Cryptography Project

Part 2: CTF

CTF– 1(Cryptanalysis)

Using monoalphabetic substitution cipher with this mapping dictionary :
{'E': 'A', 'C': 'L', 'R': 'I', 'A': 'C', 'I': 'E', 'Y': 'W', 'V': 'S', 'T': 'B', 'S': 'G', 'M': 'N', 'K': 'T', 'P': 'O', 'Q': 'V', 'B': 'R', 'W': 'Y', 'O': 'D', 'N': 'F', 'H': 'H', 'L': 'K', 'G': 'P', 'X': 'U'}

Deciphered text :

```
ALICE WAS BEGINNING TO GET VERY TIRED OF SITTING BY HER SISTER ON THE
BANK AND OF HAVING NOTHING TO DO ONCE OR TWICE SHE HAD PEEPED INTO THE
BOOK HER SISTER WAS READING BUT IT HAD NO PICTURES OR CONVERSATIONS IN
IT AND WHAT IS THE USE OF A BOOK THOUGHT ALICE WITHOUT PICTURES OR
CONVERSATIONS

SO SHE WAS CONSIDERING IN HER OWN UIND AS WELL AS SHE COULD FOR THE
DAY UADE HER FEEL VERY SLEEPY AND STUPID WHETHER THE PLEASURE OF
UAKING A DAISYCHAIN WOULD BE WORTH THE TROUBLE OF GETTING UP AND
PICKING THE DAISIES WHEN SUDDENLY A WHITE RABBIT WITH PINK EYES RAN
CLOSE BY HER

THERE WAS NOTHING SO VERY REUARKABLE IN THAT NOR DID ALICE THINK IT SO
VERY UUCH OUT OF THE WAY TO HEAR THE RABBIT SAY TO ITSELF OH DEAR OH
DEAR I SHALL BE TOO LATE BUT WHEN THE RABBIT ACTUALLY TOOK A WATCH
OUT OF ITS WAISTCOATPOCKET AND LOOKED AT IT AND THEN HURRIED ON ALICE
STARTED TO HER FEET FOR IT FLASHED ACROSS HER UIND THAT SHE HAD NEVER
BEFORE SEEN A RABBIT WITH EITHER A WAISTCOATPOCKET OR A WATCH TO TAKE
OUT OF IT AND BURNING WITH CURIOSITY SHE RAN ACROSS THE FIELD AFTER
IT AND WAS DUST IN TIUE TO SEE IT POP DOWN A LARGE RABBITHOLE UNDER
THE HEDGE IN ANOTHER UOUENT DOWN WENT ALICE AFTER IT

THE RABBITHOLE WENT STRAIGHT ON LIKE A TUNNEL FOR SOUE WAY AND THEN
DIPPED SUDDENLY DOWN SO SUDDENLY THAT ALICE HAD NOT A UOUENT TO THINK
ABOUT STOPPING HERSELF BEFORE SHE FOUND HERSELF FALLING DOWN WHAT SEEUED
TO BE A VERY DEEP WELL

EITHER THE WELL WAS VERY DEEP OR SHE FELL VERY SLOWLY FOR SHE HAD
PLENTY OF TIUE AS SHE WENT DOWN TO LOOK ABOUT HER FIRST SHE TRIED TO
UAKE OUT WHAT SHE WAS COUING TO BUT IT WAS TOO DARK TO SEE ANYTHING
THEN SHE LOOKED AT THE SIDES OF THE WELL AND NOTICED THAT THEY WERE
FILLED WITH CUPBOARDS AND BOOKSHELVES HERE AND THERE SHE SAW UAPS AND
PICTURES HUNG UPON PEGS SHE TOOK DOWN A DAR FROU ONE OF THE SHELVES AS
SHE PASSED IT WAS LABELED ORANGE UARUALADE BUT TO HER GREAT
DISAPPOINTUENT IT WAS EUPTY SHE DID NOT LIKE TO DROP THE DAR SO
UANAGED TO PUT IT INTO ONE OF THE CUPBOARDS AS SHE FELL PAST IT

DOWN DOWN DOWN WOULD THE FALL NEVER COUE TO AN END THERE WAS NOTHING
ELSE TO DO SO ALICE SOON BEGAN TALKING TO HERSELF DINAHLL UISS UE
VERY UUCH TONIGHT I SHOULD THINK DINAH WAS THE CAT I HOPE
THEYLL REUEUBER HER SAUCER OF UILK AT TEATIUE DINAH UY DEAR I WISH
YOU WERE DOWN HERE WITH UE ALICE FELT THAT SHE WAS DOZING OFF WHEN
SUDDENLY THUUP THUUP DOWN SHE CAUE UPON A HEAP OF STICKS AND DRY
LEAVES AND THE FALL WAS OVER
```

ALICE WAS NOT A BIT HURT AND SHE DUUPED UP IN A UOUENT SHE LOOKED UP BUT IT WAS ALL DARK OVERHEAD BEFORE HER WAS ANOTHER LONG PASSAGE AND THE WHITE RABBIT WAS STILL IN SIGHT HURRYING DOWN IT THERE WAS NOT A UOUENT TO BE LOST AWAY WENT ALICE LIKE THE WIND AND WAS DUST IN TIUE TO HEAR IT SAY AS IT TURNED A CORNER OH UY EARS AND WHISKERS HOW LATE ITS GETTING SHE WAS CLOSE BEHIND IT WHEN SHE TURNED THE CORNER BUT THE RABBIT WAS NO LONGER TO BE SEEN

SHE FOUND HERSELF IN A LONG LOW HALL WHICH WAS LIT UP BY A ROW OF LAUPS HANGING FROU THE ROOF THERE WERE DOORS ALL ROUND THE HALL BUT THEY WERE ALL LOCKED AND WHEN ALICE HAD BEEN ALL THE WAY DOWN ONE SIDE AND UP THE OTHER TRYING EVERY DOOR SHE WALKED SADLY DOWN THE UIDDLE WONDERING HOW SHE WAS EVER TO GET OUT AGAIN

SUDDENLY SHE CAUE UPON A LITTLE TABLE ALL UADE OF SOLID GLASS THERE WAS NOTHING ON IT BUT A TINY GOLDEN KEY AND ALICES FIRST IDEA WAS THAT THIS UIGHT BELONG TO ONE OF THE DOORS OF THE HALL BUT ALAS EITHER THE LOCKS WERE TOO LARGE OR THE KEY WAS TOO SUALL BUT AT ANY RATE IT WOULD NOT OPEN ANY OF THEU HOWEVER ON THE SECOND TIUE ROUND SHE CAUE UPON A LOW CURTAIN SHE HAD NOT NOTICED BEFORE AND BEHIND IT WAS A LITTLE DOOR ABOUT FIFTEEN INCHES HIGH SHE TRIED THE LITTLE GOLDEN KEY IN THE LOCK AND TO HER GREAT DELIGHT IT FITTED

ALICE OPENED THE DOOR AND FOUND THAT IT LED INTO A SUALL PASSAGE NOT UUCH LARGER THAN A RATHOLE SHE KNELT DOWN AND LOOKED ALONG THE PASSAGE INTO THE LOVELIEST GARDEN YOU EVER SAW HOW SHE LONGED TO GET OUT OF THAT DARK HALL AND WANDER ABOUT AUONG THOSE BEDS OF BRIGHT FLOWERS AND THOSE COOL FOUNTAINS BUT SHE COULD NOT EVEN GET HER HEAD THROUGH THE DOORWAY OH SAID ALICE HOW I WISH I COULD SHUT UP LIKE A TELESCOPE I THINK I COULD IF I ONLY KNEW HOW TO BEGIN

ALICE WENT BACK TO THE TABLE HALF HOPING SHE UIGHT FIND ANOTHER KEY ON IT OR AT ANY RATE A BOOK OF RULES FOR SHUTTING PEOPLE UP LIKE TELESCOPES THIS TIUE SHE FOUND A LITTLE BOTTLE ON IT WHICH CERTAINLY WAS NOT HERE BEFORE SAID ALICE AND TIED ROUND THE NECK OF THE BOTTLE WAS A PAPER LABEL WITH THE WORDS DRINK UE BEAUTIFULLY PRINTED ON IT IN LARGE LETTERS

NO ILL LOOK FIRST SHE SAID AND SEE WHETHER ITS UARKED POISON OR NOT FOR SHE HAD NEVER FORGOTTEN THAT IF YOU DRINK FROU A BOTTLE UARKED POISON IT IS ALUOST CERTAIN TO DISAGREE WITH YOU SOONER OR LATER HOWEVER THIS BOTTLE WAS NOT UARKED POISON SO ALICE VENTURED TO TASTE IT AND FINDING IT VERY NICE IT HAD A SORT OF UIJED FLAVOR OF CHERRYTART CUSTARD PINEAPPLE ROAST TURKEY TOFFY AND HOT BUTTERED TOAST SHE VERY SOON FINISHED IT OFF

WHAT A CURIOUS FEELING SAID ALICE I UUST BE SHUTTING UP LIKE A TELESCOPE

AND SO IT WAS INDEED SHE WAS NOW ONLY TEN INCHES HIGH AND HER FACE BRIGHTENED UP AT THE THOUGHT THAT SHE WAS NOW THE RIGHT SIZE FOR GOING THROUGH THE LITTLE DOOR INTO THAT LOVELY GARDEN

AFTER AWHILE FINDING THAT NOTHING UORE HAPPENED SHE DECIDED ON GOING INTO THE GARDEN AT ONCE BUT ALAS FOR POOR ALICE WHEN SHE GOT TO THE DOOR SHE FOUND SHE HAD FORGOTTEN THE LITTLE GOLDEN KEY AND WHEN SHE WENT BACK TO THE TABLE FOR IT SHE FOUND SHE COULD NOT POSSIBLY REACH IT SHE COULD SEE IT FUITE PLAINLY THROUGH THE GLASS AND SHE TRIED HER BEST TO CLIUB UP ONE OF THE LEGS OF THE TABLE BUT IT WAS TOO SLIPPERY AND WHEN SHE HAD TIRED HERSELF OUT WITH TRYING THE POOR LITTLE THING SAT DOWN AND CRIED

COUE THERES NO USE IN CRYING LIKE THAT SAID ALICE TO HERSELF RATHER SHARPLY I ADVISE YOU TO LEAVE OFF THIS UINUTE SHE GENERALLY GAVE HERSELF VERY GOOD ADVICE THOUGH SHE VERY SELDOU FOLLOWED IT AND SOUETIUES SHE SCOLDED HERSELF SO SEVERELY AS TO BRING TEARS INTO HER EYES

SOON HER EYE FELL ON A LITTLE GLASS BOJ THAT WAS LYING UNDER THE TABLE
SHE OPENED IT AND FOUND IN IT A VERY SUALL CAKE ON WHICH THE WORDS EAT
UE WERE BEAUTIFULLY UARKED IN CURRANTS WELL ILL EAT IT SAID
ALICE AND IF IT UAKES UE GROW LARGER I CAN REACH THE KEY AND IF IT
UAKES UE GROW SUALLER I CAN CREEP UNDER THE DOOR SO EITHER WAY ILL
GET INTO THE GARDEN AND I DONT CARE WHICH HAPPENS

SHE ATE A LITTLE BIT AND SAID ANJIOUSLY TO HERSELF WHICH WAY WHICH
WAY HOLDING HER HAND ON THE TOP OF HER HEAD TO FEEL WHICH WAY SHE WAS
GROWING AND SHE WAS FUITE SURPRISED TO FIND THAT SHE REUAINED THE SAUE
SIZE SO SHE SET TO WORK AND VERY SOON FINISHED OFF THE CAKE

CTF– 2(Packet Analysis)

We used Wireshark to read the file `packets.pcapng`, analyzed the requests, and identified those with a content type of text. Among these requests, we found the following text in one of the responses:

Gur synt vf cvpbPGS{c33xno00_1_f33_h_qrnqorrs}

This text resembles a flag format {some_text}. Upon further analysis, we discovered that a Caesar cipher with a shift of 13 was applied to this text. Decoding it, we found the plain text to be:

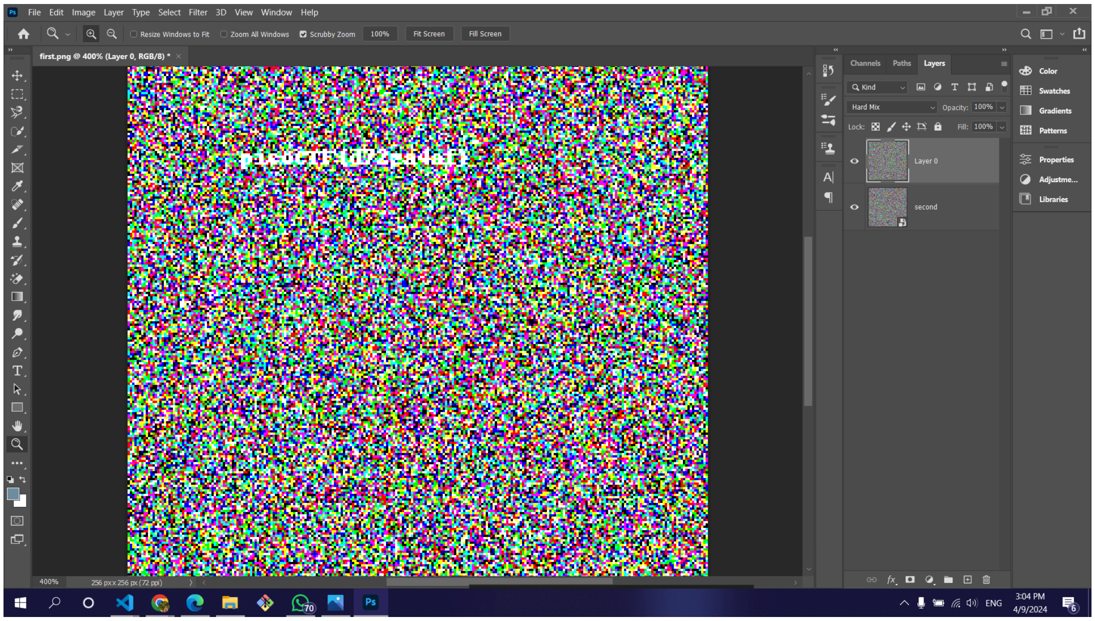
The flag is picoCTF{p33kab00_1_s33_u_deadbeef}

This appears to be the correct flag.

CTF– 3(Image Manipulation)

Added the two pictures on each other as layers on adobe photoshop and tried the filters until the one named “hard mix” showed the flag, hard mix is simply given set of base and blend layers, the individual channel values are added together (that is, reds are added to reds, greens to greens, etc.)

So the flag is: **picoCTF{d72ea4af}**



first.png @ 400% (Layer 0, RGB/8) *

Hard Mix

Opacity: 100%

Fill: 100%

Layer 0

second

400%

256 px x 256 px (72 ppi)

CTF– 4(Bit Shifting)

Using Powershell tool Format-Hex to view the text in the correct format, then using the following code to convert the ascii into bits, then rotate this bits by one, we get the following text:
Hellnand\welcomdtnfildforensibchallengd\Thirirjust\filler\text\tnmakdit\longer\\\fastctf{a_bit_tricky|
Helloand\welcometofileforensicchallenge\Thisisjust\filler\text\tomakeit\longer\\\fastctf{a_bit_trick|
The flag is **fastctf{a_bit_tricky}**

```
def ascii_to_binary(ascii_string):
    binary_chars = [format(ord(char), '08b') for char in ascii_string]
    binary_string = ''.join(binary_chars)
    return binary_string
def rotate_binary_string(binary_string, n):
    n = n % len(binary_string)
    rotated_string = binary_string[n:] + binary_string[:n]
    return rotated_string
def binary_to_ascii(binary_string):
    binary_chunks = [binary_string[i:i+8] for i in range(0,
len(binary_string), 8)]
    ascii_chars = [chr(int(chunk, 2)) for chunk in binary_chunks]
    ascii_string = ''.join(ascii_chars)
    return ascii_string
bits =
"$2¶670·2.;²¶1·¶²:734¶237¹2·9´±1´0¶62·3².*44¹4¹5:¹°.34¶62¹.:2¼:.:76°µ²4°.6
7·3²¹...30¹°1°3=°¯±4°/°94±µ¼¾"
binary_sentence=ascii_to_binary(bits)
binary_sentence = rotate_binary_string(binary_sentence, 1)
ascii_sentence = binary_to_ascii(binary_sentence)
print(ascii_sentence)
```

CTF– 5(Search)

The hint was grep so when searching about “grep” literally in the file we found the flag and the flag is:

```
picoCTF{grep_is_good_to_find_things_dba08a45}
```

CTF– 6(New Encryption)

We reversed the encryption used be implementing decode function that reverse the encode, and a function that reverse the caesar shift using the following code:

```
import string
```

```
START = ord("a")
CHARSET = string.ascii_lowercase[:16]
def decode_b16(cipher):
    decoded = ""
    for i in range(0,len(cipher),2):
        high=ord(cipher[i])-97
        low=ord(cipher[i+1])-97
        index="{0:04b}".format(high)+"{0:04b}".format(low)
        decoded+=string.ascii_lowercase[(int(index, 2)-97)%26]
    return decoded
def de_caesar_shift(c, k):
    return CHARSET[(ord(c)- ord(k) ) % len(CHARSET)]
key = "e"
dec=""
enc="jikmkjgekjkckjkbknkjlhgekflgkjgekbkfkpknkcklgekfgekbkdlkkjgcgejlkjgekckjkjkigelikdgekfkhligekkkflhligc"
for i, c in enumerate(enc):
    dec += de_caesar_shift(c, key[i % len(key)])
print("plain2: "+decode_b16(dec))
```

After trying the whole keys from the given key “secretkey” we found the “e” was the key used in encryption, then using the previous functions with the given ciphertext, the plaintext was:
Nhenenemiesnarenmakingnanmovebnqenneedntonactnfastb
The flag is **When enemies are making a move, we need to act fast.**

CTF– 7(Steganography)

Used the “steghide” tool on kali linux
The command I used is: `steghide extract -sf pepo_evil.jpg`
with a passphrase of “HIDING”
Hello, the flag is CMPN{Spring2024}

CTF– 8(Can You Help Me ?)

The sound provided is encoded using morse code which is a code that uses just dots and dashes to represent letters so we have recognised it and found out that the message is
THE RUSSIAN TERRORISTS ARE THE ONES WHO STARTED THIS, THEY ARE THE KEY. PLEASE YOU MUST EXTRACT ME
And then we used steghide online tool to try to extract information form lastcall.wav and got cipher
96 57 47 66 62 38 55 67 55 35 68 44 48 95 66 65 57 65 53 75 78 77 55 36 47 55 45 66 87 34 46 48 33 77

with link
https://en.wikipedia.org/wiki/Nihilist_cipher?keyword=polybius

So we put the keyword to Nihilist cipher and the key RUSSIAN as stated in the decoded morse code and the decrypted cipher is
THANKYOUFORSAVINGMETHEFLAGISMOSCOW
So the one who is in danger is in Moscow