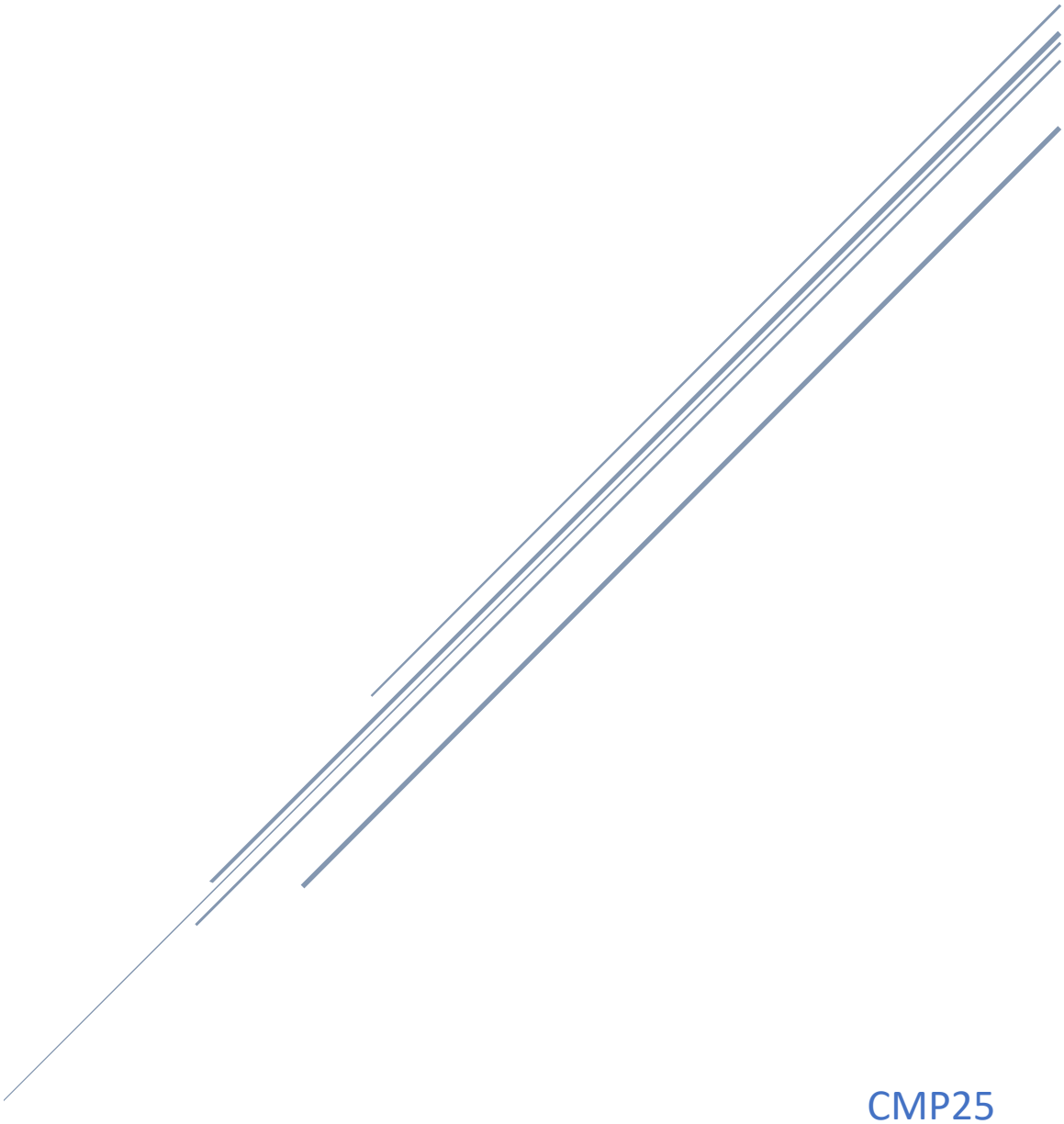
CTFS



CMP25

Cryptography and Network Security

Contents

CTF– 1(Cryptanalysis):

1. Drawing the letters frequency histogram in the encrypted document and comparing it with the English alphabets' letters frequency.
2. Trying to guess short words decrypted forms like "the" and "to".
3. After trial and error creating a mapping of each encrypted letter to its corresponding decrypted one and replacing them in the whole document.

CTF– 2(Packet Analysis):

Flag ➔ "the flag is picoctf{p33kab00_1_s33_u_deadbeef}"

1. Using wireshark to analyze packets.
2. Flag found encrypted in one of the http requests.
3. It was noticed that the flag was encrypted using Caesar cipher.
4. Decrypting the flag after guessing the number of shifts.

CTF– 3(Image Manipulation):

Flag ➔ picoCTF{d72ea4af}

1. **Blending the two images together by adding their corresponding RGB values.**

CTF– 4(Bit Shifting):

Flag ➔ "fastctf{a_bit_tricky}".

1. Converting the whole file into a bit string.
2. Shifting the whole string left by 1 position.
3. Recovering characters from the bit string and getting the flag.

CTF– 5(Search):

Flag ➔ "picoCTF{grep_is_good_to_find_things_dba08a45}"

Used the following bash command: "grep -i -E -o '(\S*ctf\S*|\S*flag\S*|\S*key\S*|\S*string\S*|\S*secret\S*|\S*token\S*)' logs"

CTF– 6(New Encryption):

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

1. Write a function to decode b_16.
2. Write a function to perform inverse Caesar cipher shift.
3. Trying all the candidate keys till getting the right one and decrypting the ciphertext.

CTF– 7(Steganography):

flag: "Hello, the flag is CMPN{Spring2024}"

Using Steghide where the passphrase is "HIDING" to get the key:

Command Used: "steghide --extract -sf pepo_evil.jpg -p HIDING".

CTF– 8(Can You Help Me ?):

the message is:

"THE RUSSIAN TERRORISTS ARE THE ONES WHO STARTED THIS, THEY ARE THE KEY. PLEASE YOU MUST EXTRACT ME."

- Using an online tool to decrypt "Morse Code" to get the message.

Using this website: https://morsecode.world/international/decoder/audio-decoder-adaptive.html

- Converting the file into a sequence of binary bits and converting each byte to its corresponding character.
- https://en.wikipedia.org/wiki/Nihilist_cipher?keyword=polybius ➔ getting this link and figuring out the message was encrypted with Nihilist cipher with keyword "**Polybius**" and key "**RUSSIAN**".
- Decrypting the message and getting the flag "**MOSCOW**"