Configuration of the JDK environment & Installation of the Bouncing Castle JCE Security Provider

T. Andrew Yang (yang@uhcl.edu)

(last updated: 1/26/2012)

Installation/Configuration instructions Common errors & solutions

---

A. Installation and Configuration Instructions

Note: This installation assumes jdk1.5 (i.e., J2SE 5.0) is installed. If a different version of JDK is used, minor adjustments in steps 2 and 3 are needed.

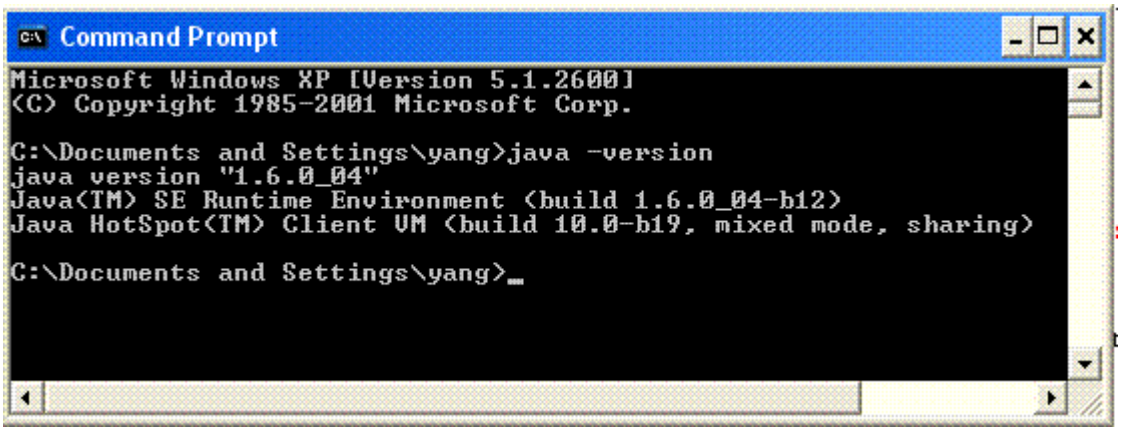
Step 1) Go to http://java.sun.com/j2se/ and download the most recent version of JDK (e.g., J2SE 5.0). After installing the JDK, set the system *path* to ensure the JDK is your default JDK.

Step 2) The JDK you downloaded and installed is of the default strength, that is, *Strong* but not *Unlimited*. To increase your JDK's strength to *Unlimited*, do the following:

(a) Download the **right** version of Java Cryptography Extension (JCE) *Unlimited Strength Jurisdiction Policy Files* from where you downloaded the JDK (e.g., http://java.sun.com/j2se/1.5.0/download.jsp). **Note1: Scroll down to the bottom of the download page to find the policy files. Note2: The version of the policy files must be the same as the version of your JDK.**

(b) Suppose the file you downloaded is called jce_policy-1_5_0.zip. Unzip the file into a temporary folder (e.g., c:\jce\ ). From the folder, copy the two .jar files (**local_policy.jar** and **US_export_policy.jar**) into the **jre\lib\security** folder **of your JDK installation**. For example, if your JDK is installed as c:\j2sdk1.4.2_04, copy the two files into the folder c:\ j2sdk1.4.2_04\jre\lib\security. **NOTE:** The folder may already have two files with the same names. Just answer 'YesToAll' when prompted to overwrite the existing files.

CAUTION: Use the '**java –version**' command to check whether you're running the java program from your JDK's bin folder or from the bin folder under your JRE (Java Runtime Environment) folder. As shown in the diagram below, the latter is true on this particular system. In the latter case, make sure you copy the two .jar files (**local_policy.jar** and **US_export_policy.jar**) into the **lib\security** folder **of your JRE folder.**



(c) It may be necessary to restart your computer before the newly installed policy files would start working.

Note: The installation procedure is described in details in the README.txt file.

Step 3) Download the **right** version of *Bouncing Castle JCE provider* for the JDK in your system from http://www.bouncycastle.org/latest_releases.html, and save it to the local disk. For example,
if your JDK is v1.4, then download the file bcprov-jdk14-131.jar. If your JDK is v1.5, then download bcprov-jdk15-131.jar instead.

Note: Initial testing appears to confirm that JDK 1.7 is compatible with Bouncing Castle 1.6.

Step 4) Set the *classpath* environment variable to include the downloaded file in step 1. To set the classpath, do the following:

a) Right click the *My Computer* icon on the desktop and then click on the properties tab.

b) Click the *Advanced* tab.

c) Click the *Environment Variables* button.

d) In the *User Variables* section click on the *New…* button.

e) Set the *Variable Name* to *classpath*

f) Set the *Variable Value* to the location of the downloaded file. For example, if the downloaded file was stored at *m:\security**bcprov-jdk15-131.jar***, then the value is set to *%classpath%; m:\security**bcprov-jdk15-131.jar*** (or the name of the *Bouncing Castle JCE provider* you downloaded in step 3). **Note:** If the file you downloaded is called *bcprov-jdk15-131.zip*, you may either change the zip extension to jar, or simply use the zip extension instead when setting the classpath.

As a temporary method, you may type, in a DOS window, the following command: 'set classpath=*%classpath%; .;m:\security\bcprov-jdk15-131.jar*'.

Note: The *set* command only sets the classpath once for that particular DOS window.
Note: The folder '**.**' refers to the current folder.

To verify the above steps, do the following:
a) Open a 'command prompt' window (START-Programs-Accessories-Command Prompt).
b) Enter the 'path' command to see if your JDK's bin folder is in the path.
c) Enter the 'set' command, and check if the classpath is correct (as in step 4).
d) Enter 'java –version' to verify the version of the java interpreter.

Step 5) In each of the .java source files, include this line of code:

Security.addProvider(new org.bouncycastle.jce.provider.BouncyCastleProvider());

anywhere before the line

Cipher cipher = Cipher.getInstance("RSA/ECB/PKCS1Padding");

For example, place it as the first statement in the *main( )* method.

Step 6) Compile and run the programs.

Note: As any other new tool you first try to use, it takes some time for a new user to become efficient. If you get compilation or runtime errors, double check the procedure above. The steps have been tested and should work, if followed correctly. The rule of thumb is always double check to ensure what you did was correct and effective. See the following table to find common errors and possible solutions.

B. Common Errors and Possible Solutions:

Errors	Possible Reasons and Solutions
a) Exception in thread "main" java.lang.**NoClassDefFoundError**	• Check your **classpath** (not **path**) environment variable; make sure the current folder (.) is included in the classpath.
b) Exception in thread "main" java.security.InvalidKeyException: **Illegal key size**	• Make sure step #2 above (configuring unlimited strength) is done correctly. The default (limited) strength does not support larger number of key bits.
c) Exception in thread "main" java.security.**NoSuchAlgorithmException**: PBEWithSHAAndTwofish-CBC SecretKeyFactory not available	• This is probably caused by improper configuration of your security provider. Make sure step

	#3, #4, and #5 are **all** done correctly.