

Cryptography

Design Problem 4

if nothing else, write `#cleancode`

Agenda

- Problem Background
- Learning Objectives
- Coding



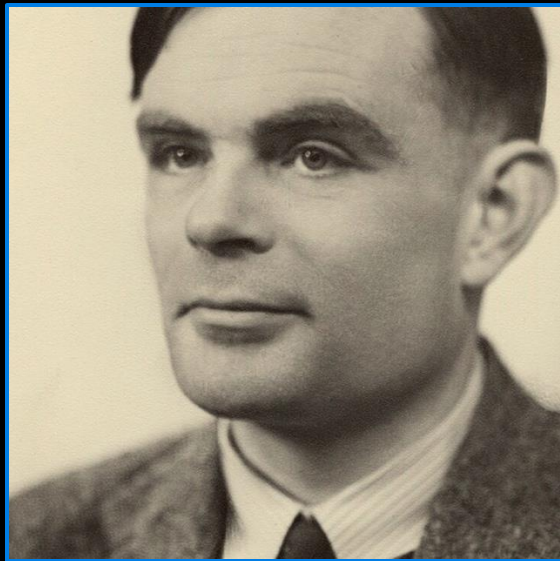
Cryptography is the study of how to communicate **securely**, especially when there are potential adversaries.

Cryptanalysis was a defining factor in **WWII**.

History + Technology

- **Alan Turing**

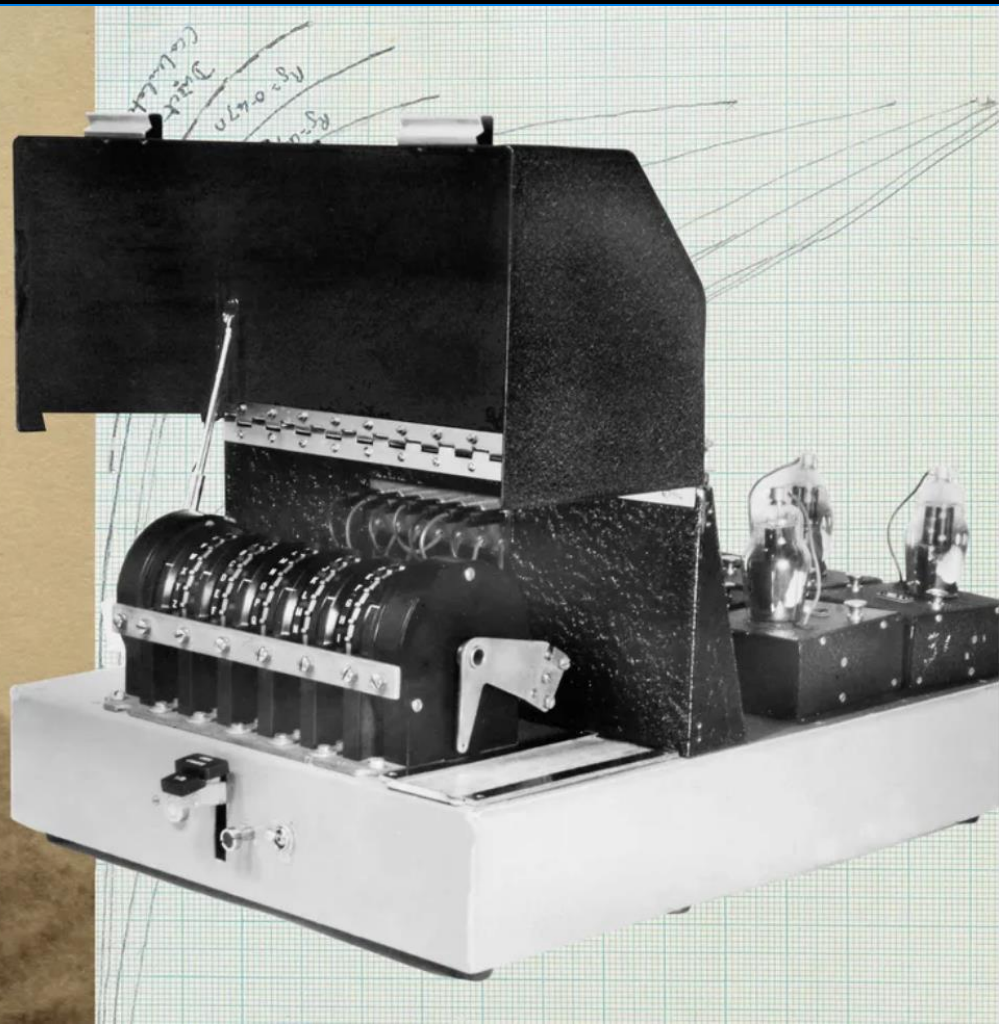
- Pioneered the technology to decrypt Nazi Germany's secret communications during World War II.
- These were called "Turing machines".



Alan Turing circa 1951

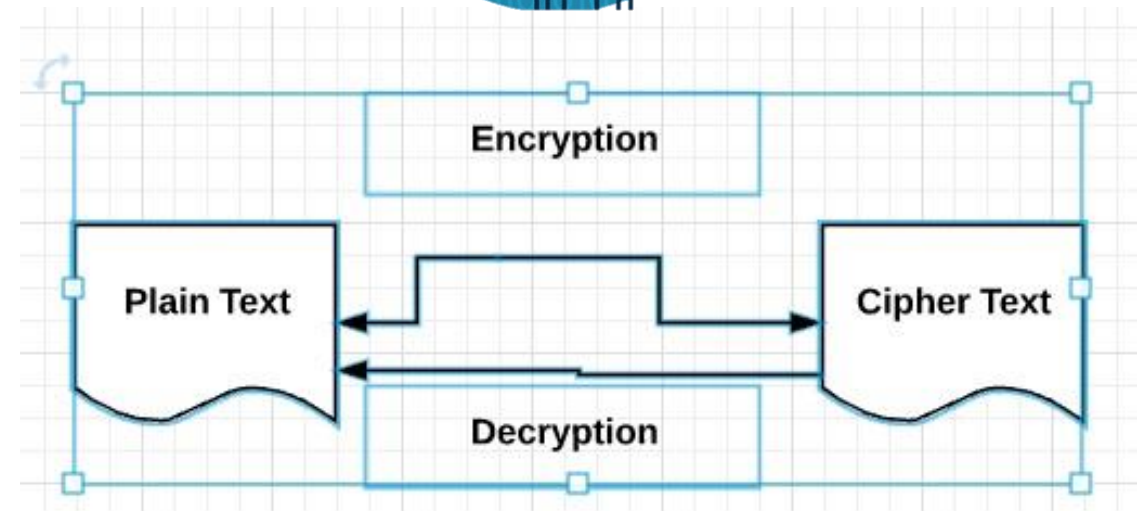


Workers of Bletchley Park circa 1938



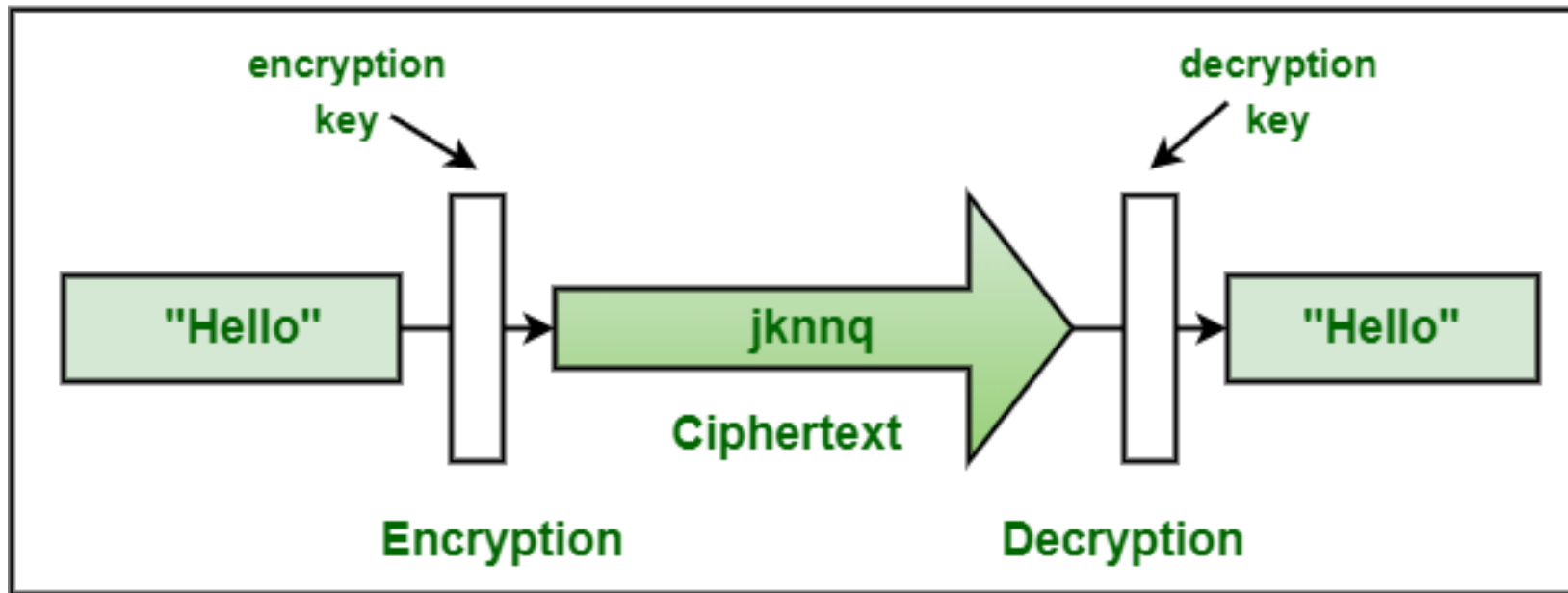
Background

- Will rely on user input, functions, for loops, conditional statements, ASCII codes, string methods, and comparison operators to create our own cryptography code!
- **Goal:** Write a Python program that enables us to encrypt a message that can only be read by someone with the secret key. 🔑



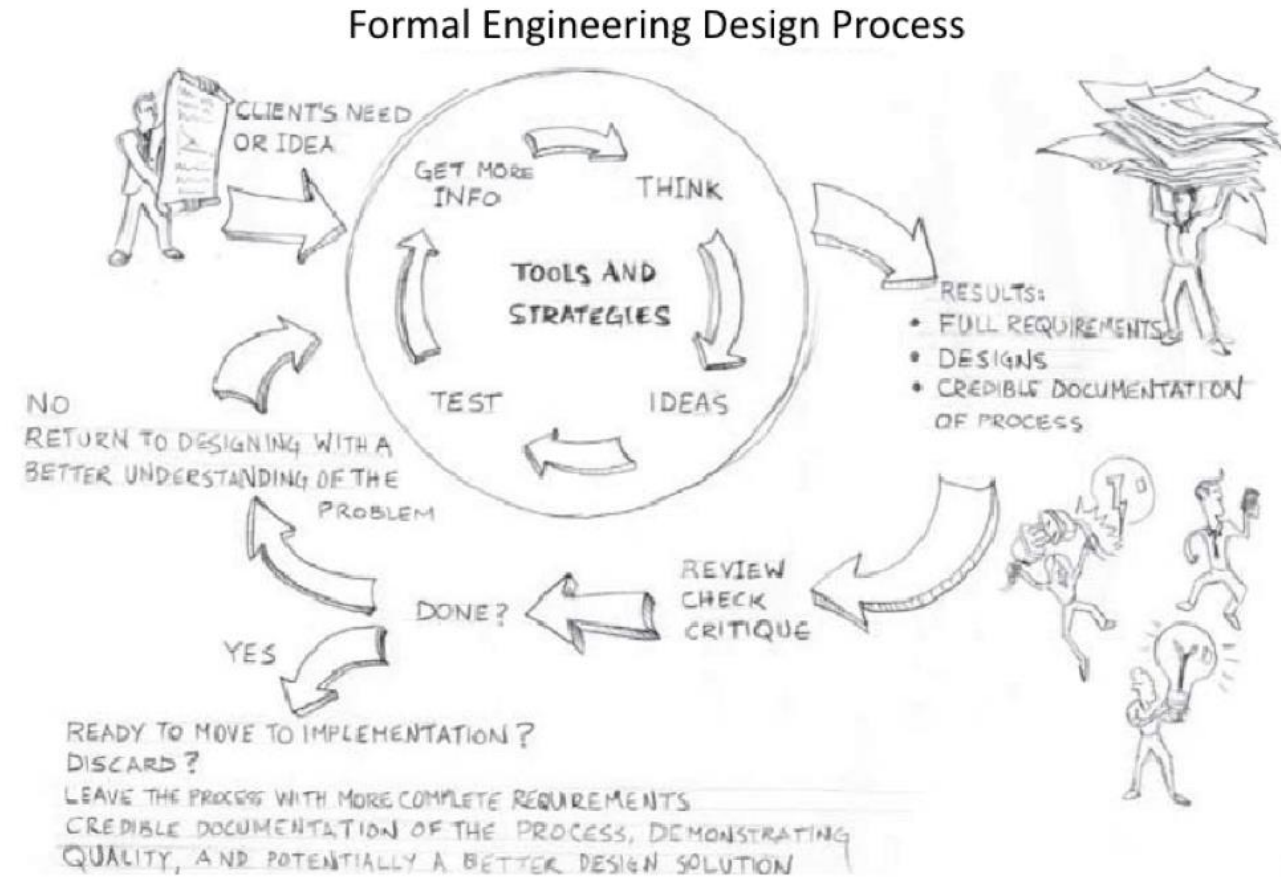
Learning Objective

- Practice combining all topics covered so far with an out-of-box application.



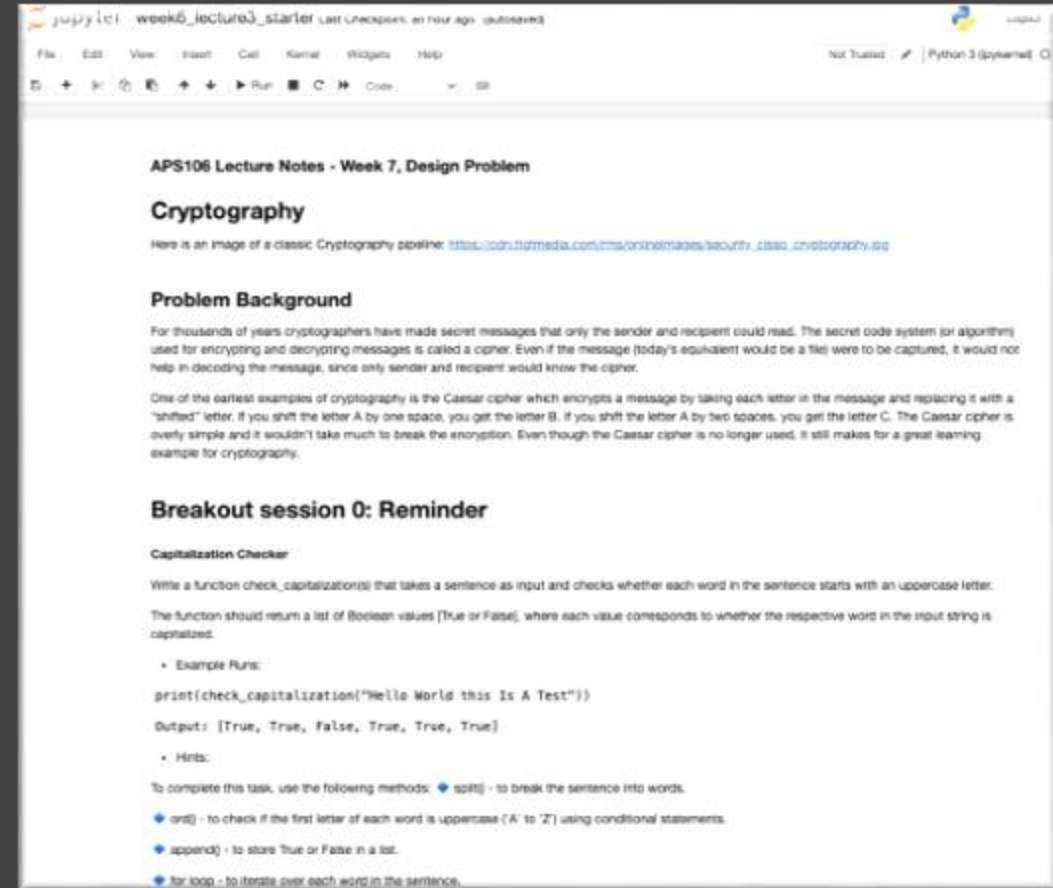
Engineering Design Process

- Define the problem properly.
- Define test cases.
- Develop an algorithm plan (i.e., a workflow!).
- Program the solution and debugging.



Cryptography

Design Problem 4



APS106 Lecture Notes - Week 7, Design Problem

Cryptography

Here is an image of a classic Cryptography pipeline: https://cdn.ffmpeg.com/tms/onlineimages/security_class_cryptography.jpg

Problem Background

For thousands of years cryptographers have made secret messages that only the sender and recipient could read. The secret code system (or algorithm) used for encrypting and decrypting messages is called a cipher. Even if the message (today's equivalent would be a file) were to be captured, it would not help in decoding the message, since only sender and recipient would know the cipher.

One of the earliest examples of cryptography is the Caesar cipher which encrypts a message by taking each letter in the message and replacing it with a "shifted" letter. If you shift the letter A by one space, you get the letter B. If you shift the letter A by two spaces, you get the letter C. The Caesar cipher is overly simple and it wouldn't take much to break the encryption. Even though the Caesar cipher is no longer used, it still makes for a great learning example for cryptography.

Breakout session 0: Reminder

Capitalization Checker

Write a function `check_capitalization(s)` that takes a sentence as input and checks whether each word in the sentence starts with an uppercase letter. The function should return a list of Boolean values [True or False], where each value corresponds to whether the respective word in the input string is capitalized.

- Example Run:

```
print(check_capitalization("Hello World this Is A Test"))
```

Output: [True, True, False, True, True, True]

- Hints:

To complete this task, use the following methods:

- `split()` - to break the sentence into words.
- `ord()` - to check if the first letter of each word is uppercase ('A' to 'Z') using conditional statements.
- `append()` - to store True or False in a list.
- `for loop` - to iterate over each word in the sentence.

if nothing else, write `#cleancode`