HW1 - Solve Two Crypto Challenges in a CTF

CNS Course Sapienza

Sultan Umarbaev, Matricola: 1954544

20/10/2020

1 CTF introduction and summary

CTF name: Hacktober CTF
CTF URL: `http://ctf.cyberhacktics.com/`
CTF URL on CTFTime.org: `https://ctftime.org/event/1108/`
CTF time: Fri, 16 Oct. 2020, 14:00 UTC — Sun, 18 Oct. 2020, 02:00 UTC

Hacktober CTF is developed by industry professionals and military veterans, including members from organizations such as **Cyber Hacktics** and **CyberUp**. It has been an annual event since 2016, starting out as a local competition in October in the St. Louis area. In 2018, Hacktober CTF became a nation-wide event and this year, it is open to a global audience. It was hosted Hacktober CTF in support of *National Cyber Security Awareness Month* [1].

2 Challenges

Hacktober CTF included wide variety of challenge categories with different level of complexity for broad audience, from beginners to professional experts [1]:

- Steganography
- Programming
- Linux
- Forensics
- Cryptography
- Web Exploitation
- SQL
- OSINT
- Traffic Analysis

From which the main focus of the work was the category of **Cryptography**.

2.1 Cryptography: Hail Caesar! (10 points)

Flag format:

```
flag{...}
```

Description of the challenge is the following:

> This image was found in Ghost Town along with the encoded message below. See if you can decipher the message. Enter the entire decoded message as the flag.
> Decode this: **TGG KUSJWV QGM**

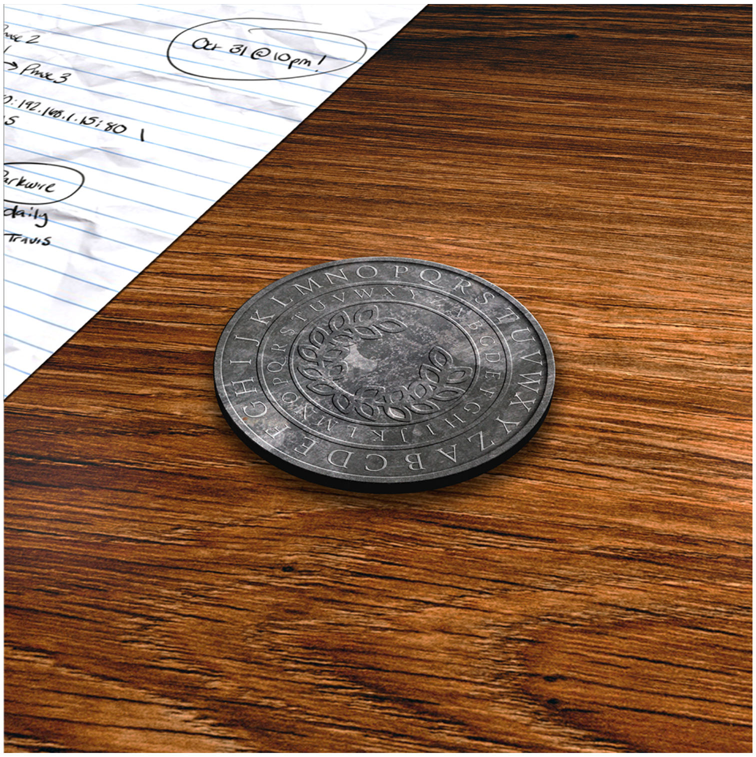


Figure 1: Challenge1 image.

2.1.1 Solution

The original text was encrypted using **Shift Cipher** technique or also known as **Caesar Cipher**. It involves replacing each letter in the message by a letter that is some fixed number of positions in the alphabet [2]. The letters are 'shifted' by some number of spaces to the left or right in alphabet. Decryption is performed using reverse direction shifts. This number of spaces/shifts is called *key*. For example, in the case of this challenge, according to the image above it is a right shift of 18 meaning that *key* = 18 and each letter is replaced by a letter which is to the right by 18 positions(e.g. letter S replaces A because it is 18 positions to the right of A's position):

```
Position:           0 1 2 3 4 5 6 7 8 9 . . .               18 19 . . .
Original alphabet:  A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Shifted alphabet:   S T U V W X Y Z A B C D E F G H I J K L M N O P Q R
```

Based on this we can decipher the encrypted message:

```
Encrypted text: TGG KUSJWV QGM
Decrypted text: BOO SCARED YOU
```

Shift Ciphers work by using the modulo operator to encrypt and decrypt messages performing modulo arithmetic:

```
Encryption: (X + key) mod 26
Decryption: (X − key) mod 26
```

Where X stands for letter position, '+' shift to the right and '-' shift to the left. Modulo arithmetic is used for the cases when after performing shifts $X < 0$ and $X > 25$ in order to keep letter position in range 0-25. For example, letter B in the original message was replaced with T: $(1+18)\%26 = 19$. In this case, the decryption can be performed by replacing each letter in ciphertext with the letter which is to the left by 18 positions:

```
TGG KUSJWV QGM
T = 19
(19 − 18) % 26 = 1 | B
G = 6
(6 − 18) % 26 = 14 | O
. . .
```

(note: in case of G, after 'shifting', letter position equals -12 which is out of range in alphabet, performing mod 26 letter position becomes one of the number from 0 to 25, in this case 14)
As a result, the flag is:

```
flag{BOO SCARED YOU}
```

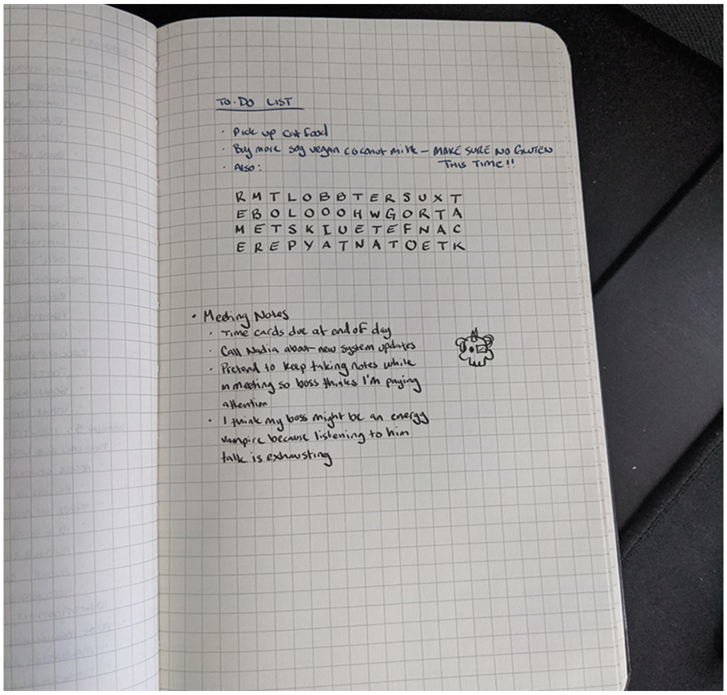
2.2 Cryptography: Down the Wrong Path (10 points)

Flag format:

```
flag{...}
```

Description of the challenge is the following:

> One of our operatives took a photo of a notebook belonging to Donnell. We think it's a message intended for another member of DEADFACE. Can you decipher the message and tell us who it's intended for?



TO-DO LIST

- Pick up cat food
- Buy more soy vegan coconut milk – MAKE SURE NO GLUTEN THIS TIME!!
- Also:

```
R M T L O B B T E R S U X T
E B O L O O O H W G O R T A
M E T S K I U E T E F N A C
E R E P Y A T N A T O E T K
```

- Meeting Notes
  - Time cards due at end of day
  - Call Nadia about new system updates
  - Pretend to keep taking notes while in meeting so boss thinks I'm paying attention
  - I think my boss might be an energy vampire because listening to him talk is exhausting

Figure 2: Challenge2 image.

2.2.1 Solution

The original text was encrypted using **Transposition Cipher** technique, specifically **Route Cipher**. In **Transposition Cipher**, the letters are reordered in some way according to a given rule which is called *key*. In a **Route Cipher** technique, plaintext is written in a grid of given dimensions [4]. One dimension is determined by the key and the second depends on the data size. The plaintext is then read off following the *route* to create a ciphertext, for example *zigzagging up and down*, *spiral inwards clockwise starting from the top right*, etc [3].
Based on the image, the message is already constructed in a grid, so there is no need to rearrange different possible grids. The only step remains is to find a right route to read a plaintext. The name of the challenge might be a hint(Down the Wrong Path), so one of the possible ways of reading is *down of the grid.* Next was to select between reading *to the right* or *to the left.* The route was discovered and message is deciphered:

```
|   R M T L O B B T E R A U X T
|   E B O L O O O H W G O R T A
|   M E T S K I U E T E F N A C
v   E R E P Y A T N A T O E T K
```

REMEMBERTOTELLSPOOKYBOIABOUTTHENEWTARGETSOFOURNEXTATTACK
REMEMBER TO TELL SPOOKY BOI ABOUT THE NEW TARGETS OF OUR NEXT ATTACK

However, this was not a flag, the challenge required to find out who this message was inteded for. Thus, the flag is:

flag{SPOOKYBOI}

References

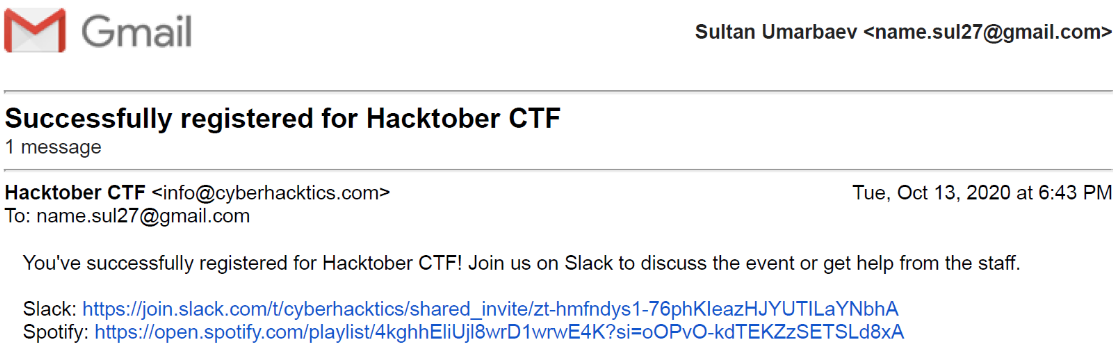
[1] HacktoberCTF Official Blog, URL: `https://blog.cyberhacktics.com/hacktober-2020/`

[2] Caesar cipher, URL: `https://en.wikipedia.org/wiki/Caesar_cipher`

[3] Route Cipher, URL: `https://crypto.interactive-maths.com/route-cipher.html`

[4] Route Cipher, URL: `http://www.crypto-it.net/eng/simple/route-cipher.html`

Appendix A Screenshots and Writeup links



Gmail

Sultan Umarbaev <name.sul27@gmail.com>

Successfully registered for Hacktober CTF

1 message

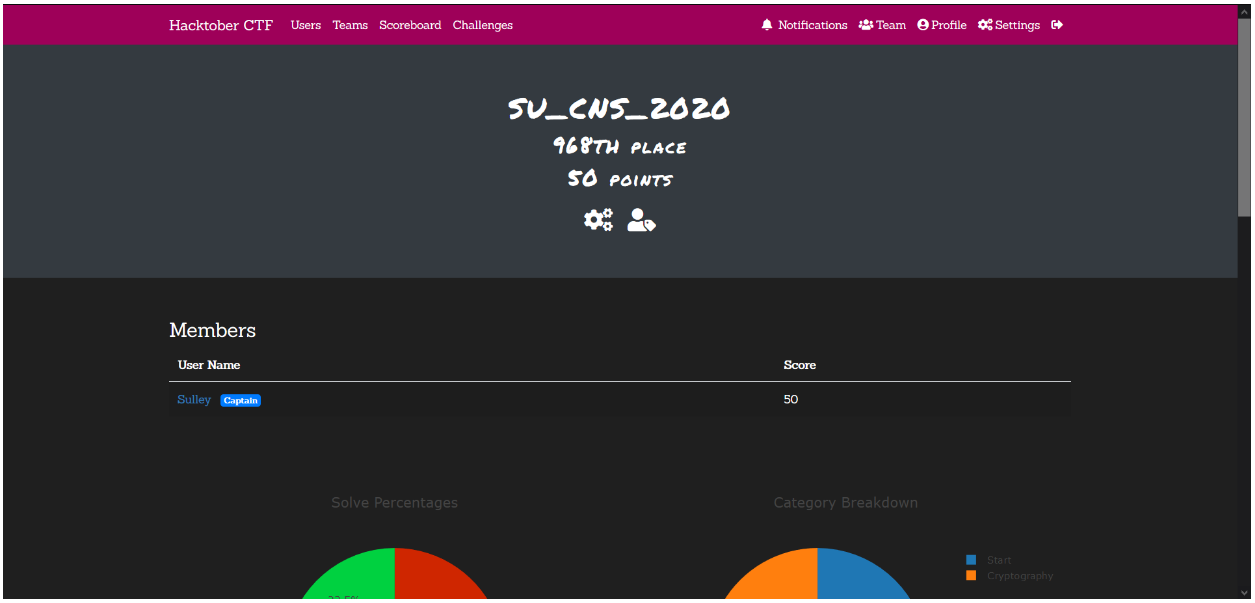
Hacktober CTF <info@cyberhacktics.com> Tue, Oct 13, 2020 at 6:43 PM

To: name.sul27@gmail.com

You've successfully registered for Hacktober CTF! Join us on Slack to discuss the event or get help from the staff.

Slack: https://join.slack.com/t/cyberhacktics/shared_invite/zt-hmfndys1-76phKleazHJYUTILaYNbhA
Spotify: https://open.spotify.com/playlist/4kghhEliUjl8wrD1wrwE4K?si=oOPvO-kdTEKZzSETSLd8xA

Figure 3: Confirmation mail from the CTF event.



SU_CNS_2020

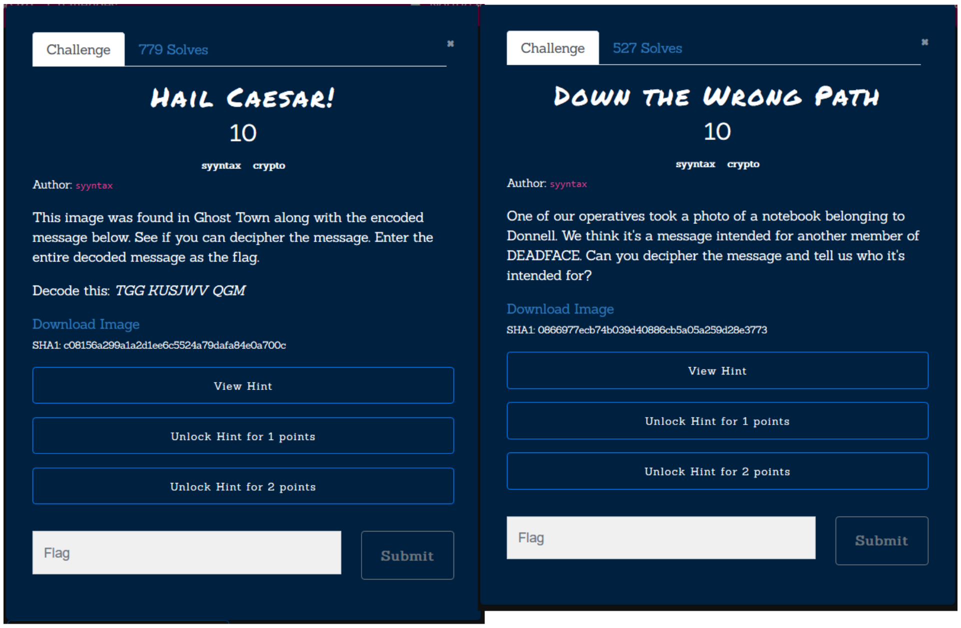
968TH PLACE

50 POINTS

Members

User Name	Score
Sulley Captain	50

Figure 4: Team information.



HAIL CAESAR!

10

syyntax crypto

Author: syyntax

This image was found in Ghost Town along with the encoded message below. See if you can decipher the message. Enter the entire decoded message as the flag.

Decode this: *TGG KUSJWV QGM*

Download Image

SHA1: c08156a299a1a2d1ee6c5524a79dafa84e0a700c

DOWN THE WRONG PATH

10

syyntax crypto

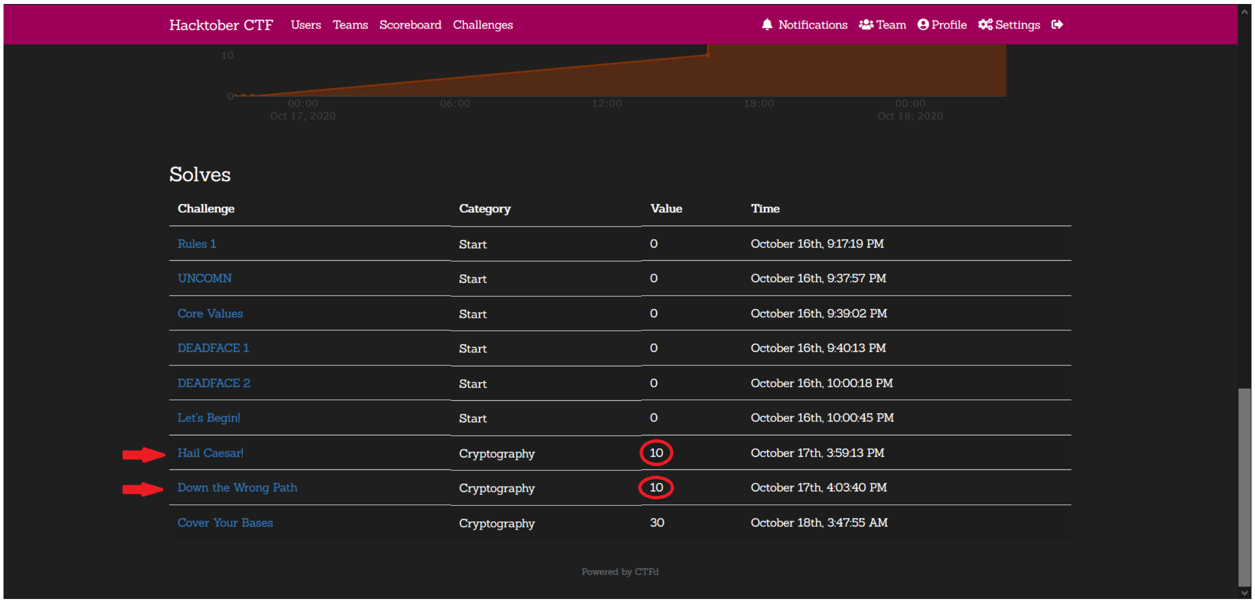
Author: syyntax

One of our operatives took a photo of a notebook belonging to Donnell. We think it's a message intended for another member of DEADFACE. Can you decipher the message and tell us who it's intended for?

Download Image

SHA1: 0866977ecb74b039d40886cb5a05a259d28e3773

Figure 5: Descriptions of challenges.



Solves

Challenge	Category	Value	Time
Rules 1	Start	0	October 16th, 9:17:19 PM
UNCOMN	Start	0	October 16th, 9:37:57 PM
Core Values	Start	0	October 16th, 9:39:02 PM
DEADFACE 1	Start	0	October 16th, 9:40:13 PM
DEADFACE 2	Start	0	October 16th, 10:00:18 PM
Let's Begin!	Start	0	October 16th, 10:00:45 PM
Hail Caesar!	Cryptography	10	October 17th, 3:59:13 PM
Down the Wrong Path	Cryptography	10	October 17th, 4:03:40 PM
Cover Your Bases	Cryptography	30	October 18th, 3:47:55 AM

Figure 6: Points on the CTF.

Links to the writeups:

- Hail Caesar!, `https://ctftime.org/writeup/24273`
- Down the Wrong Path, `https://ctftime.org/writeup/24285`

Appendix B C++ Code, Shift Cipher Decryptor for Challenge 1

```cpp
#include <iostream>

std::string decrypt(std::string msg, int shift) {

    std::string result = "";

    for (int i = 0; i < msg.length(); ++i) {

        if (msg[i] == ' ') {
            result += msg[i];
            continue;
        }

        if (isupper(msg[i]) ) {
            result += char( int(msg[i]-shift+'A')%26 + 'A' );
        }
        else {
            result += char( int(msg[i]-shift+'a')%26 + 'a' );
        }
    }

    return result;
}

int main() {

    std::string msg;
    int shift;

    std::cout << "Enter encrypted message: ";
    getline(std::cin, msg);
    std::cout << "\nShift: ";
    std::cin >> shift;
    std::cout << "\nDecrypted message: " << decrypt(msg, shift) << "\n";

    return 0;
}
```

Listing 1: Shift Cipher Decryptor.