CTF Group 5 Draft

Guo Yuchen 1004885
Meng Fanyi 1004889
Xiang Siqi 1004875
Zach Lim 1002141

Topics Covered

- Base64 encoding
- Vigenere Cipher
- Steganography

Encryption

Step1: **Set up the flag and the Vigenere key**
flag = "fcs22{wahhhhhhhh_you_found_the_flag!!!whooohooo}"
Vigenere key = counterstrike(length = 13)

Step2: Encrypt the flag

1. Convert the flag to a base64 text: ZmNzMjJ7d2FoaGhoaGhoaF95b3VfZm91bmRfdGhlX2ZsYWchISF3aG9vb2hvb299
2. Encrypt the flag using variant Vigenere cipher (refer to table[1] below).
3. Convert the encrypted flag to binary (ASCII).

	A	**B**	**...**	**Z**	**a**	**b**	**...**	**z**	**0**	**1**	**...**	**9**	**+**	**/**	**=**
A	A	B	...	Z	a	b	...	z	0	1	...	9	+	/	=
B	B	...	Z	a	b	...	z	0	1	...	9	+	/	=	A
...	...	Z	a	b	...	z	0	1	...	9	+	/	=	A	B
Z	Z	a	b	...	z	0	1	...	9	+	/	=	A	B	...
a	a	b	...	z	0	1	...	9	+	/	=	A	B	...	Z
b	b	...	z	0	1	...	9	+	/	=	A	B	...	Z	a
...	...	z	0	1	...	9	+	/	=	A	B	...	Z	a	b
z	z	0	1	...	9	+	/	=	A	B	...	Z	a	b	...

Table[1]: Variant Vigenere Cipher

Plaintext: ZmNzMjJ7d2FoaGhoaGhoaF95b3VfZm91bmRfdGhlX2ZsYWchISF3aG9vb2hvb299
Key: counterstrikecounterstrikecounterstrikecounterstrikecounterstrik
Ciphertext: <haven't computed yet>
Step3: Embed the encrypted flag into the image

1. Embed the encrypted flag into ImageFlag.pbm.
2. Specifically, substitute the last bit of each byte with the bit in the encrypted flag.

What we publish

1. Image containing encrypted flag: **ImageFlag.pbm**.
2. **Code** for students to figure out the steganography method and Vigenere lookup table.

Decryption

Step1 Retrieve the encrypted text:

1. Explore the code to figure out how the flag is encrypted.
2. Retrieve the last bit of each byte in ImageFlag.pbm.
3. Concatenate all bits retrieved.
4. Convert the bit string to a text.

Step2 Decrypt the ciphertext and gain the flag:

1. Implement brute force on each character of the cipher (in a round of key length) to retrieve the base 64 encoded flag.
    - Details: Since the first 6 characters of the flag “fcs22{” are fixed, students can easily guess the first 8 characters of the Vigenere key. Then they can carry out the attack by guessing the rest of the key according to the prefix obtained or using other kinds of attacks such as brute force.
2. Decode the ciphertext using the key obtained to retrieve the flag.