COMP8760 (2021-22)

A1: Programming Assignment

Sanjay Bhattacherjee

Submission deadline: 23:59 hrs on Monday, 22^{nd} November, 2021 (KV Week 17) .

Extension: If you face extenuating circumstances and would like to request for an extension, please write to Dr Kemi Ademoye <k.ademoye@kent.ac.uk>. In case you get an extension, your deadline for submission will be **23:59 hrs on Monday, 29^{th} November, 2021 (KV Week 18)**.

What do you submit? You will have to submit **one zip file** following the specified convention below.

- Your zip file should be named as: <your ID>.zip. For example, if your ID is ab123@kent.ac.uk, the name of your file should be "ab123.zip".
- Your zip file should contain six files - each corresponding to one task. These files should each be named after the respective task. For example, if you have written the programs in python and taken screenshots as jpeg images, then your files should be named as:

  "ab123_task1.py",
  "ab123_task2.py",
  "ab123_task3A.jpg",
  "ab123_task3B.jpg",
  "ab123_task4A.py" and
  "ab123_task4B.py".

Where to submit? Using the link on Moodle.

General Instructions:

- You have to complete four tasks as described in this sheet. Tasks 1, 2 and 4 are programming tasks. Each program should be written in a single separate file as described above, so that it can be directly executed using command-line arguments. You may use C/C++, Java or Python (>=3.0) to do these tasks.
- Each program should provide an input-output interface in the precise format as detailed under **Sample I/O** respectively. If you do not follow the format, marks may be deducted. The blanks denoted as _____ in the **Sample I/O** will be substituted with actual values while running the program.
- You should not use pre-written programming libraries other than those for standard input-output or generating (pseudo-)random numbers.
- Your program should work with $\nu \approx 20$. In other words, your program will not be tested for non-standard integer sizes ($\geq$ 32 bits). That said, if you feel adventurous, please visit the GNU Multiple Precision Arithmetic Library for more details.

Marking criteria: The total marks for this assessment has been distributed among the four tasks. The mark allotment for each task has been indicated at the beginning of the task description. You will be marked based on the following criteria.

- Syntactical correctness: If your code encounters compilation / interpreter errors you will be marked with zero for that task.
- Functional correctness: If your code works correctly for all input values it is tested with, you will qualify to get 0.8 fraction of the mark allotted to that task. Correctness will be judged based on your adherence with the **Sample I/O** format specified above as well as the correctness of the computations done by the program. You will receive partial marks if you have not met all the requirements of the task.
- Code quality: To qualify for full marks in a task, your code has to be well commented and its functionality explained.

Task 1: "Naive" RSA encryption system implementation. Marks: 30%
The program will take as input the security parameter ν. It will then generate the two ν/2-bit primes, and the integers N, e and d. It will then prompt the user to choose one of the two options - encryption and decryption. If the user chooses encryption, the program will prompt the user to enter an element from the plaintext space $\mathbb{Z}/N\mathbb{Z}$ and provide its encryption. If the user chooses decryption, the program will prompt the user to enter an element from the ciphertext space $\mathbb{Z}/N\mathbb{Z}$ and provide its decryption.
Sample I/O:

```
Please enter the security parameter 'nu':  _____
----------------------
Setup:
The first prime generated by the Setup algorithm is p = _____
The second prime generated by the Setup algorithm is q = _____
The integer N = pq = _____
The encryption exponent is e = _____
The decryption exponent is d = _____
----------------------
Please enter an option:
1 to Encrypt
2 to Decrypt
Any other number to quit
Your option:  _____
----------------------
Encryption:
Your message space is the set {Z/NZ} = {0, 1, ..., _____}
Please enter a number from this set:  _____
The ciphertext for your message _____ is _____
----------------------
Please enter an option:
1 to Encrypt
2 to Decrypt
Any other number to quit
Your option:  _____
----------------------
Decryption:
Your ciphertext space is the set {Z/NZ} = {0, 1, ..., _____}
Please enter a number from this set:  _____
The plaintext for your ciphertext _____ is _____
----------------------
```

Task 2: Goldwasser-Micali encryption system implementation. Marks: 30%
The program will take as input the security parameter ν. It will then generate the two ν/2-bit primes, and the integers N and y. It will then prompt the user to choose one of the two options - encryption and decryption. If the user chooses encryption, the program will then prompt the user to enter an element from the set $\{0, 1\}$ and provide its encryption. If the user chooses decryption, the program will then prompt the user to enter an element from the set $\mathbb{J}_N$ and provide its decryption.
Sample I/O:

```
Please enter the security parameter 'nu':  _____
----------------------
Setup:
The first prime generated by the Setup algorithm is p = _____
The second prime generated by the Setup algorithm is q = _____
The integer N = pq = _____
The public key y = _____
----------------------
Please enter an option:
1 to Encrypt
2 to Decrypt
Any other number to quit
Your option:  _____
----------------------
Encryption:
Your message space is the set:  {0, 1}
Please enter a number from this set:  _____
The ciphertext for your message _____ is _____
----------------------
Please enter an option:
1 to Encrypt
2 to Decrypt
Any other number to quit
Your option:  _____
----------------------
Decryption:
Your ciphertext space is the set J_N
Please enter a number from this set:  _____
The plaintext for your ciphertext _____ is _____
----------------------
```

Task 3: IND-CPA security. You will have to submit **one image file for each of the following tasks**. The image file should contain the screenshot of appropriate executions of the programs you have written for Tasks 1 and 2 as appropriate.

We recollect that if an encryption scheme encrypts a plaintext message to the same ciphertext every time, it is insecure against an IND-CPA adversary.

(A) **Marks: 10%**
Using the program you have written for Task 1, provide an example input-output demonstrating the insecurity of "Naive" RSA with respect to an IND-CPA adversary.

(B) **Marks: 10%**
Using the program you have written for Task 2, provide an example input-output demonstrating the security of the Goldwasser-Micali encryption scheme with respect to an IND-CPA adversary (at least in the above sense).

Task 4: IND-CCA security. In each of the tasks below, you will have to demonstrate that the the decryption of a ciphertext and its "related but modified" form can lead us to the same plaintext.

(A) **Marks: 10%**
Write a program to demonstrate that "Naive RSA" is insecure with respect to an IND-CCA adversary. The program will take as input a public key (N, e) and a ciphertext c created by the program written for Task 1. It will then output the modified ciphertext $c' = 2^e \cdot c \pmod{N}$. It will then output the element $2^{-1} \pmod{N}$. It will take as input the message m' found by decrypting c' using the program written for Task 1. It will finally output the original message m that was encrypted to c.
Sample I/O:

```
Please enter the public parameter N:  _____
Please enter the encryption exponent e:  _____
----------------------
Please enter the ciphertext c:  _____
----------------------
The modified ciphertext c' is = _____
The inverse of 2 mod _____ is = _____
----------------------
Please decrypt the modified ciphertext c' using your program from Task 1.
Please input the plaintext m' decrypted from c':  _____
The original plaintext message m computed from m' is:  _____
----------------------
```

(B) **Marks: 10%**
Write a program to demonstrate that Goldwasser-Micali encryption scheme is insecure with respect to an IND-CCA adversary. The program will take as input a public key (N, y) and a ciphertext c created by the program written for Task 2. It will then output the modified ciphertext $c' = c \cdot z^2 \pmod{N}$ for a random $z \in (\mathbb{Z}/N\mathbb{Z})^*$. This modified ciphertext $c' = c \cdot z^2 \pmod{N}$ can be decrypted using the program you have written for Task 2 to check if the decryption is correct.
Sample I/O:

```
Please enter the public parameter N:  _____
Please enter the encryption key y:  _____
----------------------
Please enter the ciphertext c:  _____
----------------------
The modified ciphertext c' is = _____
----------------------
```

Released on: Wednesday, 6^{th} October, 2021 (KV Week 10)
Queries to: Sanjay Bhattacherjee (s.bhattacherjee@kent.ac.uk)