TryHackMe: Mr. Phisher

The following writeup covers the Mr. Phisher room on TryHackMe. This room involves analysing an email with a weird attachment to find the flag.

The file we are provided with is a Microsoft Word macro-enabled document. There are tool like Olevba which are great for analysing Macro enabled documents, however, in this room we aren't provided with such tools. Therefore, I opened up the MrPhiser.docm document in LibreOffice Writer:
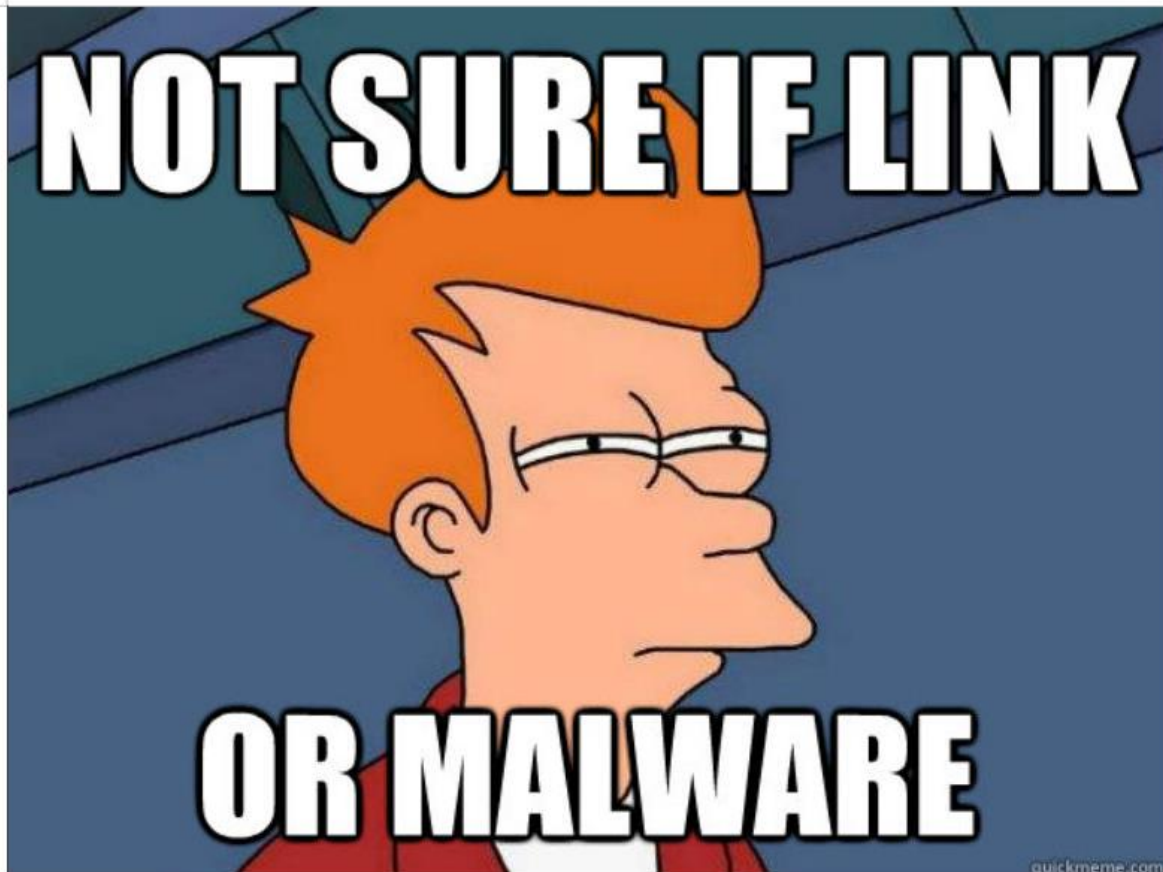
There is nothing useful to use in the document, we are only concerned with the Macros:
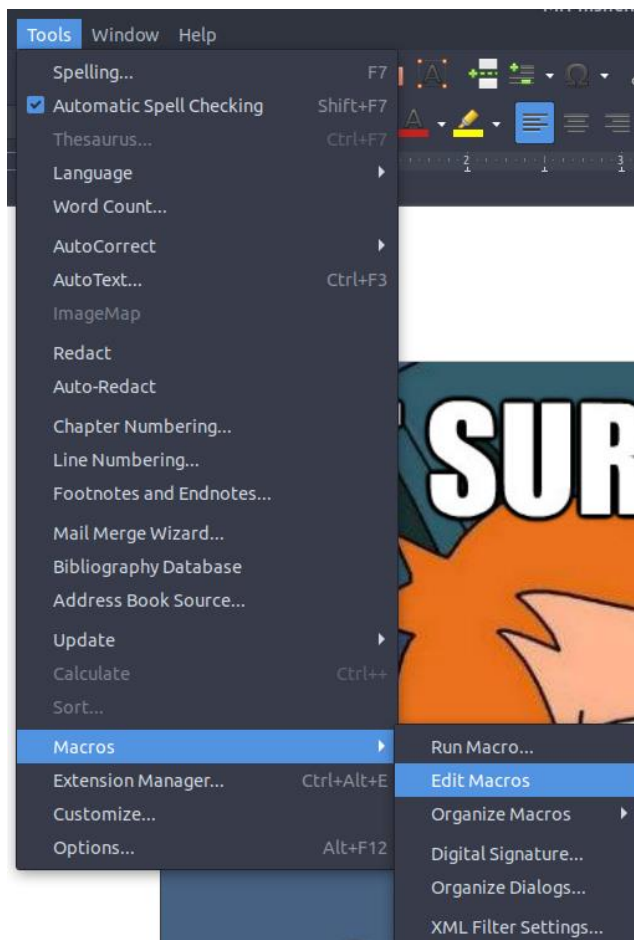
After exploring the folders, we have found a Macro:
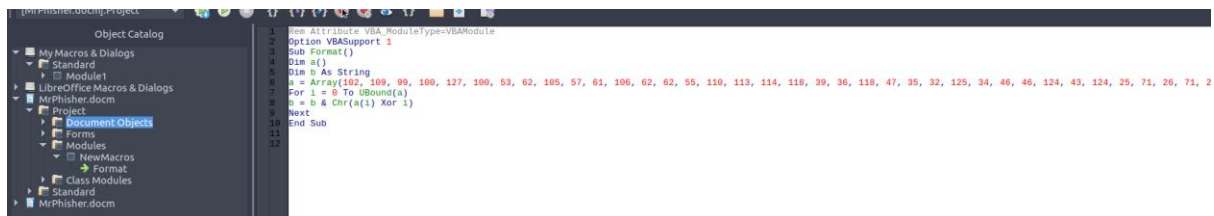
As you can see in the Macro, it is written using Visual Basics. I have no experience with Visual Basic, therefore with the help of my friend GPT 4o, I was able to create a Python script that performs the same operations as the VB code:

```
>>> # Array from the VBA code
>>> a = [102, 109, 99, 100, 127, 100, 53, 62, 105, 57, 61, 106, 62, 62, 55, 110, 113, 114, 118, 39, 36, 118, 47, 35, 32,
 125, 34, 46, 46, 124, 43, 124, 25, 71, 26, 71, 21, 88]
>>>
>>> # Decrypt the string
>>> b = ""
>>> for i in range(len(a)):
...     b += chr(a[i] ^ i)
...
>>> print(b)
flag{a39a07a239aacd40c948d852a5c9f8d1}
```