Faculty of Engineering – Cairo University

Computer Engineering Department

Third Year – Mainstream

Cryptography

Project

Name	Section	BN	ID
محمد يحي الأحمد العمر	2	14	9213024
مصطفي محمد السيد توفيق	2	23	9211194
مصطفي هاني مصطفي محمد	2	24	9211206
منة الله أحمد	2	25	9211230

Part2

CTF – 1 (Cryptanalysis)

1. Caesar Cipher Shift: Attempted to decrypt the text using a Caesar cipher by trying all possible shift values, but it didn't yield any recognizable plaintext.

2. Affine Cipher Shift: Similarly, Tried using an affine cipher, which involves a combination of multiplication and addition in modular arithmetic, but again, didn't get the original text.

3. Single Letter Frequency Analysis: Analyzed the frequency of individual letters in the cipher text using python code to plot the histogram. Ex, found that 'e' is the most common letter.

4. Trigram & Bigram Frequency Analysis: calculated the frequencies of trigrams (sequences of three letters) in the cipher text. Ex, found that "khi" is the most frequent trigram. This is a significant clue because "The" is a common word in English , second one is "vhi" which is "she" then "emo" which doesn't contain "i" so I understand that it's "and".

5. Substitution: use a substitution cipher. In a substitution cipher, each letter in the plaintext is replaced with another letter based on a predetermined mapping.

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
C	R	L	M	A	J	P	H	E	Q	T	K	N	F	D	O	V	I	G	B	X	S	Y	U	W	Z

Link for the code and decrypted text:

https://drive.google.com/drive/folders/1ZA2fO-gZQ_vUZ16tIhFje8whIIwfC6LL?usp=drive_link

CTF – 2 (Packet Analysis)

1. Open the Packet Capture File: Use Wireshark to open the packet capture file "packets.pcapng".

2. Analyze Protocol Hierarchy: Navigate to the protocol hierarchy in Wireshark to identify the relevant packets containing text data.

3. Locate Text Data: Within the protocol hierarchy, identify the packets containing line-based text data. This is where you might have hidden the flag.

4. Catch Encrypted Flag: Upon finding the text data, notice that the flag is encrypted or manipulated in some way to make it difficult to read.

" Gur synt vf cvpbPGS{c33xno00_1_f33_h_qrnqorrs} "

5. Decrypt the Flag: Apply decryption techniques to reveal the original text of the flag. Using Caesar Cipher with shift=13

The flag is picoCTF{p33kab00_1_s33_u_deadbeef}

CTF – 3 (Image Manipulation)

1. XOR Operation: Developed a Python script to perform XOR operation on the images "first.png" and "second.png" to reveal potential hidden information.

2. Make Flag Clear: Enhanced flag visibility by adjusting the color scheme of the XOR output, allowing for clear identification and extraction of the flag.

3. Catch The Flag

picoCTF{d72ea4af}

Link for the code and images output:

https://drive.google.com/drive/folders/1e65cqhLM1M9Wwn04_YReffNYYouN6TNp?usp=drive_link

CTF – 4 (Bit Shifting)

1. Noticed the hint that we want to shift even though we have same chars in the file, Tried to convert it to hexa and shift but it didn't work

3. Finally, I tried to convert text to binary first then I used this [tool] (https://www.prepostseo.com/tool/binary-translator) and tried different shifting values to the binary text and noticed the output text until I found this one through *shift right by 6 bits

4. The text found is

- Hello and welcome to file 99 forensic challenge (This is just filler text to make it longer fastctf {a_bit_tricky}.

5. Catch The Flag **fastctf {a_bit_tricky}**

CTF – 5 (Search)

1. Open Command Prompt

2. Navigate To The Directory Where The "logs" File Is Located.

3. Using This Command To Search For The Flag Within The "logs" File.

>grep -i "{" logs

4 .Catch The Flag

picoCTF{grep_is_good_to_find_things_dba08a45}

CTF – 6 (New Encryption)

1. The encryption scheme implemented in the provided code involves two steps:

Encoding in Base16 (hexadecimal), then Caesar Shift Encryption

2. To decrypt the ciphertext, we need to reverse the process using the code:

Reverse the Caesar shift encryption, then decode the Base16 encoded string back to plaintext.

3. Catch the flag

The enemies are making a move. We need to act fast.

Link for the code and images output:

https://drive.google.com/drive/folders/1MG1FjMDYa_lvLB9z3473DJM33kdv77bC?usp=drive_link

CTF – 7 (Steganography)

1. Installing Steghide: To ensure I had the necessary tool for steganography analysis, I installed Steghide using the package manager. In my case, as I use Ubuntu, Using the following command: sudo apt-get install steghide.

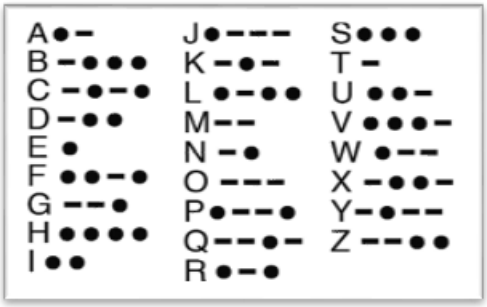
2. Extracting The Hidden Data: I proceeded to extract any concealed data from the image. Utilizing the terminal, I executed the following command: steghide extract -sf pepo_evil.jpg , Using paraphrase: HIDING (Understood from problem).

3. Catch The Flag

Hello, the flag is CMPN{Spring2024}

CTF – 8 (Can You Help Me ?)

1. Identification of Morse code: Recognized Morse code patterns within the sound file, noting its characteristic short and long signals



2. Extracted Morse code signals from the sound file

3. Got The Text

The Russian terrorists are the ones who started this. They are the key. Please, you must extract me.

4. Using command strings in linux

strings lastcall.wav

5. Using nihilist cipher to decrypt the outputed ciphertext that appear with key = RUSSIAN , and keyword = POLYBIUS

6. Catch The Flag

THANKYOUFORSAVINGMETHEFLAGISMOSCOW