Exercise 7 RSA Cryptography

Encrypt and Decrypt letter ‘A’

In this exercise, you are not making a program. Instead, your pretend that you are a computer and perform the exercise in your head writing the results and steps on paper.

Before doing the exercise, read “RSA Algorithm Overview**”** document (see **RSA Algorithm Overview.pdf** file).

In real life, RSA Algorithm uses very big numbers. In this exercise, we use small numbers and encrypt/decrypt just one letter ‘A’. Nevertheless, the intermediate numbers can become very large (depending on your calculation method). So, use online calculator at http://comptune.com/calc.php if needed.

The following parameters are given

p	7	
q	37	
e	257	
d	137	
M	65	(just one letter ‘A’)

Calculate the numbers n, $\phi(n)$, and the ciphertext number C.

Assuming that the ciphertext number C is known but the plaintext number M is not, calculate the correspondent plaintext number M'. Compare M and M' and verify that they are the same.

The second page of this document contains a form for you to fill. Print the page and write down your answers on the page including the following

- All given numbers (the parameter names and values)
- All calculated numbers
- All formulas that you used to calculate them

Bob wants everybody to be able to send him messages, encrypted via RSA, that only he can read. Alice wants to send Bob message M so only Bob can read it. Write down on paper

- What numbers Bob shall communicate to everybody?
- What numbers Bob shall keep to himself?
- What numbers Alice can safely show to other people (so the people still cannot read her message to Bob)?
- What numbers Alice has to calculate before sending the encrypted message?
- What numbers Bob has to calculate before decrypting the message (except the numbers communicated to everybody)?

If your answers do not fit on the page, use some other paper page. it is OK to write multiple names, values, and formulas on one line.

Scan the page(s) and submit the resulting image file into **Exercise7** folder.

All given numbers (the parameter names and values, it is OK to write multiple numbers on one line)

While calculating ciphertext number C

All calculated numbers (the parameter names and values)

All formulas that you used to calculate them

While calculating plaintext number M'

All calculated numbers s (the parameter names and values)

All formulas that you used to calculate them

Below write just the names, not actual values

What numbers Bob shall communicate to everybody?

What numbers Bob shall keep to himself?

What numbers Alice can safely show to other people (so the people still cannot read her message to Bob)?

What numbers Alice has to calculate before sending the encrypted message?

What numbers Bob has to calculate before decrypting the message (except the numbers communicated to everybody)?