CSE 5382: Secure Programming - Fall 2018 **Student Name** : Biswa Ranjan Nanda

Capture the Flag Bonus Exercise **Student ID** : 1001558251

# Flag Table

Place the flags once you find them in the appropriate table entries below. Each category has a maximum of 20 points with each higher level of difficulty granting an increasing number of points. Maximum score for all challenges completed is 100 points.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **Cryptography** | **Malware** | **Network Capture** | **Reverse Engineering** | **Steganography** |
| **Level 1 (2 Points)** | flag{backoff\_malware} | flag{sandworm\_apt} |  |  |  |
| **Level 2 (3 Points)** |  |  |  |  |  |
| **Level 3 (4 Points)** |  |  |  |  |  |
| **Level 4 (5 Points)** |  |  |  |  |  |
| **Level 5 (6 Points)** |  |  |  |  |  |

# Explanation of Approaches

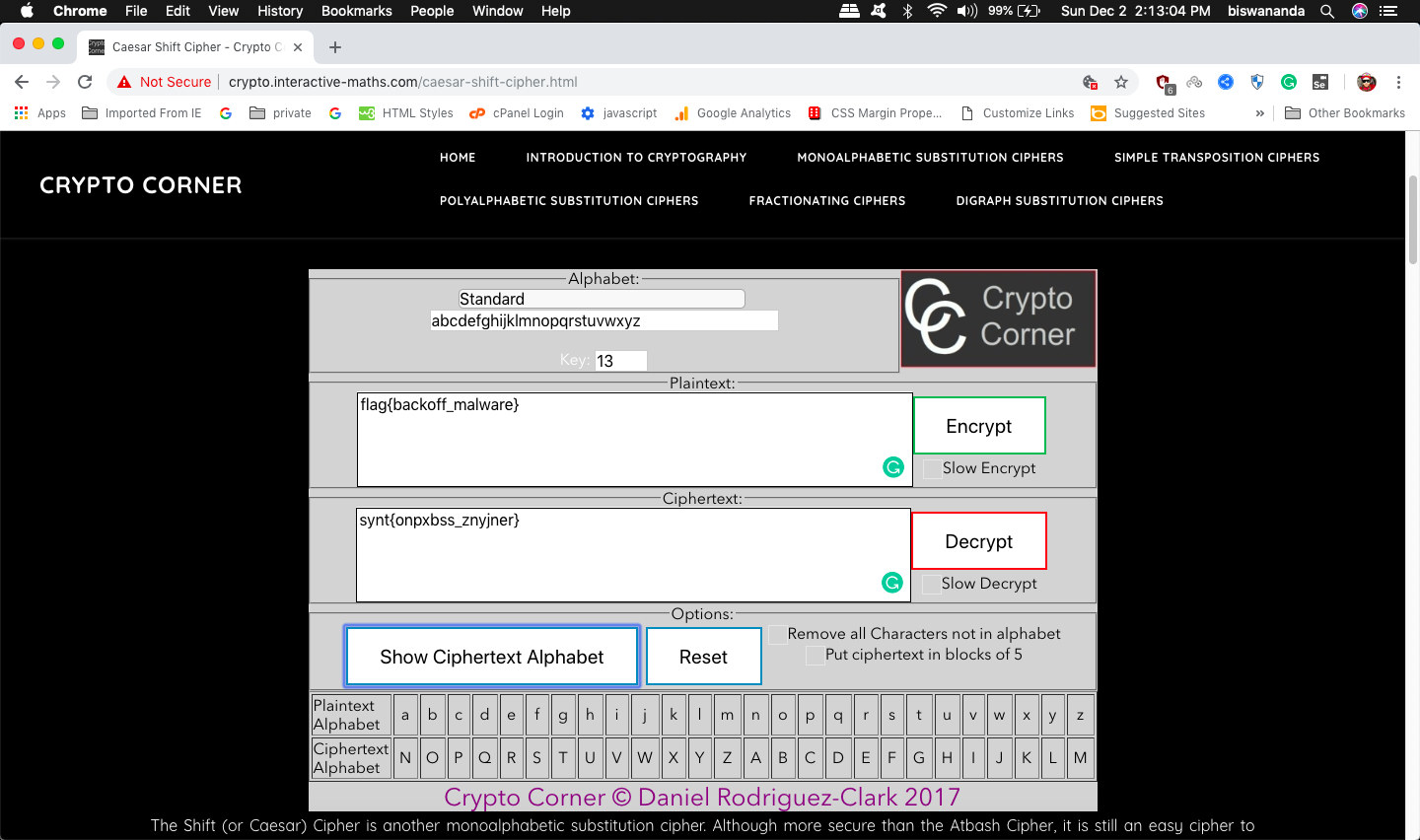
Include descriptions along with screen shots of the approaches you took to solve these challenges.

## Cryptography

### Level 1 – Orange Julius

I went to the website for crypto.interactive-maths.com/Caesar-shift-cipher.html and used our instruction to decrypt the same with key as “13”. Screenshot is mentioned below.

Flag - flag{backoff\_malware}



### Level 2 – Block Chain

### Level 3 – DASH DOT COM

### Level 4 – VIII A Small Example

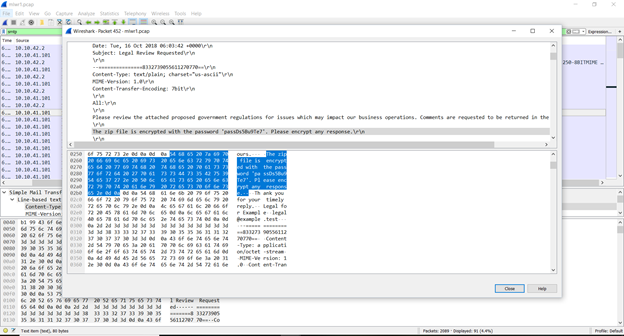
### Level 5 – Big Blue Randu

## Malware

### Level 1

Using Wireshark we open the file to check the password and using the same password, then using Networkminer, the legal.zip file is extracted and using the previous password for the flag.txt to get the flag.

Flag: flag{sandworm\_apt}





### Level 2

Opened the milk.bmp file in paint app in my Macbook Air, and I can see the flag directly.

Flag – flag{cookies\_n\_milk}



### Level 3

### Level 4

### Level 5

## Network Capture

### Level 1 – Modicon-FTP

### Level 2 – Modicon-HTTP

### Level 3 – WinXP-HAVEX

### Level 4 – MICROLOGIX56

### Level 5 – BACNET-COVERT

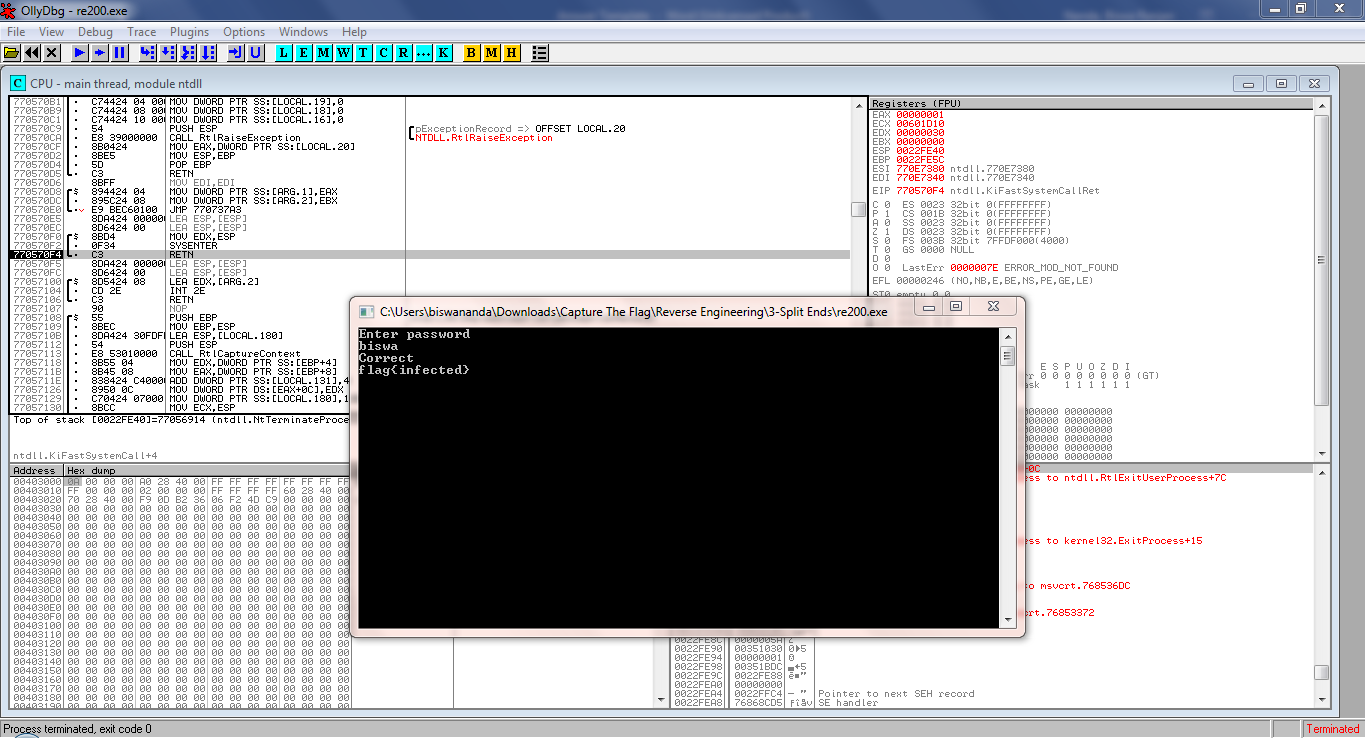
## Reverse Engineering

### Level 1 – Script Kiddie

### Level 2 – The PDF Your Parents Warned You About I

### Level 3 – Split Ends

Tools : VMWare, windows 7, ollydebugger tool



Reference: 1) http://www.ollydbg.de/download.htm

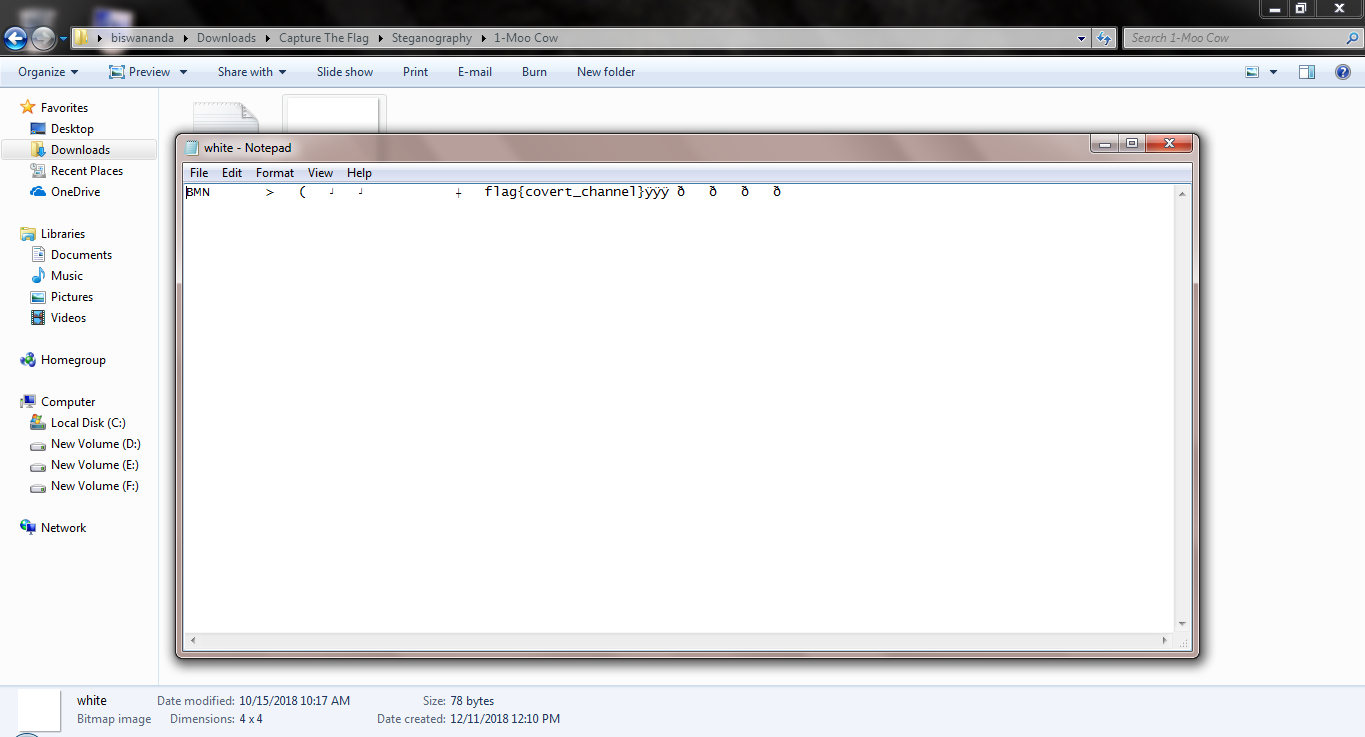
2) http://www.ollydbg.de/version2.html

### Level 4 – The PDF Your Parents Warned You About II

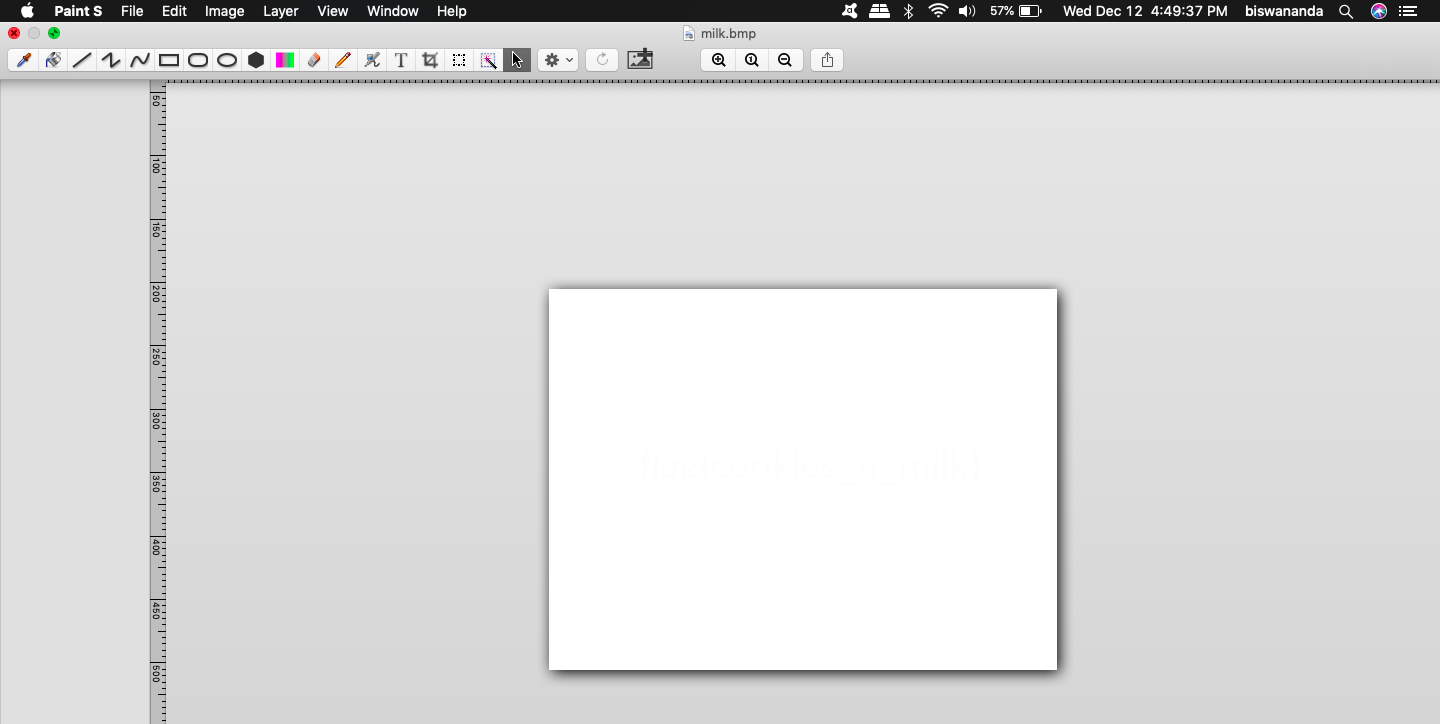
### Level 5 – Rock Scissors Paper Lizard Spock

## Steganography

### Level 1 – Moo Cow

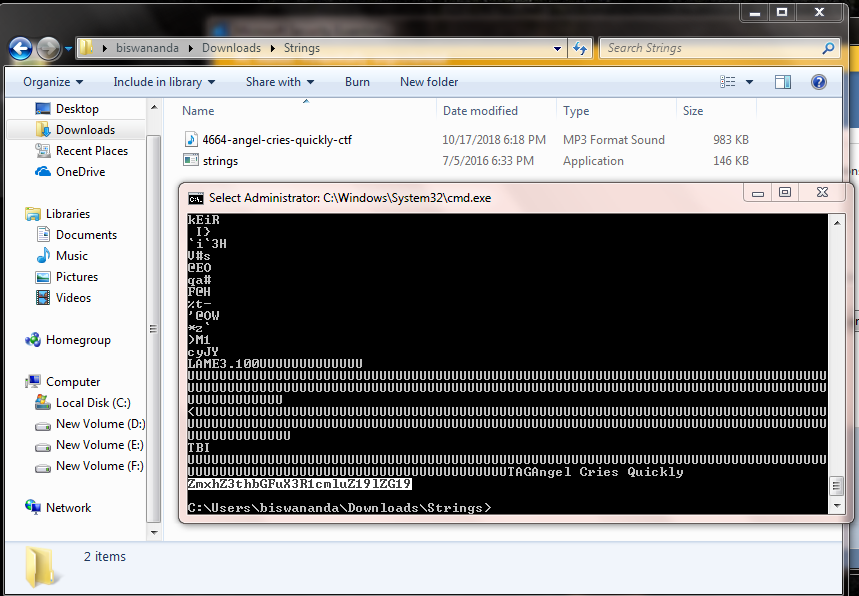


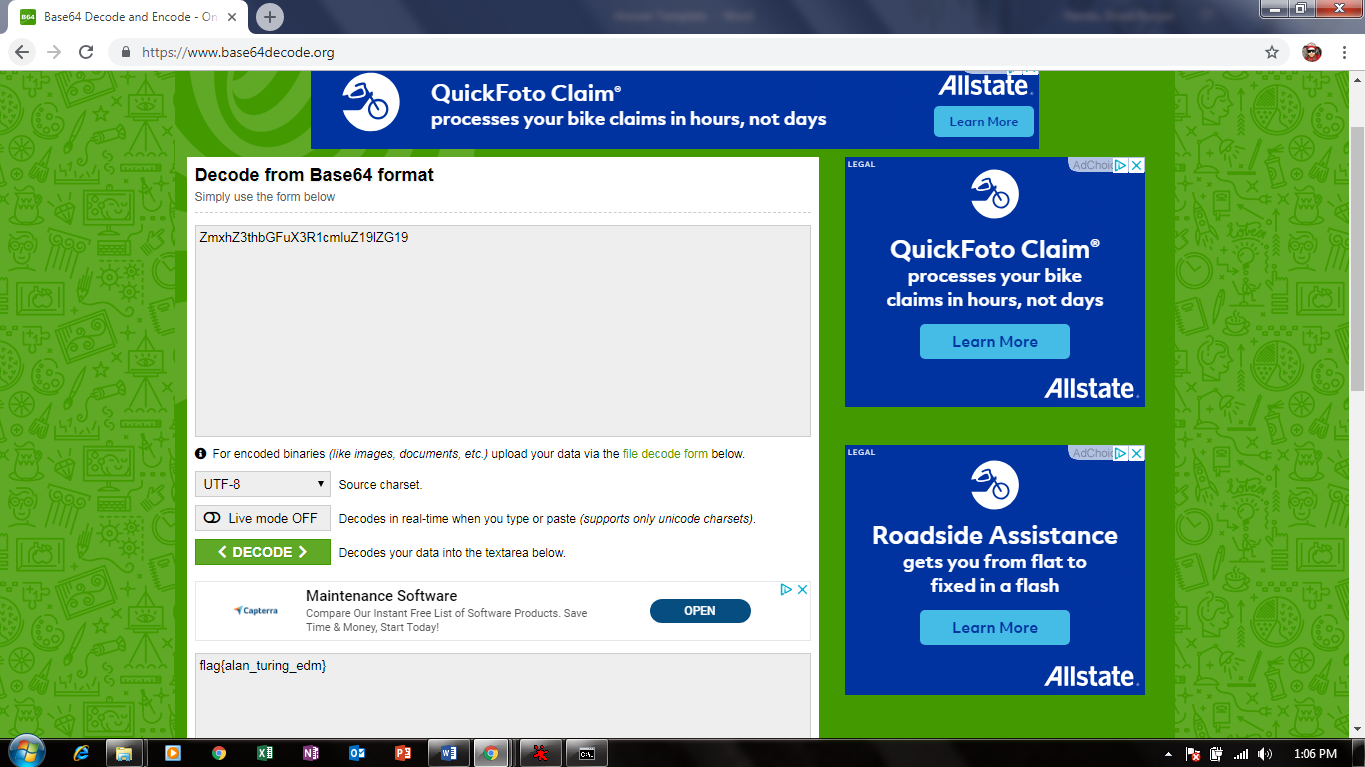
### Level 2 – Milk Run



### Level 3 – Got Root

### Level 4 – AI EDM





### Level 5 – Final Frontier