CO3326 Computer Security 2015-16

Code specification CO3326 cw2 V2

This description contains the requirements for the **code submission**, to be read in conjunction with the actual assignment with which you are already familiar. You must follow these instructions carefully, as your code submission will be processed automatically and will receive a mark of 0 if it does not pass all the test cases detailed below.

IMPORTANT:

- **There is a separate .zip download for CW2**
- **You must implement the protocol as described in the coursework assignment document. The report provides you with an opportunity to discuss other protocols and their benefits or disadvantages**
- **The test harness will check for a complete communication chain and, in order to gain the highest marks, students will need to decrypt and parse**
- **Do not use BigInteger**

Make sure you study and understand the examples of inputs and outputs which follow the general and technical guidelines. These extend on the descriptions given in the original coursework assignment document.

General guidelines

- You will submit a *single JAR file* for each coursework following a *specific naming scheme*.

- Your code must compile and run against *Java 8*.
- The entry point in your code will have a main method, which receives one command-line argument, the absolute path to an *input file*.
- Your programme will read the input file and treats each line as a separate *test case* / separate instance of the problem.
- Each line in the test file is a JSON object.
- Your programme will print a single line of text, containing one JSON object, for every single input line. Therefore the number of input lines will match the number of output lines.
- The JSON objects, both input and output, have a *strict format* you **must** conform to; details are provided below, with examples.

Prerequisites

- Make sure you have *Java 8 Development Kit* installed.

```
    $ java -version
```

```
    java version "1.8.0_66"
    Java(TM) SE Runtime Environment (build 1.8.0_66-b17
)
    Java HotSpot(TM) 64-Bit Server VM (build 25.66-b17,
mixed mode)
```

- The minor version (in this case 66) is unimportant. If you don't have Java 8 Development Kit installed, install it: http://www.oracle.com/technetwork/java/javase/downloads/ind (available for all platforms).
- Set up the *Maven* build system. Instructions are available here: https://maven.apache.org/install.html (for all platforms).
- Double-check that you have at least Maven 3.3.3:

```
    $ mvn -v
```

```
    Apache Maven 3.3.3 (7994120775791599e205a5524ec3e0d
fe41d4a06; 2015-04-22T12:57:37+01:00)
    Maven home: /usr/local/Cellar/maven/3.3.3/libexec
    Java version: 1.8.0_66, vendor: Oracle Corporation
    Java home: /Library/Java/JavaVirtualMachines/jdk1.8
.0_66.jdk/Contents/Home/jre
    Default locale: en_US, platform encoding: UTF-8
    OS name: "mac os x", version: "10.11.2", arch: "x86
_64", family: "mac"
```

Setup

- Extract the provided ZIP file and you will have a new **co3326** folder for cw2, which will be referred to as your *project folder*; navigate to it using a command-line prompt.
- Double-check that you have the following folder structure:

```
/co3326/
    |-- pom.xml
    |-- test-cw2.txt
    |-- /src/
        |-- /main/
            |-- /java/
                |-- /co3326/
                    |-- App.java
                    |-- Cw2.java
                    |-- Message.java
                    |-- User.java
            |-- /resources/
                |-- config.properties
```

- Edit the `pom.xml` file
- Look for the following lines:

```
<student.name>FamilyName</student.name>
<student.srn>27644437</student.srn>
<coursework.number>2</coursework.number>
```

- Replace `FamilyName` with your family name using a CamelCase syntax, **without** blanks or dashes or underscores, for example, if your family name is Zuckerberg, use *Zuckerberg*.
- Replace `27644437` with your SRN.
- Set the `coursework.number` accordingly, i.e. *2* for CW2.
- Save the `pom.xml` file.

Build

- Open a command-line prompt and navigate to your project folder (`co3326`).
- Build the project with the following command:

```
    $ mvn clean package
```

- This should have an output ending with:

```
    ...

    [INFO] ------------------------------------------
---------------------------
    [INFO] BUILD SUCCESS
    [INFO] ------------------------------------------
---------------------------
    [INFO] Total time: 3.114 s
    [INFO] Finished at: 2016-01-06T00:28:35+00:00
    [INFO] Final Memory: 20M/171M
    [INFO] ------------------------------------------
---------------------------
```

- A new **target** folder should have appeared in your project folder (`co3326/target/`), which should contain - among others - a `FamilyName_27644437_CO3326CW2-jar-with-dependencies.jar` file. Obviously, the file name will have your family name, SRN and the coursework number; for example, if your family name is *Zuckerberg*, your SRN is 27644437, the file will be `Zuckerberg_27644437_CO3326CW2-jar-with-dependencies.jar`

Test

- The JAR file obtained with the build process is executable and contains both the Java byte code and the source code.
- There is a *test file* in your project folder, `test-cw2.txt` which is a valid test file. You must ensure that your code runs successfully against the test file; this will satisfy the automatic testing process, which will use a similar test.
- In a command-line prompt issue the following command:

```
    $ java -jar target/FamilyName_27644437_CO3326CW2-ja
r-with-dependencies.jar test-cw2.txt
```

- The output should be similar to this (with your family name and

SRN):

```
FamilyName
27644437
{}
{"A":{}}
{"A":{},"B":{},"S":{}}
```

Develop

The source folder, where your code will have to go is `src/main/java/` within yout project folder. You have a **co3326** top level package (`src/main/java/co3326`). Look at the `App.java` , `Cw2.java` , `Message.java` and `User.java` files which are already in there. These provide a starting point for your code and help you with the reading of the input file, parsing of the input lines and creation of JSON representations of the test cases as well as printing the JSON results. You can place your code next to these files. The *main* method is in the `co3326.App` class.

For serializing / de-serializing JSON objects, Google's Gson library is used (https://github.com/google/gson). The build system (i.e. Maven) sorts out the dependency for you and bundles the library in your JAR file when you build the project.

You may use an IDE of your choice. Eclipse, IntelliJ IDEA and NetBeans are popular choices and available for all platforms. Most IDEs, including the ones mentioned, have support for Maven and will recognise your project when you import it.

Required output: *Coursework 2*

Inspect the `test-cw2.txt` in your project folder:

```
{  }
{ "A" : { "rsa" : { "p" : 313, "q" : 787 }, "nonce" : 1
066 } }
{ "A" : { "rsa" : { "p" : 313, "q" : 787, "e" : 196091
}, "nonce" : 1812 }, "B": { "rsa" : { "p" : 157, "q" :
641, "e" : 29203 }, "nonce" : 1989 }, "S" : { "rsa" : {
"p" : 373, "q" : 977, "e" : 258845 } } }
```

The following output is correct for this test file, both in terms of *format* and *content*:

FirstnameLastname
27644437
{"A":{"rsa":{"p":109,"q":811,"e":33013,"n":88399,"r":87480,"d":32437},"nonce":756132204},"B":{"rsa":{"p":353,"q":1013,"e":324535,"n":357589,"r":356224,"d":341127},"nonce":1048794305},"S":{"rsa":{"p":277,"q":643,"e":141295,"n":178111,"r":177192,"d":157255}},"communication":[{"text":"Dear S, This is A and I would like to get B-s public key. Yours sincerely, A.","encoded":[68,101,97,114,32,83,44,32,84,104,105,115,32,105,115,32,65,32,97,110,100,32,73,32,119,111,117,108,100,32,108,105,107,101,32,116,111,32,103,101,116,32,66,45,115,32,112,117,98,108,105,99,32,107,101,121,46,32,89,111,117,114,115,32,115,105,110,99,101,114,101,108,121,44,32,65,46]},{"text":"Dear A, Here is B-s public key [324535,357589] signed by me. Yours sincerely, S.","encoded":[68,101,97,114,32,65,44,32,72,101,114,101,32,105,115,32,66,45,115,32,112,117,98,108,105,99,32,107,101,121,32,91,51,50,52,53,51,53,44,51,53,55,53,56,57,93,32,115,105,103,110,101,100,32,98,121,32,109,101,46,32,89,111,117,114,115,32,115,105,110,99,101,114,101,108,121,44,32,83,46],"encrypted":[161763,139071,154994,53299,156678,30367,118819,156678,7435,139071,53299,139071,156678,167243,79198,156678,153222,114130,79198,156678,110653,71583,68220,142586,167243,133295,156678,88739,139071,117787,156678,117181,56924,93519,58094,47794,56924,47794,118819,56924,47794,58654,47794,138849,53823,74060,156678,79198,167243,41771,69139,139071,140946,156678,68220,117787,156678,112724,139071,150947,156678,101303,15636,71583,53299,79198,156678,79198,167243,69139,133295,139071,53299,139071,142586,117787,118819,156678,110058,150947]},{"text":"Dear B, This is A and I have sent you a nonce [756132204] only you can read. Yours sincerely, A.","encoded":[68,101,97,114,32,66,44,32,84,104,105,115,32,105,115,32,65,32,97,110,100,32,73,32,104,97,118,101,32,115,101,110,116,32,121,111,117,32,97,32,110,111,110,99,101,32,91,55,53,54,49,51,50,50,48,52,93,32,111,110,108,121,32,121,111,117,32,99,97,110,32,114,101,97,100,46,32,89,111,117,114,115,32,115,105,110,99,101,114,101,108,121,44,32,65,46],"encrypted":[94936,143730,225689,124426,264573,50465,12993,264573,15958,27850,351072,26388,264573,351072,26388,264573,279269,264573,225689,159830,49833,264573,275401,264573,27850,225689,291493,143730,264573,26388,143730,159830,32553

6,264573,207921,324145,14569,264573,225689,264573,15983
0,324145,159830,280113,143730,264573,237652,43566,17832
8,44893,44514,113778,262994,262994,317051,95428,75341,2
64573,324145,159830,303758,207921,264573,207921,324145,
14569,264573,280113,225689,159830,264573,124426,143730,
225689,49833,350682,264573,213795,324145,14569,124426,2
6388,264573,26388,351072,159830,280113,143730,124426,14
3730,303758,207921,12993,264573,279269,350682]},{"text"
:"Dear S, This is B and I would like to get A-s public
key. Yours sincerely, B.","encoded":[68,101,97,114,32,8
3,44,32,84,104,105,115,32,105,115,32,66,32,97,110,100,3
2,73,32,119,111,117,108,100,32,108,105,107,101,32,116,1
11,32,103,101,116,32,65,45,115,32,112,117,98,108,105,99
,32,107,101,121,46,32,89,111,117,114,115,32,115,105,110
,99,101,114,101,108,121,44,32,66,46]},{"text":"Dear B,
Here is A-s public key [33013,88399] signed by me. Your
s sincerely, S.","encoded":[68,101,97,114,32,66,44,32,7
2,101,114,101,32,105,115,32,65,45,115,32,112,117,98,108
,105,99,32,107,101,121,32,91,51,51,48,49,51,44,56,56,51
,57,57,93,32,115,105,103,110,101,100,32,98,121,32,109,1
01,46,32,89,111,117,114,115,32,115,105,110,99,101,114,1
01,108,121,44,32,83,46],"encrypted":[161763,139071,1549
94,53299,156678,153222,118819,156678,7435,139071,53299,
139071,156678,167243,79198,156678,30367,114130,79198,15
6678,110653,71583,68220,142586,167243,133295,156678,887
39,139071,117787,156678,117181,56924,56924,52341,63310,
56924,118819,138849,138849,56924,53823,53823,74060,1566
78,79198,167243,41771,69139,139071,140946,156678,68220,
117787,156678,112724,139071,150947,156678,101303,15636,
71583,53299,79198,156678,79198,167243,69139,133295,1390
71,53299,139071,142586,117787,118819,156678,110058,1509
47]},{"text":"Dear A, Here is my nonce [1048794305] and
yours [756132204], proving I decrypted it. Yours sincer
ely, B.","encoded":[68,101,97,114,32,65,44,32,72,101,11
4,101,32,105,115,32,109,121,32,110,111,110,99,101,32,91
,49,48,52,56,55,57,52,51,48,53,93,32,97,110,100,32,121,
111,117,114,115,32,91,55,53,54,49,51,50,50,48,52,93,44,
32,112,114,111,118,105,110,103,32,73,32,100,101,99,114,
121,112,116,101,100,32,105,116,46,32,89,111,117,114,115
,32,115,105,110,99,101,114,101,108,121,44,32,66,46],"en
crypted":[78984,81306,63225,32925,22813,28075,3426,2281
3,41487,81306,32925,81306,22813,44468,67741,22813,12208
,70191,22813,40658,62132,40658,8815,81306,22813,87374,1

7911,65489,20434,69773,39731,28289,20434,69766,65489,30398,80099,22813,63225,40658,84126,22813,70191,62132,77398,32925,67741,22813,87374,39731,30398,54,17911,69766,29092,29092,65489,20434,80099,3426,22813,49512,32925,62132,25092,44468,40658,59135,22813,43076,22813,84126,81306,8815,32925,70191,49512,35086,81306,84126,22813,44468,35086,31329,22813,38776,62132,77398,32925,67741,22813,67741,44468,40658,8815,81306,32925,81306,85237,70191,3426,22813,56528,31329]},{"text":"Dear B, Here is your nonce [1048794305] proving I decrypted it. Yours sincerely, A.","encoded":[68,101,97,114,32,66,44,32,72,101,114,101,32,105,115,32,121,111,117,114,32,110,111,110,99,101,32,91,49,48,52,56,55,57,52,51,48,53,93,32,112,114,111,118,105,110,103,32,73,32,100,101,99,114,121,112,116,101,100,32,105,116,46,32,89,111,117,114,115,32,115,105,110,99,101,114,101,108,121,44,32,65,46],"encrypted":[94936,143730,225689,124426,264573,50465,12993,264573,35862,143730,124426,143730,264573,351072,26388,264573,207921,324145,14569,124426,264573,159830,324145,159830,280113,143730,264573,237652,44514,317051,95428,180788,43566,132930,95428,113778,317051,178328,75341,264573,57768,124426,324145,291493,351072,159830,288269,264573,275401,264573,49833,143730,280113,124426,207921,57768,325536,143730,49833,264573,351072,325536,350682,264573,213795,324145,14569,124426,26388,264573,26388,351072,159830,280113,143730,124426,143730,303758,207921,12993,264573,279269,350682]}]}
{"A":{"rsa":{"p":313,"q":787,"e":151819,"n":246331,"r":245232,"d":58963},"nonce":1066},"B":{"rsa":{"p":349,"q":743,"e":146623,"n":259307,"r":258216,"d":156367},"nonce":1884542388},"S":{"rsa":{"p":389,"q":661,"e":24881,"n":257129,"r":256080,"d":43361}},"communication":[{"text":"Dear S, This is A and I would like to get B-s public key. Yours sincerely, A.","encoded":[68,101,97,114,32,83,44,32,84,104,105,115,32,105,115,32,65,32,97,110,100,32,73,32,119,111,117,108,100,32,108,105,107,101,32,116,111,32,103,101,116,32,66,45,115,32,112,117,98,108,105,99,32,107,101,121,46,32,89,111,117,114,115,32,115,105,110,99,101,114,101,108,121,44,32,65,46]},{"text":"Dear A, Here is B-s public key [146623,259307] signed by me. Yours sincerely, S.","encoded":[68,101,97,114,32,65,44,32,72,101,114,101,32,105,115,32,66,45,115,32,112,117,98,108,105,99,32,107,101,121,32,91,49,52,54,54,50,51,44,50,

53,57,51,48,55,93,32,115,105,103,110,101,100,32,98,121,32,109,101,46,32,89,111,117,114,115,32,115,105,110,99,101,114,101,108,121,44,32,83,46],"encrypted":[224497,34730,255646,71417,56123,247739,151719,56123,71364,34730,71417,34730,56123,38246,208619,56123,46757,20926,208619,56123,203932,84339,88214,133126,38246,95618,56123,211357,34730,18142,56123,99307,83313,19080,242154,242154,156349,46265,151719,156349,101753,122729,46265,203887,251596,92673,56123,208619,38246,138226,76197,34730,116036,56123,88214,18142,56123,95158,34730,104859,56123,70675,39027,84339,71417,208619,56123,208619,38246,76197,95618,34730,71417,34730,133126,18142,151719,56123,179487,104859]},{"text":"Dear B, This is A and I have sent you a nonce [1066] only you can read. Yours sincerely, A.","encoded":[68,101,97,114,32,66,44,32,84,104,105,115,32,105,115,32,65,32,97,110,100,32,73,32,104,97,118,101,32,115,101,110,116,32,121,111,117,32,97,32,110,111,110,99,101,32,91,49,48,54,54,93,32,111,110,108,121,32,121,111,117,32,99,97,110,32,114,101,97,100,46,32,89,111,117,114,115,32,115,105,110,99,101,114,101,108,121,44,32,65,46],"encrypted":[48133,9385,232314,147475,159475,165738,247301,159475,70192,27996,161063,17711,159475,161063,17711,159475,16999,159475,232314,103212,221095,159475,183394,159475,27996,232314,5794,9385,159475,17711,9385,103212,247461,159475,15082,69210,247275,159475,232314,159475,103212,69210,103212,224649,9385,159475,160177,33478,111411,170523,170523,247356,159475,69210,103212,201484,15082,159475,15082,69210,247275,159475,224649,232314,103212,159475,147475,9385,232314,221095,48544,159475,86522,69210,247275,147475,17711,159475,17711,161063,103212,224649,9385,147475,9385,201484,15082,247301,159475,16999,48544]},{"text":"Dear S, This is B and I would like to get A-s public key. Yours sincerely, B.","encoded":[68,101,97,114,32,83,44,32,84,104,105,115,32,105,115,32,66,32,97,110,100,32,73,32,119,111,117,108,100,32,108,105,107,101,32,116,111,32,103,101,116,32,65,45,115,32,112,117,98,108,105,99,32,107,101,121,46,32,89,111,117,114,115,32,115,105,110,99,101,114,101,108,121,44,32,66,46]},{"text":"Dear B, Here is A-s public key [151819,246331] signed by me. Yours sincerely, S.","encoded":[68,101,97,114,32,66,44,32,72,101,114,101,32,105,115,32,65,45,115,32,112,117,98,108,105,99,32,107,101,121,32,91,49,53,49,56,49,57,44,50,52,54,51,51,49,93,32,115,105,103,110,101,100

,32,98,121,32,109,101,46,32,89,111,117,114,115,32,115,1
05,110,99,101,114,101,108,121,44,32,83,46],"encrypted":
[224497,34730,255646,71417,56123,46757,151719,56123,713
64,34730,71417,34730,56123,38246,208619,56123,247739,20
926,208619,56123,203932,84339,88214,133126,38246,95618,
56123,211357,34730,18142,56123,99307,83313,101753,83313
,84450,83313,122729,151719,156349,19080,242154,46265,46
265,83313,92673,56123,208619,38246,138226,76197,34730,1
16036,56123,88214,18142,56123,95158,34730,104859,56123,
70675,39027,84339,71417,208619,56123,208619,38246,76197
,95618,34730,71417,34730,133126,18142,151719,56123,1794
87,104859]},{"text":"Dear A, Here is my nonce [18845423
88] and yours [1066], proving I decrypted it. Yours sin
cerely, B.","encoded":[68,101,97,114,32,65,44,32,72,101
,114,101,32,105,115,32,109,121,32,110,111,110,99,101,32
,91,49,56,56,52,53,52,50,51,56,56,93,32,97,110,100,32,1
21,111,117,114,115,32,91,49,48,54,54,93,44,32,112,114,1
11,118,105,110,103,32,73,32,100,101,99,114,121,112,116,
101,100,32,105,116,46,32,89,111,117,114,115,32,115,105,
110,99,101,114,101,108,121,44,32,66,46],"encrypted":[90
843,32273,24766,31335,150397,86468,36588,150397,27699,3
2273,31335,32273,150397,155105,183725,150397,82612,1391
04,150397,171852,157712,171852,45484,32273,150397,10825
3,62339,197197,197197,21795,165241,21795,221906,136905,
197197,197197,159373,150397,24766,171852,72824,150397,1
39104,157712,62319,31335,183725,150397,108253,62339,861
33,78196,78196,159373,36588,150397,117641,31335,157712,
63963,155105,171852,123748,150397,100109,150397,72824,3
2273,45484,31335,139104,117641,104921,32273,72824,15039
7,155105,104921,164526,150397,107893,157712,62319,31335
,183725,150397,183725,155105,171852,45484,32273,31335,3
2273,50845,139104,36588,150397,29037,164526]},{"text":"
Dear B, Here is your nonce [1884542388] proving I decry
pted it. Yours sincerely, A.","encoded":[68,101,97,114,
32,66,44,32,72,101,114,101,32,105,115,32,121,111,117,11
4,32,110,111,110,99,101,32,91,49,56,56,52,53,52,50,51,5
6,56,93,32,112,114,111,118,105,110,103,32,73,32,100,101
,99,114,121,112,116,101,100,32,105,116,46,32,89,111,117
,114,115,32,115,105,110,99,101,114,101,108,121,44,32,65
,46],"encrypted":[48133,9385,232314,147475,159475,16573
8,247301,159475,205632,9385,147475,9385,159475,161063,1
7711,159475,15082,69210,247275,147475,159475,103212,692
10,103212,224649,9385,159475,160177,33478,190745,190745

,124640,164300,124640,133125,45215,190745,190745,247356
,159475,135008,147475,69210,5794,161063,103212,218884,1
59475,183394,159475,221095,9385,224649,147475,15082,135
008,247461,9385,221095,159475,161063,247461,48544,15947
5,86522,69210,247275,147475,17711,159475,17711,161063,1
03212,224649,9385,147475,9385,201484,15082,247301,15947
5,16999,48544]}]}
{"A":{"rsa":{"p":313,"q":787,"e":196091,"n":246331,"r":
245232,"d":52883},"nonce":1812},"B":{"rsa":{"p":157,"q"
:641,"e":29203,"n":100637,"r":99840,"d":48667},"nonce":
1989},"S":{"rsa":{"p":373,"q":977,"e":258845,"n":364421
,"r":363072,"d":74933}},"communication":[{"text":"Dear
S, This is A and I would like to get B-s public key. Yo
urs sincerely, A.","encoded":[68,101,97,114,32,83,44,32
,84,104,105,115,32,105,115,32,65,32,97,110,100,32,73,32
,119,111,117,108,100,32,108,105,107,101,32,116,111,32,1
03,101,116,32,66,45,115,32,112,117,98,108,105,99,32,107
,101,121,46,32,89,111,117,114,115,32,115,105,110,99,101
,114,101,108,121,44,32,65,46]},{"text":"Dear A, Here is
B-s public key [29203,100637] signed by me. Yours since
rely, S.","encoded":[68,101,97,114,32,65,44,32,72,101,1
14,101,32,105,115,32,66,45,115,32,112,117,98,108,105,99
,32,107,101,121,32,91,50,57,50,48,51,44,49,48,48,54,51,
55,93,32,115,105,103,110,101,100,32,98,121,32,109,101,4
6,32,89,111,117,114,115,32,115,105,110,99,101,114,101,1
08,121,44,32,83,46],"encrypted":[118729,40313,161154,53
846,184591,39926,183659,184591,138538,40313,53846,40313
,184591,151404,359645,184591,230781,346794,359645,18459
1,638,267401,228780,67179,151404,145992,184591,47308,40
313,363125,184591,74612,209108,1042,209108,50072,130951
,183659,312418,50072,50072,18558,130951,227987,272757,1
84591,359645,151404,196392,69537,40313,47323,184591,228
780,363125,184591,162611,40313,171648,184591,271083,330
341,267401,53846,359645,184591,359645,151404,69537,1459
92,40313,53846,40313,67179,363125,183659,184591,246996,
171648]},{"text":"Dear B, This is A and I have sent you
a nonce [1812] only you can read. Yours sincerely, A.",
"encoded":[68,101,97,114,32,66,44,32,84,104,105,115,32,
105,115,32,65,32,97,110,100,32,73,32,104,97,118,101,32,
115,101,110,116,32,121,111,117,32,97,32,110,111,110,99,
101,32,91,49,56,49,50,93,32,111,110,108,121,32,121,111,
117,32,99,97,110,32,114,101,97,100,46,32,89,111,117,114
,115,32,115,105,110,99,101,114,101,108,121,44,32,65,46]

,"encrypted":[27990,59078,35467,66900,42626,82686,92235,42626,49830,56320,99728,89644,42626,99728,89644,42626,67016,42626,35467,81691,76960,42626,61012,42626,56320,35467,73566,59078,42626,89644,59078,81691,70742,42626,11375,83667,26987,42626,35467,42626,81691,83667,81691,14074,59078,42626,75727,66318,14084,66318,96662,9907,42626,83667,81691,18776,11375,42626,11375,83667,26987,42626,14074,35467,81691,42626,66900,59078,35467,76960,27803,42626,52865,83667,26987,66900,89644,42626,89644,99728,81691,14074,59078,66900,59078,18776,11375,92235,42626,67016,27803]},{"text":"Dear S, This is B and I would like to get A-s public key. Yours sincerely, B.","encoded":[68,101,97,114,32,83,44,32,84,104,105,115,32,105,115,32,66,32,97,110,100,32,73,32,119,111,117,108,100,32,108,105,107,101,32,116,111,32,103,101,116,32,65,45,115,32,112,117,98,108,105,99,32,107,101,121,46,32,89,111,117,114,115,32,115,105,110,99,101,114,101,108,121,44,32,66,46]},{"text":"Dear B, Here is A-s public key [196091,246331] signed by me. Yours sincerely, S.","encoded":[68,101,97,114,32,66,44,32,72,101,114,101,32,105,115,32,65,45,115,32,112,117,98,108,105,99,32,107,101,121,32,91,49,57,54,48,57,49,44,50,52,54,51,51,49,93,32,115,105,103,110,101,100,32,98,121,32,109,101,46,32,89,111,117,114,115,32,115,105,110,99,101,114,101,108,121,44,32,83,46],"encrypted":[118729,40313,161154,53846,184591,230781,183659,184591,138538,40313,53846,40313,184591,151404,359645,184591,39926,346794,359645,184591,638,267401,228780,67179,151404,145992,184591,47308,40313,363125,184591,74612,312418,1042,18558,50072,1042,312418,183659,209108,341547,18558,130951,130951,312418,272757,184591,359645,151404,196392,69537,40313,47323,184591,228780,363125,184591,162611,40313,171648,184591,271083,330341,267401,53846,359645,184591,359645,151404,69537,145992,40313,53846,40313,67179,363125,183659,184591,246996,171648]},{"text":"Dear A, Here is my nonce [1989] and yours [1812], proving I decrypted it. Yours sincerely, B.","encoded":[68,101,97,114,32,65,44,32,72,101,114,101,32,105,115,32,109,121,32,110,111,110,99,101,32,91,49,57,56,57,93,32,97,110,100,32,121,111,117,114,115,32,91,49,56,49,50,93,44,32,112,114,111,118,105,110,103,32,73,32,100,101,99,114,121,112,116,101,100,32,105,116,46,32,89,111,117,114,115,32,115,105,110,99,101,114,101,108,121,44,32,66,46],"encrypted":[117085,188708,48899,135065,24013,196694,93836,24

```
013,139698,188708,135065,188708,24013,106578,124623,240
13,142303,186041,24013,111704,224593,111704,151707,1887
08,24013,6174,139087,17852,120287,17852,11443,24013,488
99,111704,120577,24013,186041,224593,233078,135065,1246
23,24013,6174,139087,120287,139087,209854,11443,93836,2
4013,167972,135065,224593,233246,106578,111704,127625,2
4013,182822,24013,120577,188708,151707,135065,186041,16
7972,43990,188708,120577,24013,106578,43990,119287,2401
3,162971,224593,233078,135065,124623,24013,124623,10657
8,111704,151707,188708,135065,188708,83742,186041,93836
,24013,3922,119287]},{"text":"Dear B, Here is your nonc
e [1989] proving I decrypted it. Yours sincerely, A.","
encoded":[68,101,97,114,32,66,44,32,72,101,114,101,32,1
05,115,32,121,111,117,114,32,110,111,110,99,101,32,91,4
9,57,56,57,93,32,112,114,111,118,105,110,103,32,73,32,1
00,101,99,114,121,112,116,101,100,32,105,116,46,32,89,1
11,117,114,115,32,115,105,110,99,101,114,101,108,121,44
,32,65,46],"encrypted":[27990,59078,35467,66900,42626,8
2686,92235,42626,12634,59078,66900,59078,42626,99728,89
644,42626,11375,83667,26987,66900,42626,81691,83667,816
91,14074,59078,42626,75727,66318,1226,14084,1226,9907,4
2626,29104,66900,83667,73566,99728,81691,54948,42626,61
012,42626,76960,59078,14074,66900,11375,29104,70742,590
78,76960,42626,99728,70742,27803,42626,52865,83667,2698
7,66900,89644,42626,89644,99728,81691,14074,59078,66900
,59078,18776,11375,92235,42626,67016,27803]}]}
```


Similar to the output of CW1, the first two lines are *your name* (in CamelCase) and *your SRN*. The following 3 lines are the outputs corresponding to the 3 input lines. To explain the output, we'll look at each input-output pairs in turn.

First example

This is the simplest input:

```
{  }
```

Nothing is given about Alice (**A**), Bob (**B**) and the trusted 3rd party (**S**), therefore *all* their key-pairs have to be generated by you. In addition, you also have to generate the **nonce** values for Alice and Bob.

Possible output

Outputs will vary depending on what *p*, *q* and *e* values you have generated for **A**, **B** and **S**, but the correct format of the output is the following:


```
{
    "A":{"rsa":{"p":109,"q":811,"e":33013,"n":88399,"r"
:87480,"d":32437},"nonce":756132204},
    "B":{"rsa":{"p":353,"q":1013,"e":324535,"n":357589,
"r":356224,"d":341127},"nonce":1048794305},
    "S":{"rsa":{"p":277,"q":643,"e":141295,"n":178111,"
r":177192,"d":157255}},
    "communication":[
        {
            "text":"Dear S, This is A and I would like
to get B-s public key. Yours sincerely, A.",
            "encoded":[68,101,97,114,32,83,44,32,84,104
,105,115,32,105,115,32,65,32,97,110,100,32,73,32,119,11
1,117,108,100,32,108,105,107,101,32,116,111,32,103,101,
116,32,66,45,115,32,112,117,98,108,105,99,32,107,101,12
1,46,32,89,111,117,114,115,32,115,105,110,99,101,114,10
1,108,121,44,32,65,46]
        }, {
            "text":"Dear A, Here is B-s public key [324
535,357589] signed by me. Yours sincerely, S.",
            "encoded":[68,101,97,114,32,65,44,32,72,101
,114,101,32,105,115,32,66,45,115,32,112,117,98,108,105,
99,32,107,101,121,32,91,51,50,52,53,51,53,44,51,53,55,5
3,56,57,93,32,115,105,103,110,101,100,32,98,121,32,109,
101,46,32,89,111,117,114,115,32,115,105,110,99,101,114,
101,108,121,44,32,83,46],
            "encrypted":[161763,139071,154994,53299,156
678,30367,118819,156678,7435,139071,53299,139071,156678
,167243,79198,156678,153222,114130,79198,156678,110653,
71583,68220,142586,167243,133295,156678,88739,139071,11
7787,156678,117181,56924,93519,58094,47794,56924,47794,
118819,56924,47794,58654,47794,138849,53823,74060,15667
8,79198,167243,41771,69139,139071,140946,156678,68220,1
17787,156678,112724,139071,150947,156678,101303,15636,7
1583,53299,79198,156678,79198,167243,69139,133295,13907
1,53299,139071,142586,117787,118819,156678,110058,15094
7]
        }, {
            "text":"Dear B, This is A and I have sent y
```

ou a nonce [756132204] only you can read. Yours sincere
ly, A.",
"encoded":[68,101,97,114,32,66,44,32,84,104
,105,115,32,105,115,32,65,32,97,110,100,32,73,32,104,97
,118,101,32,115,101,110,116,32,121,111,117,32,97,32,110
,111,110,99,101,32,91,55,53,54,49,51,50,50,48,52,93,32,
111,110,108,121,32,121,111,117,32,99,97,110,32,114,101,
97,100,46,32,89,111,117,114,115,32,115,105,110,99,101,1
14,101,108,121,44,32,65,46],
"encrypted":[94936,143730,225689,124426,264
573,50465,12993,264573,15958,27850,351072,26388,264573,
351072,26388,264573,279269,264573,225689,159830,49833,2
64573,275401,264573,27850,225689,291493,143730,264573,2
6388,143730,159830,325536,264573,207921,324145,14569,26
4573,225689,264573,159830,324145,159830,280113,143730,2
64573,237652,43566,178328,44893,44514,113778,262994,262
994,317051,95428,75341,264573,324145,159830,303758,2079
21,264573,207921,324145,14569,264573,280113,225689,1598
30,264573,124426,143730,225689,49833,350682,264573,2137
95,324145,14569,124426,26388,264573,26388,351072,159830
,280113,143730,124426,143730,303758,207921,12993,264573
,279269,350682]
}, {
"text":"Dear S, This is B and I would like
to get A-s public key. Yours sincerely, B.",
"encoded":[68,101,97,114,32,83,44,32,84,104
,105,115,32,105,115,32,66,32,97,110,100,32,73,32,119,11
1,117,108,100,32,108,105,107,101,32,116,111,32,103,101,
116,32,65,45,115,32,112,117,98,108,105,99,32,107,101,12
1,46,32,89,111,117,114,115,32,115,105,110,99,101,114,10
1,108,121,44,32,66,46]
}, {
"text":"Dear B, Here is A-s public key [330
13,88399] signed by me. Yours sincerely, S.",
"encoded":[68,101,97,114,32,66,44,32,72,101
,114,101,32,105,115,32,65,45,115,32,112,117,98,108,105,
99,32,107,101,121,32,91,51,51,48,49,51,44,56,56,51,57,5
7,93,32,115,105,103,110,101,100,32,98,121,32,109,101,46
,32,89,111,117,114,115,32,115,105,110,99,101,114,101,10
8,121,44,32,83,46],
"encrypted":[161763,139071,154994,53299,156
678,153222,118819,156678,7435,139071,53299,139071,15667
8,167243,79198,156678,30367,114130,79198,156678,110653,

71583,68220,142586,167243,133295,156678,88739,139071,117787,156678,117181,56924,56924,52341,63310,56924,118819,138849,138849,56924,53823,53823,74060,156678,79198,167243,41771,69139,139071,140946,156678,68220,117787,156678,112724,139071,150947,156678,101303,15636,71583,53299,79198,156678,79198,167243,69139,133295,139071,53299,139071,142586,117787,118819,156678,110058,150947]
        }, {
            "text":"Dear A, Here is my nonce [1048794305] and yours [756132204], proving I decrypted it. Yours sincerely, B.",
            "encoded":[68,101,97,114,32,65,44,32,72,101,114,101,32,105,115,32,109,121,32,110,111,110,99,101,32,91,49,48,52,56,55,57,52,51,48,53,93,32,97,110,100,32,121,111,117,114,115,32,91,55,53,54,49,51,50,50,48,52,93,44,32,112,114,111,118,105,110,103,32,73,32,100,101,99,114,121,112,116,101,100,32,105,116,46,32,89,111,117,114,115,32,115,105,110,99,101,114,101,108,121,44,32,66,46],
            "encrypted":[78984,81306,63225,32925,22813,28075,3426,22813,41487,81306,32925,81306,22813,44468,67741,22813,12208,70191,22813,40658,62132,40658,8815,81306,22813,87374,17911,65489,20434,69773,39731,28289,20434,69766,65489,30398,80099,22813,63225,40658,84126,22813,70191,62132,77398,32925,67741,22813,87374,39731,30398,54,17911,69766,29092,29092,65489,20434,80099,3426,22813,49512,32925,62132,25092,44468,40658,59135,22813,43076,22813,84126,81306,8815,32925,70191,49512,35086,81306,84126,22813,44468,35086,31329,22813,38776,62132,77398,32925,67741,22813,67741,44468,40658,8815,81306,32925,81306,85237,70191,3426,22813,56528,31329]
        }, {
            "text":"Dear B, Here is your nonce [1048794305] proving I decrypted it. Yours sincerely, A.",
            "encoded":[68,101,97,114,32,66,44,32,72,101,114,101,32,105,115,32,121,111,117,114,32,110,111,110,99,101,32,91,49,48,52,56,55,57,52,51,48,53,93,32,112,114,111,118,105,110,103,32,73,32,100,101,99,114,121,112,116,101,100,32,105,116,46,32,89,111,117,114,115,32,115,105,110,99,101,114,101,108,121,44,32,65,46],
            "encrypted":[94936,143730,225689,124426,264573,50465,12993,264573,35862,143730,124426,143730,264573,351072,26388,264573,207921,324145,14569,124426,264573,159830,324145,159830,280113,143730,264573,237652,44514

```
,317051,95428,180788,43566,132930,95428,113778,317051,1
78328,75341,264573,57768,124426,324145,291493,351072,15
9830,288269,264573,275401,264573,49833,143730,280113,12
4426,207921,57768,325536,143730,49833,264573,351072,325
536,350682,264573,213795,324145,14569,124426,26388,2645
73,26388,351072,159830,280113,143730,124426,143730,3037
58,207921,12993,264573,279269,350682]
        }
    ]
}
```

Important: the actual output will be a single line, but a pretty-print is used in this description so that you can better understand what is expected.

- There must be exactly 4 entries: the details of **A**, **B** and **S** (the RSA keys for all 3 parties and nonce values you generate for **A** and **B**) and the **communication** between them as specified by the protocol provided in the coursework description.
- The **communication** must be an array of 7 messages, which follow the description provided, with the only slight change that the *nonce* values and *keys* are detailed in square brackets, as shown in the example.
- Each message is either a *pair* of **text** and **encoded** (messages 1. and 4., as these are not encrypted according to the protocol) or a *triplet* of **text**, **encoded** and **encrypted** (messages 2., 3., 5., 6. and 7.).
- See the Help section further down, which may help you on how to encode a text (= transform a string to an array of integers).
- The encryption is a signature of the encoded text with the appropriate public key, as described in the protocol.
- The automatic tester will decrypt your encrypted text with the keys you provide and compare the output with your encoded text. It will then decode your encoded text and check whether the appropriate keys and nonces are present in the phrase. So make sure you test this before you submit your code.

Second example

A partially specified input:

```
{ "A" : { "rsa" : { "p" : 313, "q" : 787 }, "nonce" : 1
066 } }
```

Here only the RSA details and *nonce* of Alice (**A**) are provided, which have to be used. The details of Bob (**B**) as well as the trusted 3rd party (**S**) have to be generated by you.

Possible output

Outputs will vary depending on what *nonce* you generate for **B** and what *p*, *q* and *e* values you generate for **B** and **S**, but the correct format of the output is:


```
{
    "A":{"rsa":{"p":313,"q":787,"e":151819,"n":246331,"
r":245232,"d":58963},"nonce":1066},
    "B":{"rsa":{"p":349,"q":743,"e":146623,"n":259307,"
r":258216,"d":156367},"nonce":1884542388},
    "S":{"rsa":{"p":389,"q":661,"e":24881,"n":257129,"r
":256080,"d":43361}},
    "communication":[
        {
            "text":"Dear S, This is A and I would like
to get B-s public key. Yours sincerely, A.",
            "encoded":[68,101,97,114,32,83,44,32,84,104
,105,115,32,105,115,32,65,32,97,110,100,32,73,32,119,11
1,117,108,100,32,108,105,107,101,32,116,111,32,103,101,
116,32,66,45,115,32,112,117,98,108,105,99,32,107,101,12
1,46,32,89,111,117,114,115,32,115,105,110,99,101,114,10
1,108,121,44,32,65,46]
        }, {
            "text":"Dear A, Here is B-s public key [146
623,259307] signed by me. Yours sincerely, S.",
            "encoded":[68,101,97,114,32,65,44,32,72,101
,114,101,32,105,115,32,66,45,115,32,112,117,98,108,105,
99,32,107,101,121,32,91,49,52,54,54,50,51,44,50,53,57,5
1,48,55,93,32,115,105,103,110,101,100,32,98,121,32,109,
101,46,32,89,111,117,114,115,32,115,105,110,99,101,114,
101,108,121,44,32,83,46],
            "encrypted":[224497,34730,255646,71417,5612
3,247739,151719,56123,71364,34730,71417,34730,56123,382
46,208619,56123,46757,20926,208619,56123,203932,84339,8
8214,133126,38246,95618,56123,211357,34730,18142,56123,
99307,83313,19080,242154,242154,156349,46265,151719,156
349,101753,122729,46265,203887,251596,92673,56123,20861
9,38246,138226,76197,34730,116036,56123,88214,18142,561
23,95158,34730,104859,56123,70675,39027,84339,71417,208
619,56123,208619,38246,76197,95618,34730,71417,34730,13
```

```
3126,18142,151719,56123,179487,104859]
        }, {
            "text":"Dear B, This is A and I have sent y
ou a nonce [1066] only you can read. Yours sincerely, A
.",
            "encoded":[68,101,97,114,32,66,44,32,84,104
,105,115,32,105,115,32,65,32,97,110,100,32,73,32,104,97
,118,101,32,115,101,110,116,32,121,111,117,32,97,32,110
,111,110,99,101,32,91,49,48,54,54,93,32,111,110,108,121
,32,121,111,117,32,99,97,110,32,114,101,97,100,46,32,89
,111,117,114,115,32,115,105,110,99,101,114,101,108,121,
44,32,65,46],
            "encrypted":[48133,9385,232314,147475,15947
5,165738,247301,159475,70192,27996,161063,17711,159475,
161063,17711,159475,16999,159475,232314,103212,221095,1
59475,183394,159475,27996,232314,5794,9385,159475,17711
,9385,103212,247461,159475,15082,69210,247275,159475,23
2314,159475,103212,69210,103212,224649,9385,159475,1601
77,33478,111411,170523,170523,247356,159475,69210,10321
2,201484,15082,159475,15082,69210,247275,159475,224649,
232314,103212,159475,147475,9385,232314,221095,48544,15
9475,86522,69210,247275,147475,17711,159475,17711,16106
3,103212,224649,9385,147475,9385,201484,15082,247301,15
9475,16999,48544]
        }, {
            "text":"Dear S, This is B and I would like
to get A-s public key. Yours sincerely, B.",
            "encoded":[68,101,97,114,32,83,44,32,84,104
,105,115,32,105,115,32,66,32,97,110,100,32,73,32,119,11
1,117,108,100,32,108,105,107,101,32,116,111,32,103,101,
116,32,65,45,115,32,112,117,98,108,105,99,32,107,101,12
1,46,32,89,111,117,114,115,32,115,105,110,99,101,114,10
1,108,121,44,32,66,46]
        }, {
            "text":"Dear B, Here is A-s public key [151
819,246331] signed by me. Yours sincerely, S.",
            "encoded":[68,101,97,114,32,66,44,32,72,101
,114,101,32,105,115,32,65,45,115,32,112,117,98,108,105,
99,32,107,101,121,32,91,49,53,49,56,49,57,44,50,52,54,5
1,51,49,93,32,115,105,103,110,101,100,32,98,121,32,109,
101,46,32,89,111,117,114,115,32,115,105,110,99,101,114,
101,108,121,44,32,83,46],
            "encrypted":[224497,34730,255646,71417,5612
```

3,46757,151719,56123,71364,34730,71417,34730,56123,3824
6,208619,56123,247739,20926,208619,56123,203932,84339,8
8214,133126,38246,95618,56123,211357,34730,18142,56123,
99307,83313,101753,83313,84450,83313,122729,151719,1563
49,19080,242154,46265,46265,83313,92673,56123,208619,38
246,138226,76197,34730,116036,56123,88214,18142,56123,9
5158,34730,104859,56123,70675,39027,84339,71417,208619,
56123,208619,38246,76197,95618,34730,71417,34730,133126
,18142,151719,56123,179487,104859]
        }, {
            "text":"Dear A, Here is my nonce [188454238
8] and yours [1066], proving I decrypted it. Yours sinc
erely, B.",
            "encoded":[68,101,97,114,32,65,44,32,72,101
,114,101,32,105,115,32,109,121,32,110,111,110,99,101,32
,91,49,56,56,52,53,52,50,51,56,56,93,32,97,110,100,32,1
21,111,117,114,115,32,91,49,48,54,54,93,44,32,112,114,1
11,118,105,110,103,32,73,32,100,101,99,114,121,112,116,
101,100,32,105,116,46,32,89,111,117,114,115,32,115,105,
110,99,101,114,101,108,121,44,32,66,46],
            "encrypted":[90843,32273,24766,31335,150397
,86468,36588,150397,27699,32273,31335,32273,150397,1551
05,183725,150397,82612,139104,150397,171852,157712,1718
52,45484,32273,150397,108253,62339,197197,197197,21795,
165241,21795,221906,136905,197197,197197,159373,150397,
24766,171852,72824,150397,139104,157712,62319,31335,183
725,150397,108253,62339,86133,78196,78196,159373,36588,
150397,117641,31335,157712,63963,155105,171852,123748,1
50397,100109,150397,72824,32273,45484,31335,139104,1176
41,104921,32273,72824,150397,155105,104921,164526,15039
7,107893,157712,62319,31335,183725,150397,183725,155105
,171852,45484,32273,31335,32273,50845,139104,36588,1503
97,29037,164526]
        }, {
            "text":"Dear B, Here is your nonce [1884542
388] proving I decrypted it. Yours sincerely, A.",
            "encoded":[68,101,97,114,32,66,44,32,72,101
,114,101,32,105,115,32,121,111,117,114,32,110,111,110,9
9,101,32,91,49,56,56,52,53,52,50,51,56,56,93,32,112,114
,111,118,105,110,103,32,73,32,100,101,99,114,121,112,11
6,101,100,32,105,116,46,32,89,111,117,114,115,32,115,10
5,110,99,101,114,101,108,121,44,32,65,46],
            "encrypted":[48133,9385,232314,147475,15947

```
5,165738,247301,159475,205632,9385,147475,9385,159475,1
61063,17711,159475,15082,69210,247275,147475,159475,103
212,69210,103212,224649,9385,159475,160177,33478,190745
,190745,124640,164300,124640,133125,45215,190745,190745
,247356,159475,135008,147475,69210,5794,161063,103212,2
18884,159475,183394,159475,221095,9385,224649,147475,15
082,135008,247461,9385,221095,159475,161063,247461,4854
4,159475,86522,69210,247275,147475,17711,159475,17711,1
61063,103212,224649,9385,147475,9385,201484,15082,24730
1,159475,16999,48544]
        }
    ]
}
```

Important: the actual output will be a single line, but a pretty-print is used in this description so that you can better understand what is expected.

Third example

Fully specified input:

```
{
    "A" : {
        "rsa" : { "p" : 313, "q" : 787, "e" : 196091 },
        "nonce" : 1812
    },
    "B" : {
        "rsa" : { "p" : 157, "q" : 641, "e" : 29203 },
        "nonce" : 1989
    },
    "S" : { "rsa" : { "p" : 373, "q" : 977, "e" : 25884
5 } }
}
```

Here *all* the RSA details and *nonce* values of Alice (**A**), Bob (**B**) and the trusted 3rd party (**S**) are provided, which have to be used.

Output

The output is deterministic and will have to be exactly as shown here:

```
{
    "A":{"rsa":{"p":313,"q":787,"e":196091,"n":246331,"
```

```
r":245232,"d":52883},"nonce":1812},
    "B":{"rsa":{"p":157,"q":641,"e":29203,"n":100637,"r
":99840,"d":48667},"nonce":1989},
    "S":{"rsa":{"p":373,"q":977,"e":258845,"n":364421,"
r":363072,"d":74933}},
    "communication":[
        {
            "text":"Dear S, This is A and I would like
to get B-s public key. Yours sincerely, A.",
            "encoded":[68,101,97,114,32,83,44,32,84,104
,105,115,32,105,115,32,65,32,97,110,100,32,73,32,119,11
1,117,108,100,32,108,105,107,101,32,116,111,32,103,101,
116,32,66,45,115,32,112,117,98,108,105,99,32,107,101,12
1,46,32,89,111,117,114,115,32,115,105,110,99,101,114,10
1,108,121,44,32,65,46]
        }, {
            "text":"Dear A, Here is B-s public key [292
03,100637] signed by me. Yours sincerely, S.",
            "encoded":[68,101,97,114,32,65,44,32,72,101
,114,101,32,105,115,32,66,45,115,32,112,117,98,108,105,
99,32,107,101,121,32,91,50,57,50,48,51,44,49,48,48,54,5
1,55,93,32,115,105,103,110,101,100,32,98,121,32,109,101
,46,32,89,111,117,114,115,32,115,105,110,99,101,114,101
,108,121,44,32,83,46],
            "encrypted":[118729,40313,161154,53846,1845
91,39926,183659,184591,138538,40313,53846,40313,184591,
151404,359645,184591,230781,346794,359645,184591,638,26
7401,228780,67179,151404,145992,184591,47308,40313,3631
25,184591,74612,209108,1042,209108,50072,130951,183659,
312418,50072,50072,18558,130951,227987,272757,184591,35
9645,151404,196392,69537,40313,47323,184591,228780,3631
25,184591,162611,40313,171648,184591,271083,330341,2674
01,53846,359645,184591,359645,151404,69537,145992,40313
,53846,40313,67179,363125,183659,184591,246996,171648]
        }, {
            "text":"Dear B, This is A and I have sent y
ou a nonce [1812] only you can read. Yours sincerely, A
.",
            "encoded":[68,101,97,114,32,66,44,32,84,104
,105,115,32,105,115,32,65,32,97,110,100,32,73,32,104,97
,118,101,32,115,101,110,116,32,121,111,117,32,97,32,110
,111,110,99,101,32,91,49,56,49,50,93,32,111,110,108,121
,32,121,111,117,32,99,97,110,32,114,101,97,100,46,32,89
```

,111,117,114,115,32,115,105,110,99,101,114,101,108,121,44,32,65,46],"encrypted":[27990,59078,35467,66900,42626,82686,92235,42626,49830,56320,99728,89644,42626,99728,89644,42626,67016,42626,35467,81691,76960,42626,61012,42626,56320,35467,73566,59078,42626,89644,59078,81691,70742,42626,11375,83667,26987,42626,35467,42626,81691,83667,81691,14074,59078,42626,75727,66318,14084,66318,96662,9907,42626,83667,81691,18776,11375,42626,11375,83667,26987,42626,14074,35467,81691,42626,66900,59078,35467,76960,27803,42626,52865,83667,26987,66900,89644,42626,89644,99728,81691,14074,59078,66900,59078,18776,11375,92235,42626,67016,27803]
        }, {
            "text":"Dear S, This is B and I would like to get A-s public key. Yours sincerely, B.",
            "encoded":[68,101,97,114,32,83,44,32,84,104,105,115,32,105,115,32,66,32,97,110,100,32,73,32,119,111,117,108,100,32,108,105,107,101,32,116,111,32,103,101,116,32,65,45,115,32,112,117,98,108,105,99,32,107,101,121,46,32,89,111,117,114,115,32,115,105,110,99,101,114,101,108,121,44,32,66,46]
        }, {
            "text":"Dear B, Here is A-s public key [196091,246331] signed by me. Yours sincerely, S.",
            "encoded":[68,101,97,114,32,66,44,32,72,101,114,101,32,105,115,32,65,45,115,32,112,117,98,108,105,99,32,107,101,121,32,91,49,57,54,48,57,49,44,50,52,54,51,51,49,93,32,115,105,103,110,101,100,32,98,121,32,109,101,46,32,89,111,117,114,115,32,115,105,110,99,101,114,101,108,121,44,32,83,46],
            "encrypted":[118729,40313,161154,53846,184591,230781,183659,184591,138538,40313,53846,40313,184591,151404,359645,184591,39926,346794,359645,184591,638,267401,228780,67179,151404,145992,184591,47308,40313,363125,184591,74612,312418,1042,18558,50072,1042,312418,183659,209108,341547,18558,130951,130951,312418,272757,184591,359645,151404,196392,69537,40313,47323,184591,228780,363125,184591,162611,40313,171648,184591,271083,330341,267401,53846,359645,184591,359645,151404,69537,145992,40313,53846,40313,67179,363125,183659,184591,246996,171648]
        }, {
            "text":"Dear A, Here is my nonce [1989] and

```
yours [1812], proving I decrypted it. Yours sincerely,
B.",
            "encoded":[68,101,97,114,32,65,44,32,72,101
,114,101,32,105,115,32,109,121,32,110,111,110,99,101,32
,91,49,57,56,57,93,32,97,110,100,32,121,111,117,114,115
,32,91,49,56,49,50,93,44,32,112,114,111,118,105,110,103
,32,73,32,100,101,99,114,121,112,116,101,100,32,105,116
,46,32,89,111,117,114,115,32,115,105,110,99,101,114,101
,108,121,44,32,66,46],
            "encrypted":[117085,188708,48899,135065,240
13,196694,93836,24013,139698,188708,135065,188708,24013
,106578,124623,24013,142303,186041,24013,111704,224593,
111704,151707,188708,24013,6174,139087,17852,120287,178
52,11443,24013,48899,111704,120577,24013,186041,224593,
233078,135065,124623,24013,6174,139087,120287,139087,20
9854,11443,93836,24013,167972,135065,224593,233246,1065
78,111704,127625,24013,182822,24013,120577,188708,15170
7,135065,186041,167972,43990,188708,120577,24013,106578
,43990,119287,24013,162971,224593,233078,135065,124623,
24013,124623,106578,111704,151707,188708,135065,188708,
83742,186041,93836,24013,3922,119287]
        }, {
            "text":"Dear B, Here is your nonce [1989] p
roving I decrypted it. Yours sincerely, A.",
            "encoded":[68,101,97,114,32,66,44,32,72,101
,114,101,32,105,115,32,121,111,117,114,32,110,111,110,9
9,101,32,91,49,57,56,57,93,32,112,114,111,118,105,110,1
03,32,73,32,100,101,99,114,121,112,116,101,100,32,105,1
16,46,32,89,111,117,114,115,32,115,105,110,99,101,114,1
01,108,121,44,32,65,46],
            "encrypted":[27990,59078,35467,66900,42626,
82686,92235,42626,12634,59078,66900,59078,42626,99728,8
9644,42626,11375,83667,26987,66900,42626,81691,83667,81
691,14074,59078,42626,75727,66318,1226,14084,1226,9907,
42626,29104,66900,83667,73566,99728,81691,54948,42626,6
1012,42626,76960,59078,14074,66900,11375,29104,70742,59
078,76960,42626,99728,70742,27803,42626,52865,83667,269
87,66900,89644,42626,89644,99728,81691,14074,59078,6690
0,59078,18776,11375,92235,42626,67016,27803]
        }
    ]
}
```

Important: the actual output will be a single line, but a pretty-print is used in this description so that you can better understand what is expected.

Help

To *encode* plain texts (i.e. strings) to an array of integers that can be encrypted / decrypted, you may use the following functions (*Java 8*):

```
    public static int[] encode(String message) {
        ByteBuffer buffer = ByteBuffer.wrap(message.get
Bytes());
        return IntStream.generate(buffer::get).limit(bu
ffer.remaining()).toArray();
    }

    public static String decode(int[] message) {
        return Arrays.stream(message)
                .mapToObj(i -> (char) i)
                .reduce(new StringBuilder(), (sb, c) ->
sb.append(c), StringBuilder::append)
                .toString();
    }
```

These functions use the ASCII values of the characters that make up the string to convert between string and a list of integers.

Submission

Once you're happy with your code

- rebuild your project, following the instructions in the Build section,
- re-test your project, following the instructions in the Test section,
- double-check that the output in the required format,
- submit the `FamilyName_27644437_CO3326CW2-jar-with-dependencies.jar` JAR file, which will obviously have your family name, SRN and the coursework number; for example, if your family name is Zuckerberg, your SRN is 27644437, the file would be `Zuckerberg_27644437_CO3326CW2-jar-with-dependencies.jar` This file is located in your project's `target` folder.

Important

Only a JAR file, which uses the correct naming scheme and produces output in the described format will be looked at, and **only** if it passes the automatic tests. A ZIPed project folder or individual Java or Class files will **not** be looked at, and will be awarded a *0* mark. If you correctly follow the description above, the JAR file you submit will contain the source code that you worked on and will give the marker the opportunity to check it, once your byte code passes the automatic execution phase.

Last modified: Saturday, 5 March 2016, 8:53 AM