

# SM4 加密北大 logo

## 实验思路：

sm4 的输入是二进制流，实验的图片是 .jpg 格式，先将它转化为 .rgba 格式的图片。然后用 gmssl 库的加密算法对 .rgba 格式的图片加密，然后在利用工具将其转回 .jpg 格式。原图如下：




## 实验步骤：

1. 利用 python 的 PIL 的库将将原材料转化为 rgba

```
EncPKUlogo.py x
1  from PIL import Image
2
3  pku = Image.open('pkulogo.jpg')
4  pku_rgba = pku.convert('RGBA')
5  pku_rgba.save('pkulogo_rgba')
```

2. 利用 gmssl 给 .rgba 格式的图片加密

```
yz@yz-virtual-machine:~/PycharmProjects/SM4$ source ~/.profile
yz@yz-virtual-machine:~/PycharmProjects/SM4$ gmssl
GmSSL> ^C
yz@yz-virtual-machine:~/PycharmProjects/SM4$ gmssl
GmSSL> ^C
yz@yz-virtual-machine:~/PycharmProjects/SM4$ gmssl enc -sms4 -ecb -in pkulogo.rgba -out pkulogo_ecb.rgba
enc: Unknown cipher ecb
enc: Use -help for summary.
yz@yz-virtual-machine:~/PycharmProjects/SM4$ gmssl enc -sms4 -ecb -e -in pkulogo.rgba -out pkulogo_ecb.rgba
enc: Unknown cipher ecb
enc: Use -help for summary.
yz@yz-virtual-machine:~/PycharmProjects/SM4$ gmssl enc -sms4-ecb -e -in pkulogo.rgba -out pkulogo_ecb.rgba
enter sms4-ecb encryption password:
Verifying - enter sms4-ecb encryption password:
yz@yz-virtual-machine:~/PycharmProjects/SM4$
```



pkulogo\_ecb.rgba

3. 利用工具将.rgba 转成.jpg，显示结果如下：

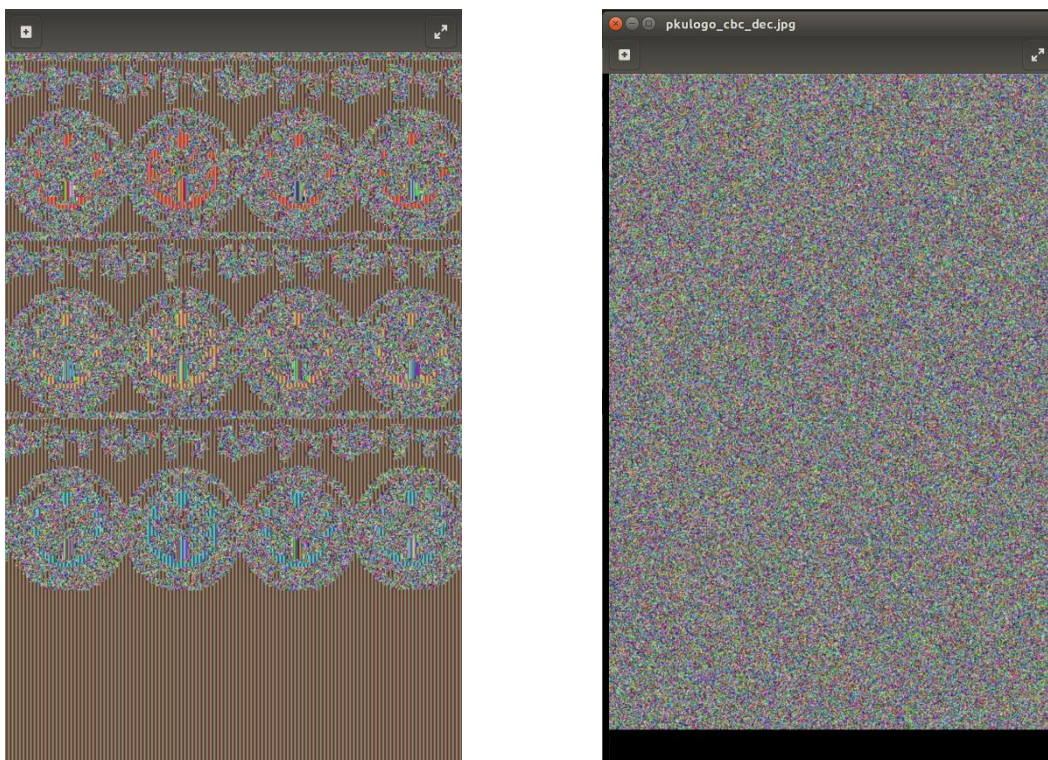


图 1 ecb 加密图片（左）和 cbc 加密图片（右）

## 实验结果：

观察加密结果发现，ecb 加密的图片仍然有迹可循，但是 cbc 加密的图片完全没有痕迹。