    2014    2395    476    1019    479    1274    2014    2296
        602    1770    194    1274    1205    1770    1950    540    1205
        2395    1770    640    2011    640    479    1019    586    1142
        1019    1770    586    1142    1770    2395    2296    640    1770
        1285    1274    2395    640    1770    1205    640    1904    640
        1142    2395    586    640    1205    1770    1274    1142    1741
        1770    640    1274    479    1285    602    1770    640    586
        1019    2296    2395    586    640    1205    174    1770    2395
        2296    640    1770    1319    1274    2395    586    476    1142
        1274    1285    1770    1295    640    1421    540    479    586
        2395    602    1770    1    1019    640    1142    1421    602
        1770    2011    1274    1741    640    1770    1205    640    1904
        640    479    1274    1285    1770    1274    2395    2395    640
        2011    2014    2395    1205    1770    2395    476    1770    1348
        540    1274    1205    2296    1770    586    2395    1216];
```

2. 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:

Laboratory Session 5



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

3. 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 .
4. 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.

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

```
c = [4514  5363  2971  7198  1332  5465  2980  454   7130  1332
      2682  4485  6069  5363  1332  6069  5363  7130  1332  1889
      2957  2682  5943  2971  4580  1332  1889  5561  2980  4580
      6069  2971  4580  7130  1332  4485  2178  1332  4580  5561
      3243  1889  6069  4485  5465  5561  2980  1889  5363  3243
      1332  5943  4485  6069  7198  1332  4485  2178  1332  2957
      3647  7130  4900  1889  7130  4580  6069  7130  1145  1332
      1889  2957  2682  5943  2971  4580  2971  6069  3243  656
      7023  1332  5585  5363  2971  6069  2178  2971  7130  5943
      1145  1332  431   2971  2178  2178  2971  7130  1332  2971
      3647  1332  7023   1    1889  1889  5943  2971  7130  1145
      1332  108   5561  3243  1889  6069  4485  5465  5561  2980
      1889  5363  3243  3646  7023  656   1332  6689  2980  2682
      5561  2971  1145  5465  7130  1145  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 .

Laboratory Session 5

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

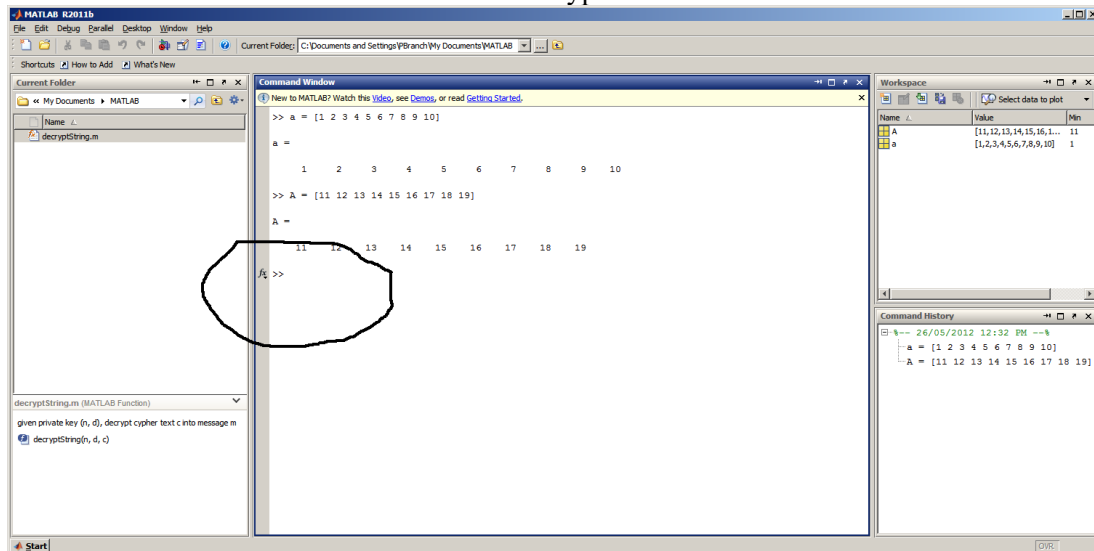
To encrypt m , compute $c = (m^e) \bmod n$

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.



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 $A(7)$

Laboratory Session 5

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`

Laboratory Session 5

5. Assessment

Assessment of this lab is from a short report explaining what you did, what you observed and explanation as to what you saw. Grade is either pass / not pass. If the report is not passed you will be asked to resubmit an improved version of it.

The report is to comprise:

Title

This is to be “NSR/AS Lab 4 – Public Key Cryptography” followed by the student’s name and student id.

Abstract

No more than 200 words summarising the report.

Introduction to Public Key Cryptography

This is to be no more than 1 A4 page describing RSA public key algorithm (NOTE: One page is a maximum, not a recommendation.) It is to outline of the RSA algorithm.

Breaking the RSA algorithm

This is to be no more than one A4 page. This is to include your MATLAB code for breaking the algorithm with explanation as to what the code does.

Results

This is to be no more than two A4 pages.

This section is to include:

- The results from running your code and the first decrypted message
- The results from running your code and second decrypted message

Conclusion

No more than half a page summarising the main points of the report.

References

All sources are to be properly referenced. Use IEEE referencing. DO NOT JUST PROVIDE A LIST OF WEBPAGES.

Diagrams

All diagrams are to be numbered and captioned. If they are not the student’s original work, they are to be referenced.

You may use any standard formatting you like, although IEEE is preferred.