Final Draft

Group Name: Team B-

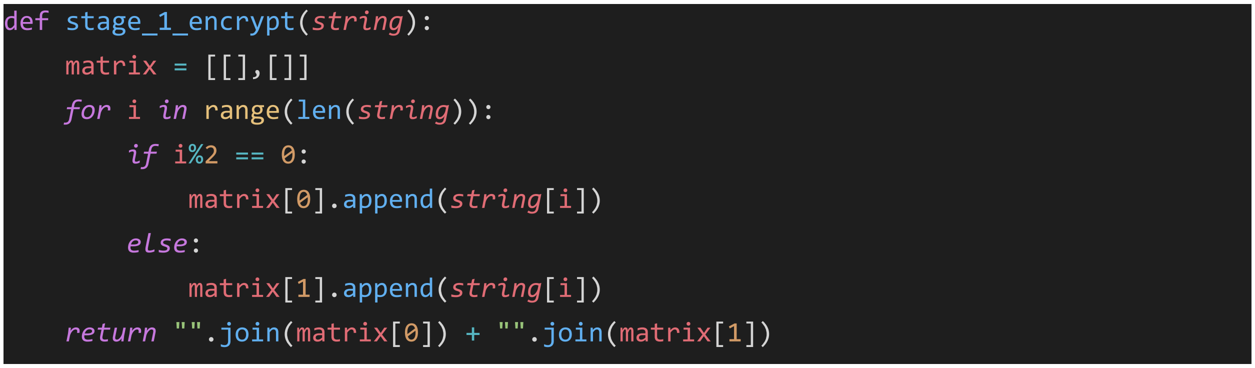
Group Members: Toh Hong Jing (1006056), Dylan Toh (1006371), Sarang Nirwan(1006403), Dhruv (1006585), Azad (1005948)

Stage 1

Decrypt the following hyperlink: hts/cf1wrpescmtp:/t5.odrs.o

Hint: The link above is encrypted using the very simple Rail-Fence Technique

Hint 2: The following algorithm is used for encrypting



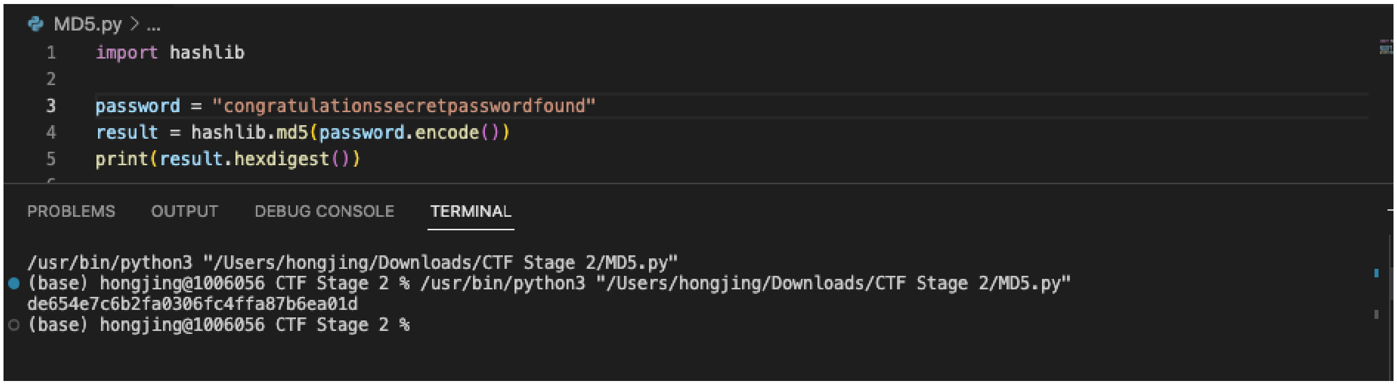
```
def stage_1_encrypt(string):
    matrix = [[],[]]
    for i in range(len(string)):
        if i%2 == 0:
            matrix[0].append(string[i])
        else:
            matrix[1].append(string[i])
    return "".join(matrix[0]) + "".join(matrix[1])
```

Stage 2

Travel to the hyperlink and use the hints provided in the WordPress document to concatenate a password together.

The first question requires participants to decrypt a Caesar Cipher with ciphertext “pbatenghyngvbaf” which results in the plaintext **“congratulations”** with key = 13.
The second question is “What term in steganography refers to the data or message that is hidden within the carrier? Hint: It is also used in cryptography to describe information or processes that are supposed to remain undisclosed or unknown and it starts with a letter ‘s’.”
Answer: **secret**
The third question involves reading the blog post titled “The Unsung Hero of Cryptography – The “P” Word” and guessing the answer, which is **“password”**.
The last question involves reading the blog post titled “Unraveling Cryptographic Mysteries: A Treasure Found!” and guessing the answer, which is **“found”**.

Their next task is to hash this password using MD5. With the MD5 hash in hand, participants are then required to verify their answer by comparing their hash with the one provided in the blog as part of the challenge. If the hash matches, they've successfully cracked the password and are able to unlock the password protected image.



```python
import hashlib

password = "congratulationssecretpasswordfound"
result = hashlib.md5(password.encode())
print(result.hexdigest())
```

```
/usr/bin/python3 "/Users/hongjing/Downloads/CTF Stage 2/MD5.py"
● (base) hongjing@1006056 CTF Stage 2 % /usr/bin/python3 "/Users/hongjing/Downloads/CTF Stage 2/MD5.py"
de654e7c6b2fa0306fc4ffa87b6ea01d
○ (base) hongjing@1006056 CTF Stage 2 %
```

The expected password is "congratulationssecretpasswordfound".
The expected hash digest is de654e7c6b2fa0306fc4ffa87b6ea01d.

Hint: Read the blogs in a chronological order and concatenate your answers together to form the password (no caps, no space).

Stage 3

Use the password from stage 2 to unlock the image provided in the WordPress document. The image uses steganography to hide the final flag. There will be a message hidden using the pixel of the image which are the RGB values. The goal of this method is to incorporate the secret message while bearing in mind not to change the RGB values so much that it distorts the original picture. The participants are to find the hidden message in the pixels of the image. To do so, the participants are to load the encoded image and read the pixels of the image. For each pixel, it represents 3 bits which are the RGB values, if each RGB value is an even number, it means that the bit is 0 else 1. For example, in one pixel the RGB value is (1, 2, 3) it means that the 3 bit value is "101". These extracted bits will be the binary representation of the hidden message. If the participants are able to extract and convert the binary bits, they will obtain the hidden message successfully.

Hint:

1. Read the RGB values in each pixel of the encoded image, convert them into binary, then integer (ASCII numbers) then translate them into readable words.
2. "H" in binary is 01001000, this requires 3 pixels to hide the message in.
   a. Pixel 1: (141, 90, 236) → (142, 91, 236)
   b. Pixel 2: (37, 66, 217) → (38, 67, 218)
   c. Pixel 3: (12, 6, 43) → (12, 6, 44)

Final flag

fcs23{dylanhongjingsarangazaddhruv}