

There are 1 questions for a total of 10 points.

In the lecture on modern cryptography, we mentioned how secure communication happens between your browser and sites such as amazon.ae. The key concept is *Public Key Cryptography* which is the foundational concept on which many of the cryptographic protocols used in practice are based. Some of the tasks in this assignment will be graded while others will not be graded, but you will be encouraged to complete them to be able to appreciate the topic better.

Task 1 (not graded): Please read the short writeup on Public Key Cryptography (<https://www.cse.iitd.ac.in/~rjaiswal/Teaching/2025/AGRL112/Homework/Week-02/PKC.pdf>) that I wrote some time back (written as a background material for the *blockchain* technology) to understand how secure communication happen between browser and a secure website such as amazon.ae.

Task 2 (not graded): You can generate your own public-private key pair using `openssl` library (*a widely used software library for secure communication over internet*). Please see https://wiki.openssl.org/index.php/Command_Line_Uutilities for some command-line tools documentation. You should at least try the following commands to generate public-private keys and then use them to encrypt and decrypt.

```
openssl genrsa -out private_key.pem 2048
openssl rsa -in private_key.pem -pubout -out public_key.pem
openssl pkeyutl -encrypt -pubin -inkey public_key.pem -in input.txt -out encrypted.enc
openssl pkeyutl -decrypt -inkey private_key.pem -in encrypted.enc -out decrypted.txt
```

Knowing the command line tools for `openssl` should enable you to have secure communications with each other! I'll encourage everyone to learn to use these tools for secure communication.

For the graded component, you will be asked to break a *substitution cipher*. A substitution cipher is typically the first cipher that we try as kids for secret communication. Here, we substitute one alphabet for another so that the text looks gibberish.

1. (10 points) (*Breaking a substitution cipher*) A substitution cipher has been used to encrypt a portion of a popular book available freely on the internet. Each one will receive a different substitution cipher of a distinct portion of this book. You will have to do *frequency analysis* (https://en.wikipedia.org/wiki/Frequency_analysis) to figure out which book and which portion of the book was assigned to you. You will be asked to submit the first paragraph of the portion assigned to you on gradescope. All the codes can be found in the zip file (<https://www.cse.iitd.ac.in/~rjaiswal/Teaching/2025/AGRL112/Homework/Week-02/Codes.zip>), and the assignment of student to the code is given in the table below:

Student	Code
ABHIRAMACHANDRA VEMPARALA	cipher1.txt
ADITYA MURUGESH	cipher10.txt
ADITYA MOHAN	cipher12.txt
AHAD ABDULLAH ALGHAMRI	cipher3.txt
AYACHI PADMANABH MISHRA	cipher5.txt
CHAUDHARY PARVA TEJAS	cipher13.txt
EHSAN MOHAMED K	cipher22.txt
EVAN JOHAN TOBIAS	cipher16.txt
FARHAN FAIZY	cipher11.txt
HAMAD MOHAMMED ALALBI	cipher17.txt
HIMANSHU NAYAN RATHI	cipher6.txt
JAMES JOSHUA KOSHY	cipher14.txt
JOEL JOBI	cipher19.txt
KANNAPU SUJEETH KEVIN	cipher4.txt
KARTHIK NAMBIAR PUTHIYEDATHU VELLUVA	cipher8.txt
LATIFA TARIQ ALMARZOOQI	cipher23.txt
PAUL TIJU	cipher9.txt
RAWAAN YOUSOF ALHAMMADI	cipher21.txt
SAKET SHARMA	cipher15.txt
SYEDA ESHAL ILHAN DAIMI	cipher24.txt
TANVI PARSAM	cipher2.txt
VARANASI SUMANT	cipher7.txt
VIPULAV BATRA	cipher20.txt
KRISHNA CHANDRA SINGH	cipher18.txt