Codefest CTF 2018

Problem: Intercept (200, Forensics)
Garry encrypted a message with his public key and mailed it to Monika. Sure Garry is an idiot. The intercepted mail is given below as seen from Monika's side. Decrypt the message to get the key.

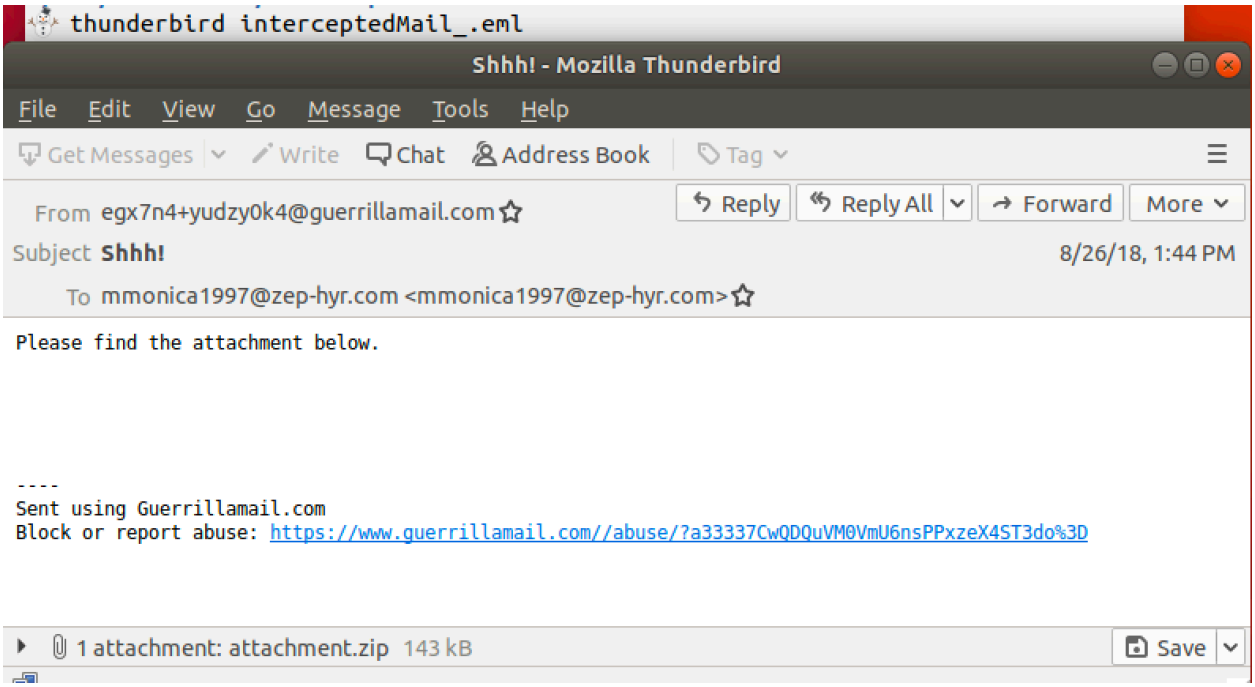
interceptedMail.eml

Output Format
CodefestCTF{flag}

Solution:
After downloading the file provided, I first examine it using the **file** command:

```
file interceptedMail_.eml
interceptedMail_.eml: RFC 822 mail, ASCII text, with CRLF line terminators
```

Running the **strings** command on the file gives nothing useful. Knowing that it is a .eml extension and confirming that it is a saved mail file with the **file** command, I opened it with the default mail client in Ubuntu which is **Thunderbird**:



There is an attachment in the mail, so it is downloaded and examined it with the **file** command:

```
ls
attachment.zip  interceptedMail_.eml
~/ctf/codefest18/intercept
file attachment.zip
attachment.zip: Zip archive data, at least v2.0 to extract
```

The **unzip** command is used to extract the contents:

```
unzip attachment.zip
Archive:  attachment.zip
  inflating: flag.enc
  inflating: Public_Key_Encryption_.docx
~/ctf/codefest18/intercept
ls
attachment.zip  flag.enc  interceptedMail_.eml  Public_Key_Encryption_.docx
```

Both the **flag.enc** and **Public_Key_Encryption.docx** files are then examined with the **file** command:

```
file flag.enc
flag.enc: data
~/ctf/codefest18/intercept
file Public_Key_Encryption_.docx
Public_Key_Encryption_.docx: Zip archive data, at least v2.0 to extract
```

Knowing that a Word document file is a zip archive, the **unzip** command can be used to extract the contents. Running the **strings** command didn't give any useful information other than the file hierarchy paths of the Word document file. So, the document is first opened using **libreoffice** command and it looks like it is a document explaining Public Key Encryption. Using the **unzip** command on the document file, I navigated to the **word/media** folder since it contains the images used in the document. This would be a good place to look for any **Steg** that may have been used, before navigating to other file paths. They are confirmed to be image files with the **file** command:

```
file image*
image1.png: PNG image data, 603 x 404, 8-bit/color RGBA, non-interlaced
image2.png: PNG image data, 525 x 513, 8-bit/color RGBA, non-interlaced
image3.png: PNG image data, 380 x 570, 8-bit/color RGBA, non-interlaced
~/ctf/codefest18/intercept/word/media
```

I then use the **strings** command on the **image1.png** file:

```
j/Y+
IEND
-----BEGIN
 PRIVATE KEY-----
MIIEpQIBAAKCAQEAwi6zjwdY8hkkQSdzCTp7guXaGVLkH1K+tQrzAELr82mOdlqr
WE0qhrjzliWhCM+jg8ruVmWf1sw2J2YqR6G5gXFF/+f3LEYgAhgZz3yBSLpPcxcO
tI2Lqyyka3Pv8FmvrwbPFP8ZkQxKrz2YC1vYgu9TGLfciq3EOMT7aV7XnU0u+7Vi
HdL1GM2nVtwfxQHIWL+awuxhv9nqd0rBuy9lu5XipJKRXITW4rVD38qKAU/DPSiN
F1RV9iUON3TjMiAi8Z3jtESB7IXoFlpAvpqtrmXjVt+hHPBZAXMUHCB66E3upXz2
JrsucK+s7D1T+8v29C5kUlecGZ37rDvZ30kq+wIDAQABAoIBAQCtFhXFqyX0fsab
MP/QPQn1Ls8OfZ2L8iS9manrFLvfN7rd8ooC5p2+gsPVlWsKQJMfGdcCugkU3Oh0
jBOp0BVbtU1RA0KGe2dylmsDUJao7jF9hBL+i6DwjpVslmZMlpUL7YTO0WjHqu4z
cDLEBTVj2NH4GYODNcrPU35KeVi2A5W/xdErMY41wFVJVUe1XsRztjM4DFxBu4oO
10XCdZIEGfLqSwhlfvDMweNXxIx/dQYSjDyzzTr0LT/elXxLOHT4bQ9d46qQWBew
12dwffijlg3Gr1/0R+s27TvHCbd1w4KNdW+XtH2lY6m515C/4LI8eeworMKyF8JN
y0sbouuZAoGBAOjdmsmws95UMfIlMGFIY9cw5k3Q+rlcRC0Ys9JlLz9V6xaNLHPK
ysg7pP4rqjZJ4q4QVKCBJaOxPo2TSOXnYflc57JXubIi+O+pOmZZsiY5AslcEPwS
geJM7aW5HXYfssWm5habIhE/mayu6TV1PMa8MlBn34lxTHLG8Gx3EQBPAoGBANV5
R3zhEJYQNGUt6IxR5XdRNvoDfPTGto9AxoPf7D5aJpMn2scXXhSdI5kESrqWFVjW
6EmdF/QQIMYH+PMQo6GYPmHMk0I8K72QThSinQ1tTZrTDyhsVjJhsa0R3gISwSc2
BnsmoT76zRwgT+w8qKzb4aiZkEmrQcvVKksYF/OVAoGBAJwjUtFfyQsPOzoYk3r3
VfKJGDMfJ6433oK6aIBvViHKk0nYuPCfDh76VyQR1Rx3qCV8T7IbRkie5Ml680ss
PTY9hCHBzoJSDsZrmvvbsqcMXQD02XKbWjmJyWLwX3+/u1fqE6cet9YG5hyyXy54
AJtkvvvI2krHDDJ9j+G6aEzjAoGAeaxYrLrzYzT1SD40b9Y1/h4SQco/LJ0ebOQ0
wfGdi6SCnBl5P0T4YLN4GL0zgsoMfMhxOZQKlRekNntQz+nJ+k72L3QU8wmsvK1F
c8mDzqVgOEDYQOgO8URxqv2mFnRuF1VZuFO6UFVPFxrrsvCYC36ATkLI1NSB+hYT
tx2SeUkCgYEAyydGPEYC8jfzRhTc5IdmJ181f5e4k1pjrT/NCmIwDR1G6UZDr+qK
udVV2UEL/hUSRE51nu0i1skdktBDkknIiMTyCZWM+05tZCGn93w2EUAm+5ujozdX
j/Y3ilCR0pbf+mgR225qVBXgqwVd0zbwlfLHqFLZpY6XWD5tQ8vUEMY=
-----END RSA PRIVATE KEY-----
```

An RSA private key is hidden in the image with a minor format error. The key is copied and saved to **prkey.pem** file, and stored in the same path where **flag.enc** file is, with the first line correctly formatted as follows:

```
-----BEGIN RSA PRIVATE KEY-----
```

The **openssl** command is used as follows:

```
openssl rsautl -decrypt -in flag.enc -out flag.dec -inkey prkey.pem
```

Yielding the flag:

```
~/ctf/codefest18/intercept
openssl rsautl -decrypt -in flag.enc -out flag.dec -inkey prkey.pem
~/ctf/codefest18/intercept
ls
 attachment.zip          docProps    interceptedMail_.eml          _rels
'[Content_Types].xml'    flag.dec    prkey.pem                     word
 customXml               flag.enc    Public_Key_Encryption_.docx
~/ctf/codefest18/intercept
cat flag.dec
The flag is kristeinStewart_is_5EXY~/ctf/codefest18/intercept
```

Flag:
CodeFest{kristeinStewart_is_5EXY}