NZCSC 2020 Solutions

July 2020

R0 - Challenge 1

Theme: Cryptography – Caesar cipher

Tools used:

- https://www.dcode.fr/caesar-cipher
- https://www.rapidtables.com/convert/number/decimal-to-hex.html

"THE ANCIENTS ENVISIONED THEIR WORLD IN TWO HALVES. - DA VINCI CODE"

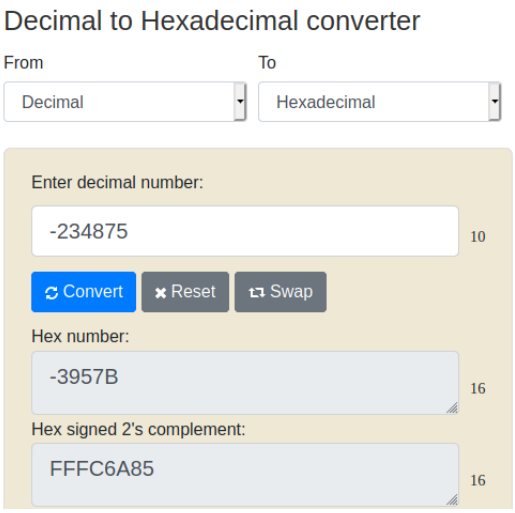
Kszqcas hc hvwg qcadshwhwcb! Vsfs wg hvs hslh hc hvs twfgh vozt ct hvs qvozzsbus: cgbyly

Beware of the witches! They will put a hex on you.

Solution:

1. Find the most suitable text which is (+14 shift), that gives us the first part of the flag `osnkxk`

2. Next, convert the negative decimal number to a hexadecimal, signed 2's complement representation, giving us the second part of the flag `FC6A85`



3. Get the last 6 digits to form the second part of the 12-character flag
4. Concatenate this second part of the flag with the first part

Flag:

`flag:osnkxkFC6A85`

R0 - Challenge 2

Theme: Steganography

Tool used:

- `ExifTool`: https://exiftool.org/
- `unzip`: https://linux.die.net/man/1/unzip

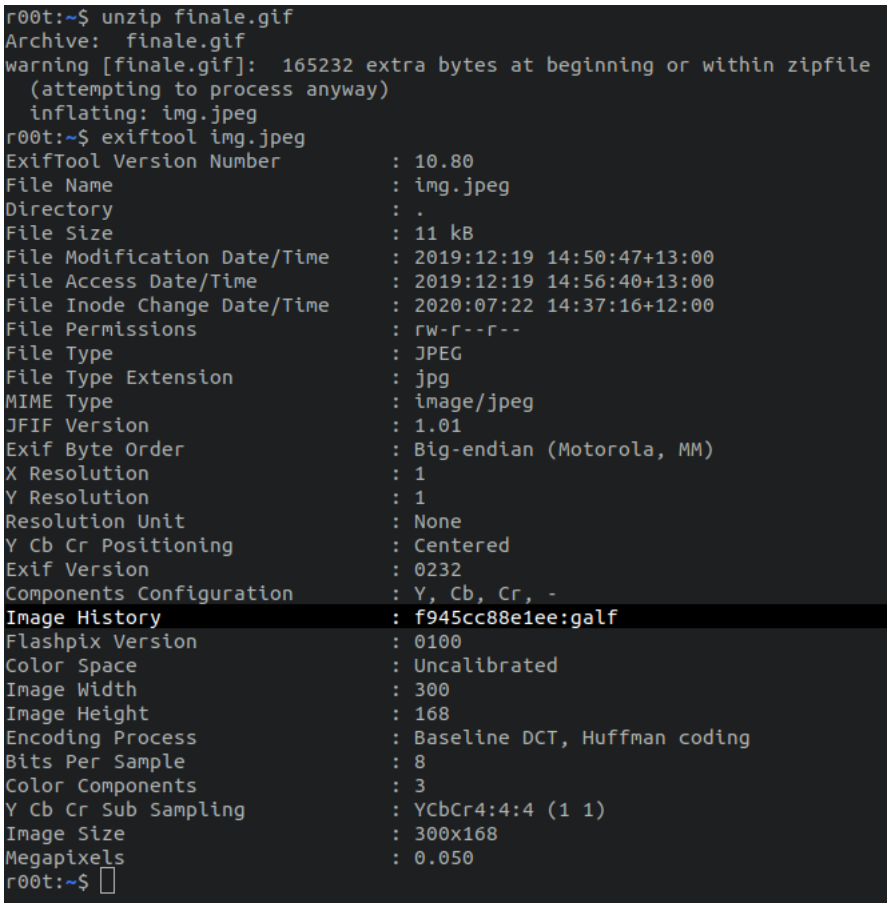
This challenge has a link to the file `Finale.gif`.

Solution:

1. Open the gif in ExifTool.

```
r00t:~$ exiftool finale.gif
ExifTool Version Number         : 10.80
File Name                       : finale.gif
Directory                       : .
File Size                       : 173 kB
File Modification Date/Time     : 2020:07:22 14:34:59+12:00
File Access Date/Time           : 2020:07:22 14:35:19+12:00
File Inode Change Date/Time     : 2020:07:22 14:35:12+12:00
File Permissions                : rw-rw-r--
File Type                       : GIF
File Type Extension             : gif
MIME Type                       : image/gif
GIF Version                     : 89a
Image Width                     : 220
Image Height                    : 193
Has Color Map                   : Yes
Color Resolution Depth          : 8
Bits Per Pixel                  : 8
Background Color                : 240
Animation Iterations            : Infinite
Comment                         : imgjpeg
Frame Count                     : 11
Duration                        : 1.63 s
Image Size                      : 220x193
Megapixels                      : 0.042
r00t:~$
```

2. In the `comment` section, there is a hint about the existence of an imgjpeg
3. Unzip the GIF to get an img.jpeg
4. Examine the img.jpeg using Exiftool



5. The flag can be found in the Image History section, by reversing the order of the characters.

Flag:

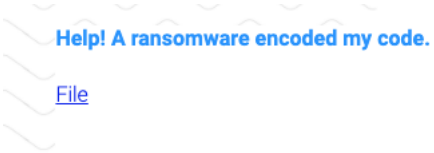
`flag:ee1e88cc549f`

R0 - Challenge 3

Theme: Reverse Engineering

Tool: JSF*ck

Participants are given an encoded file, which is encoded as a series of 6 characters: '(', ')', '!', '+', '[', ']'



Solution:

JSF*ck is an online educational programming style based on the atomic parts of JavaScript. It uses only six different characters to write and execute code. Alternatively, one could write a script to decode the file.

After running the code through the online tool, the flag can pops up as an `alert`.

Flag:

`flag:d382557fdab1`

R0 - Challenge 4

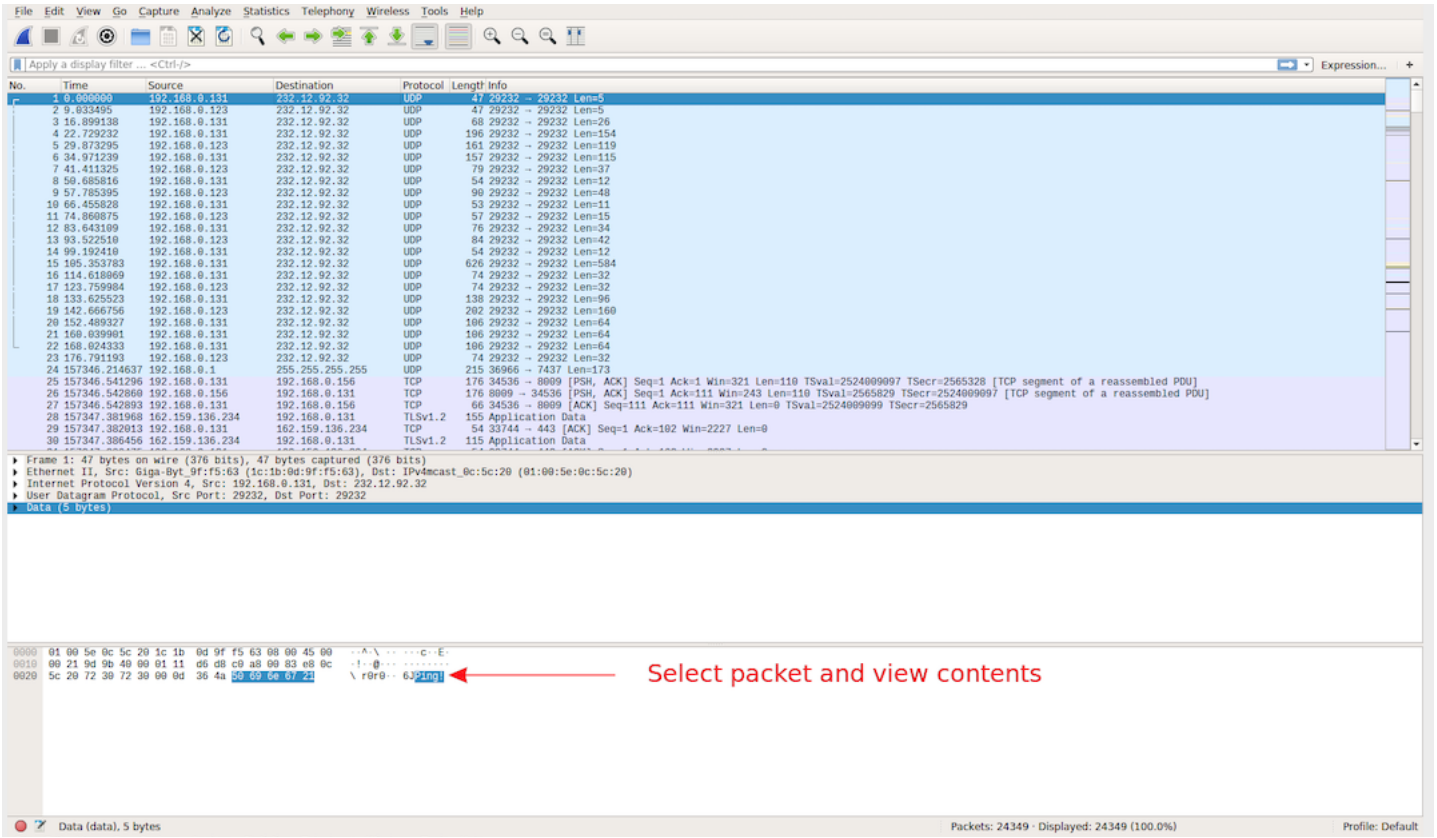
Theme: Network Traffic Analysis

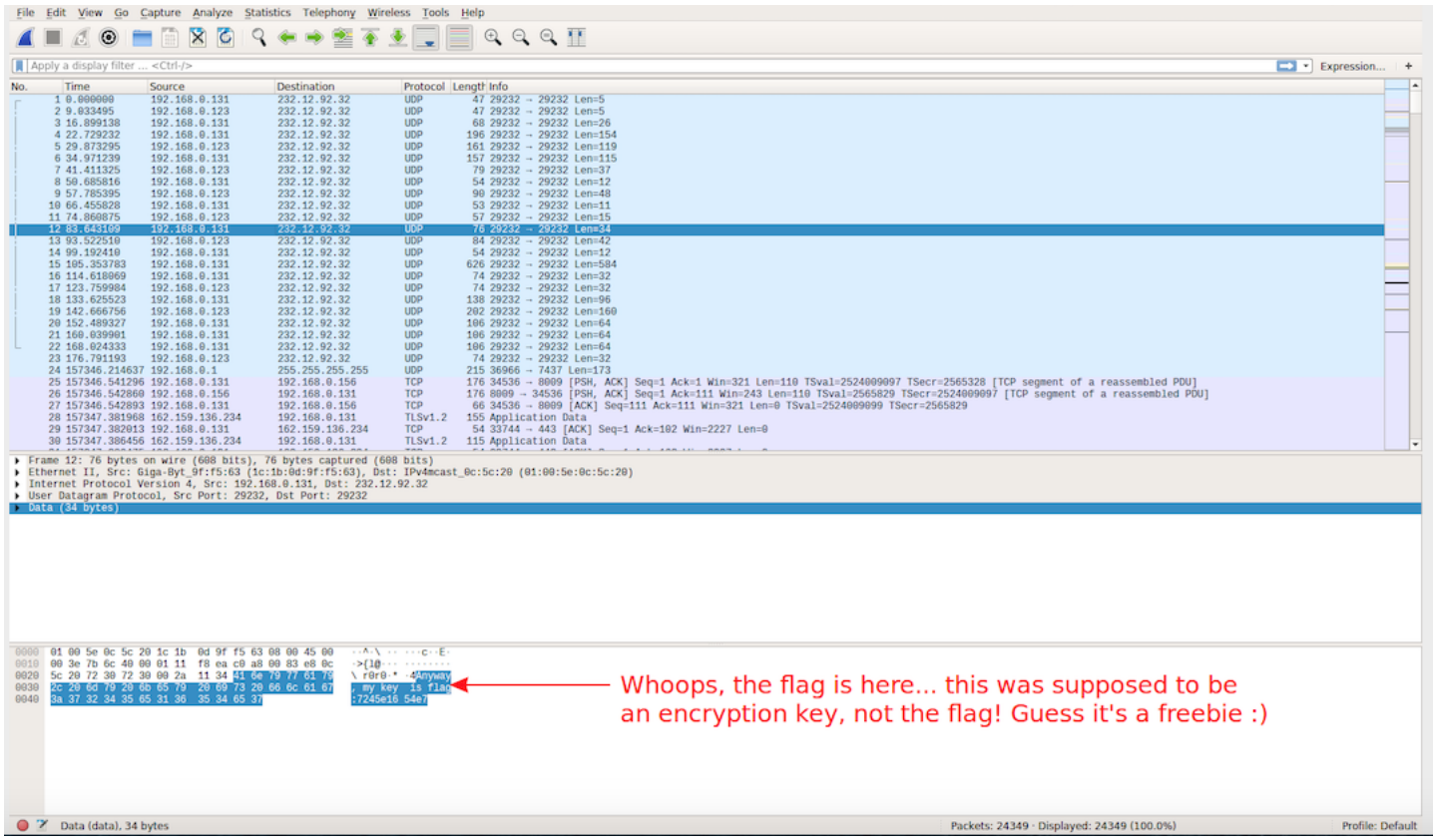
Tools:

- https://www.wireshark.org/

We intercepted this communication. We believe it has something you are looking for.

Click here for the File.





Flag:

`flag:7245e1654e7`

R0 - Challenge 5

Theme: Forensics

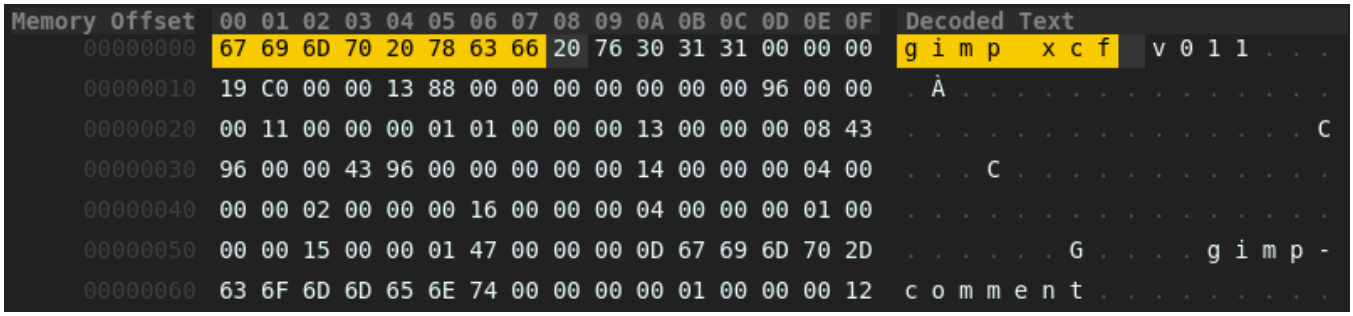
Tools:

- A hex-editor of your choice
- https://www.gimp.org/

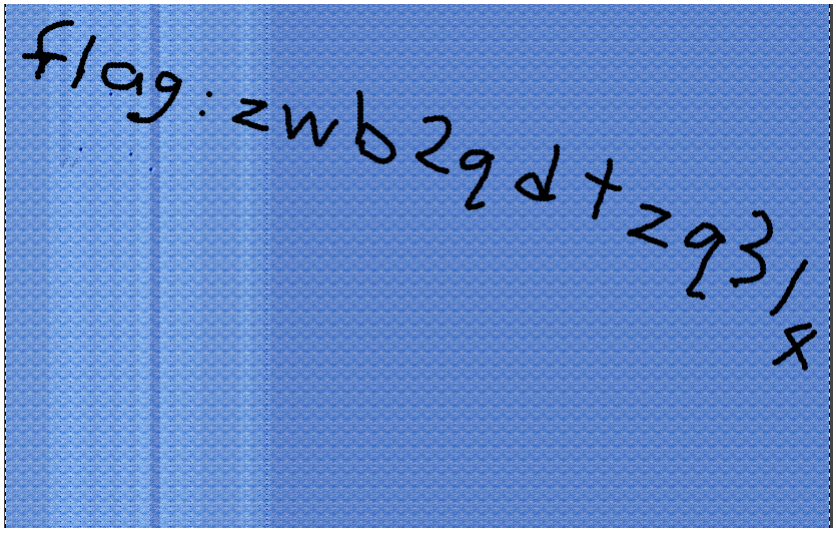
This challenge has a link to the file `img.xcf`. This is a corrupted image file whose header has been modified.

Solution:

Open the img.xcf file using a hex-editor, and search for the correct file header for xcf file (`67 69 6d 70 20 78 63 66 20`). Replace the file header with the correct value.



Open the `img.xcf` file using Gimp to obtain the flag.



Flag:

`flag:zwb2qdtzq314`

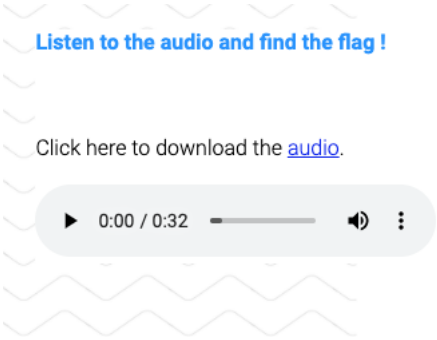
R0 - Challenge 6

Theme: Steganography

Tools:

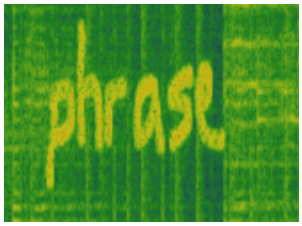
- Sonic Visualiser: https://sonicvisualiser.org/
- `steghide`: https://github.com/StefanoDeVuono/steghide

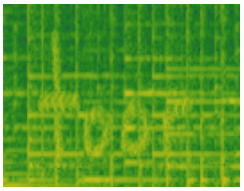
This challenge has a file called `FINAL.wav`, which is an audio file containing a clue to find the flag.



Solution:

Download and analyse the audio file using Sonic Visualiser. When analysing the audio, take note of the phrase "`toor`".





Next, open the command prompt and extract a secret text file. When prompted for a password, enter the phrase `toor`.

The secret text file contains the flag.

```
r00t:~$ steghide extract -sf FINAL.wav
Enter passphrase:
wrote extracted data to "secret.txt".
r00t:~$ cat secret.txt
flag:a37666fc86de
r00t:~$
```

Flag:

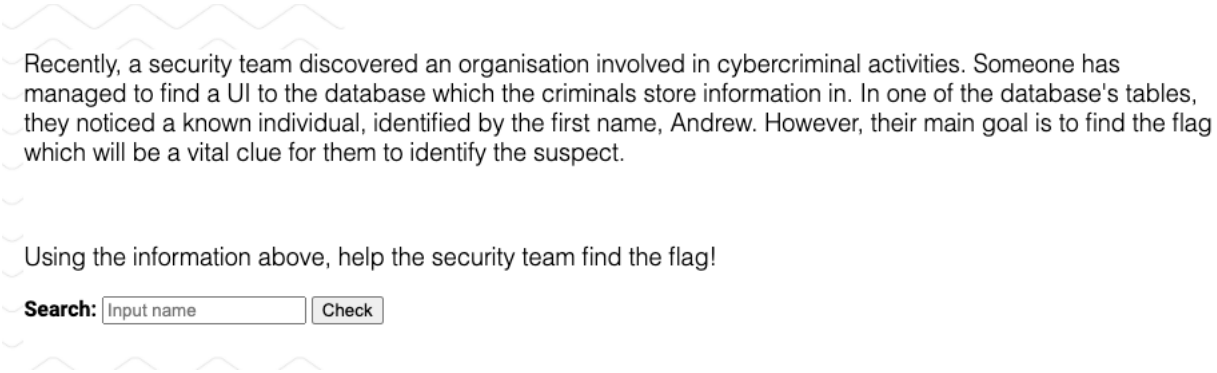
`flag:a37666fc86de`

R0 - Challenge 7

Theme: SQL Injection

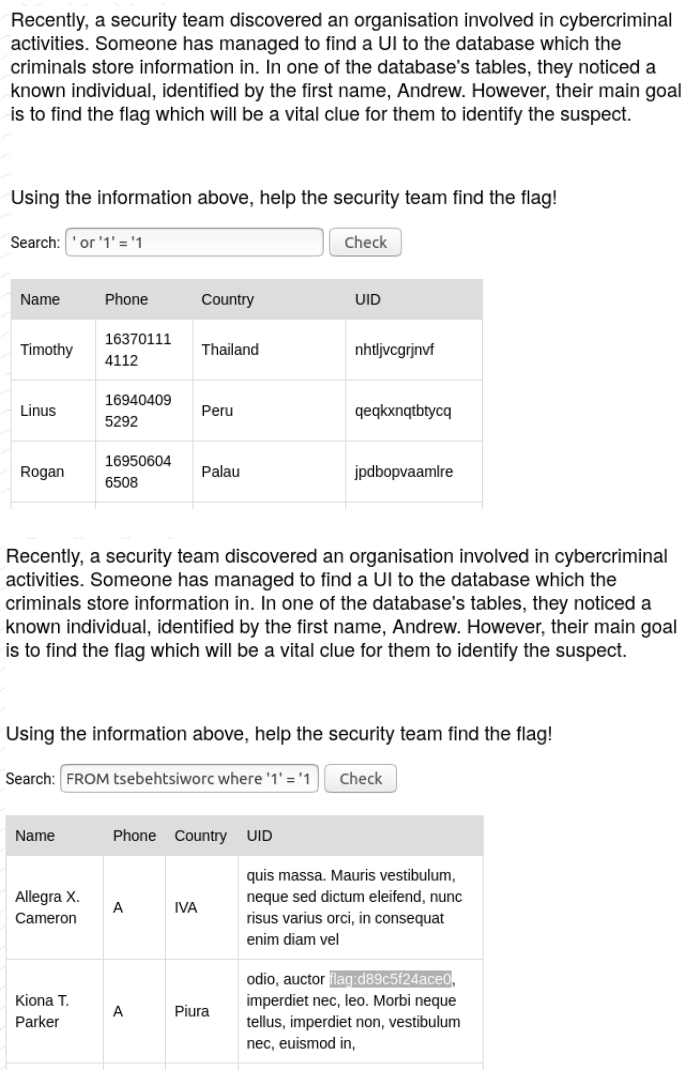
Tools Used:

None



Solution:

Perform SQL injection to the search box to get all the data from the table: `' or '1' = '1`



The UID columns represent all the different tables in the database

After trying all the tables, the correct table is `tsebehtsiworc`

The SQL injection which retrieves the flag is `‘ UNION SELECT * FROM tsebehtsiworc where ‘1’ = ‘1`

Flag:

`flag:d89c5f24ace0`

R0 - Challenge 8

Theme: Affine Cipher

Tools Used:

- https://www.dcode.fr/affine-cipher

This challenge involves steganography and encryption.

Upon downloading the image, we use the `strings` command to test whether the image contains a hidden element.

```
r00t:~$ strings linear.png | tail
T]]]^
Jgye
8Tom
vA'!
#U;`
OPXY
^#i'1
J@2+
IEND
aufz:menrtgzjrihm
r00t:~$
```

It can be seen that there is a string of the same format as a flag – `aufz:menrtgzjrihm`.

A brute force approach with the Caesar cipher will fail to retrieve the key. However, the name of the file hints at using a linear cipher.

An Affine cipher encrypts data using a linear equation of the form `E(x) = ax + b mod m`. This matches the form of the equation in the image: `E(x) = 25x + 5`.

Since the format of the flag only contains lower case alphabetic characters, the value of `m` should be 26. This results in the equation `E(x) = 25x + 5 mod 26`, which can be easily solved using a tool such as https://www.dcode.fr/affine-cipher.

Flag:

`flag:tbsomzgwoxyt`