Assignment for Grid Infrastructure 24-28th February 2011

Please note that the mark for the assignment is **60%**.

**Submission deadline: Friday 7th March 2011**

1. Classic description of RSA algorithm uses two characters Alice and Bob, with Bob sending Alice an encrypted message that Alice decrypts. Create a workflow of an example RSA algorithm to encrypt an integer and demonstrate the decryption. You can create the workflow from a WSDL based webservice or as a Java application.

* Use smaller prime numbers to create the workflow using Taverna on your laptop.
* Download and install Liferay portal on your laptop. Modify your RSA application to receive the two prime numbers and the message as input. Embed your application within Liferay portal with a customised user interface to input the parameters for your application and submit/execute that. Your portal interface should display the public key exponent, the private key exponent, the Euler number and the encrypted message and the decrypted message.
* Use the P-Grade portal workflow to demonstrate your application using larger prime numbers by submitting the job to NGS. You can use publicly available software to:
* generate larger prime numbers,
* calculate the multiplicative inverse which is the private key exponent. The algorithm for this is the Extended Euclidean algorithm.
* (Optional): You may use MPI and run your job on more than one processor.

1. Write a short critical review on ease of use, based on your experience, of Taverna, Liferay and P-Grade portal (around 800 words).