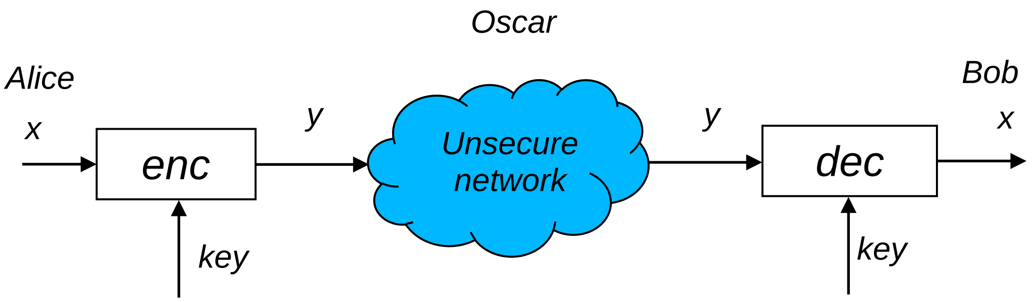
Software Optimization

(40 points)

Project and Report

Task .1 (10 points):

Your job is to write a program to achieve encryption and decryption using the ***Monoalphabetic Substitution Cipher system***. The key can be generated randomly by Alice and sent to Bob securely. The task must:



1- Alice will send the following text:

I remember as a child, and as a young budding naturalist, spending all my time observing and testing the world around me moving pieces, altering the flow of things, and documenting ways the world responded to me. Now, as an adult and a professional naturalist, I’ve approached language in the same way, not from an academic point of view but as a curious child still building little mud dams in creeks and chasing after frogs. So this book is an odd thing: it is a naturalist’s walk through the language-making landscape of the English language, and following in the naturalist’s tradition it combines observation, experimentation, speculation, and documentation activities we don’t normally associate with language.

This book is about testing, experimenting, and playing with language. It is a handbook of tools and techniques for taking words apart and putting them back together again in ways that I hope are meaningful and legitimate (or even illegitimate). This book is about peeling back layers in search of the language-making energy of the human spirit. It is about the gaps in meaning that we urgently need to notice and name the places where our dreams and ideals are no longer fulfilled by a society that has become fast-paced and hyper-commercialized.

Language is meant to be a playful, ever-shifting creation but we have been taught, and most of us continue to believe, that language must obediently follow precisely prescribed rules that govern clear sentence structures, specific word orders, correct spellings, and proper pronunciations. If you make a mistake or step out of bounds there are countless, self-appointed language experts who will promptly push you back into safe terrain and scold you for your errors. And in case you need reminding, there are hundreds of dictionaries and grammar books to ensure that you remember the "right" way to use English.

1. Bob will receive the ciphered text and be able to read it.
2. Meanwhile, Oscar will attempt to hack the ciphered text and read the message without knowing the key. "Find the best way to perform the hacking and implement it."
3. Alice will send a message in another language, such as "Select your mother language" or "German language," and repeat steps 2 and 3.

Task .2 (10 points):

- Repeat Task 1 with Polyalphabetic Substitution Cipher.
- Can Oscar break the ciphering, and how long does it take

Task .3 (20 points):

1- Repeat Task 1 (Points 1 and 2) using DES ciphering. You have to implement all the steps of DES.

2- Repeat Task 1 (Points 1 and 2) by sending a bitmap image. Show the image before encryption, after encryption, and after decryption.

Homework submission requirements

1- The homework is individual work, so do not share your work with friends. Any copying will be considered as cheating, and both parties will receive a zero.

2- Use only Python version 3.0 or Java version 8.0 or above as the programming language; no other programming languages are allowed.

3- Write all steps in a report. Your report must include the solution, screenshots, and results. Include a report cover page.

4- Submit the homework in the Microsoft Teams assignment section. Submissions via email will not be considered.

5- Homework without a report will not be accepted.

6- Submit all the codes and implemnatation test files and results, and user guide in the MsTeam assignment section along with report in one zip file.

7- The submission deadline is non-negotiable. Please be aware that you will not be able to submit after the deadline.

8- If you miss the deadline, you will receive a zero, and you may fail the course. Partial submissions of the homework are also accepted.*Dead line is 20 of May, at 11:00 PM*

9- *Please submit all the files, your code, and the report as pdf as one zip file. Name you zip file as*:

FirstName_lastName_SOHW.zip

Good Luck

Prof. Dr. Rand Kouatly