**UTPB-COSC-4380-Project3-4**

**Project 3**

**Project Goals:**

1. Improve understanding of coding in Java and/or Python as a method of accomplishing simple tasks and solving relatively simple problems.
2. Improve understanding of the DHE and RSA algorithms.
3. Provide students with potentially useful implementations of modern key exchange and encryption algorithms.

**Description:**

For Project 3, I am asking you to use the provided Java and/or Python as a basis to implement a library for performing a Diffie-Hellman key exchange and using RSA to encrypt/decrypt and cryptographically sign messages. The provided Java code contains JavaDoc comments which specify all of the expected methods, their parameters and return values. Note that one of the methods in the Crypto class is not fully implemented yet. To complete the project, you will need to fill in the implementations of the methods marked with TODO comments. When grading your code, I will execute a set of tests against it more-or-less identical to the placeholder testing code I have provided in the main() methods in the DHE and RSA classes.

**Grading Criteria:**

1. If the final code uploaded to your repo does not compile, the grade is zero.
2. If the code crashes due to forseeable unhandled exceptions, the grade is zero.
3. For full points, the code should implement the algorithms and interfaces as described, and all interfaces should be easy to use and not unnecessarily complicated.

**Deliverables:**

For Project 3, a program written in either Java or Python which implements the requirements as specified, along with some documentation of the process involved in writing the code and any resources referenced.

**Project 4**

**Project Goals:**

1. Improve understanding of coding in Java and/or Python as a method of accomplishing simple tasks and solving relatively simple problems.
2. Improve understanding the AES algorithm and block ciphers.
3. Provide students with a potentially useful implementation of a block cipher encryption algorithm.

**Description:**

For Project 4, I am asking you to use either the provided Java code or the provided Python code, and write a complete implementation of the AES algorithm in both ECB mode and CBC mode. The interface should expose an encrypt() method which accepts a String of plaintext, a key String, and a mode boolean, and returns a String of ciphertext. It should likewise expose a decrypt() method which accepts a String of ciphertext, a key String, and a mode boolean and returns a String of plaintext. The code should be implemented such that there exists a debug flag which, when set to true, outputs the state of each block of the cipher following each step of the algorithm. When grading your code, I will use this debug output to compare to a similar output I generate. For testing purposes, I have provided a sample debug output file (AES Debug.txt). The SubBytes, MixColumns, and ShiftRows operations output the full 4x4 block (in hex) both input and output for each step (meaning that the output of step n and the input of step n+1 should be identical in all cases. The AddRoundKey step has two inputs, so the 4x4 block of the current key bytes is also printed between the input and output blocks. The plaintext, key, key schedule, and ciphertext are all included in the output.

**Grading Criteria:**

1. If the final code uploaded to your repo does not compile, the grade is zero.
2. If the code crashes due to forseeable unhandled exceptions, the grade is zero.
3. For full points, the code should implement the algorithms and interfaces as described, and all interfaces should be easy to use and not unnecessarily complicated.

**Deliverables:**

For Project 4, a program written in either Java or Python which implements the requirements as specified, along with some documentation of the process involved in writing the code and any resources referenced.