DEEP RED DUST - MISC 200

Armstrong, the Astronaut-in-Chief has sent an email saying he's leaving the Mars mission. This is very odd, especially as Armstrong has spent decades working on the project. His email contains an attachment in an unknown format. What is it? R-boy must dig deeper to find out what's going on – help him investigate.

```
$ file Deep_Red_Dust
Deep_Red_Dust: data

$ binwalk Deep_Red_Dust
DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
-----
94            0x5E            Zlib compressed data, default compression
1112488       0x10F9A8        Zip archive data, encrypted at least v2.0 to
extract, compressed size: 34029, uncompressed size: 37936, name:
Goodbye.docm
1146685       0x117F3D        End of Zip archive
```

The original file was a PNG + ZIP. The ZIP was ok and we extracted it with foremost and tried to unzip it but a password was required.

The PNG was corrupted the magic number (first 4 bytes) was 0x52424F59 (“RBOY”) instead of 0x89504E47. So we fixed it so we were able to open the image and inside we found, written on the sand, the password for the ZIP.

So we used the password *K33pItS3cr3t* that was in the image in order to extract the zip content: a word file with macro.
We extracted the macro:

```
Private Sub CommandButton1_Click()
If Not (TextBox1.TextLength = 0) Then
Dim tbox As String
tbox = TextBox1.Text
Dim encrypt As Variant
encrypt = Array(52, 54, 60, 40, 72, 64, 42, 35, 93, 26, 38, 110, 3,
47, 56, 26, 64, 1, 49, 33, 71, 38, 7, 25, 20, 92, 1, 9)
Dim inputChar() As Byte
```

```
inputChar = StrConv(tbox, vbFromUnicode)
Dim plaintext(28) As Variant
Dim i As Integer
For i = 0 To 27
plaintext(i) = inputChar(i Mod TextBox1.TextLength) Xor encrypt(i)
Next
MsgBox "Congrats!!"
End If
End Sub
```

The message was ciphered with a simple xor with the key passed using TextBox1.
Flags always starts with {FLG: so we can extract the key's first five characters using the xor associative property: Oppor.
After some tries we thought that the key could be Opportunity, a martian rover, and it was the right guess. Xoring the key with encrypt variable and got the flag

{FLG:4_M4n_!s_Wh4t_H3_Hid3s}