用 SM4 的 ECB 模式和 CBC 模式加密图片

-

首先在 Linux 系统下安装 gmssl 和 ImageMagick

gmssl：

```
$ ./config no-saf no-sdf no-skf no-sof no-zuc
    $ make
    $ sudo make install
```

ImageMagick：

```
sudo  apt-get install imagemagick
```

选择的北大 logo 如下所示：

用 ImageMagick 的 convert 把 JPG 格式换成 RGBA 格式：

```
convert -depth 8 logo.jpg logo.rgba
```

接着使用 gmssl，分别用 ECB 和 CBC 模式进行加解密：

ECB：

```
加密 gmssl enc -sms4-ecb -e -in logo.rgba -out logo-ecb.rgba
解密 gmssl sms4-ebc -d -in logo-ecb.rgba -out logo-ecb-dec.rgba
```

CBC：

```
加密 gmssl enc -sms4-cbc -e -in logo.rgba -out logo-cbc.rgba
解密 gmssl sms4-cbc -d -in logo-cbc.rgba -out logo-cbc-dec.rgba
```

我们得到加密和解密得到的都是 RGBA 格式的图像，为了得到 JPG 的图像，还需要再进行 convert 转换。

进行转换前，首先我们需要知道 logo.jpg 的宽和高，利用

```
#identify logo.jpg
```

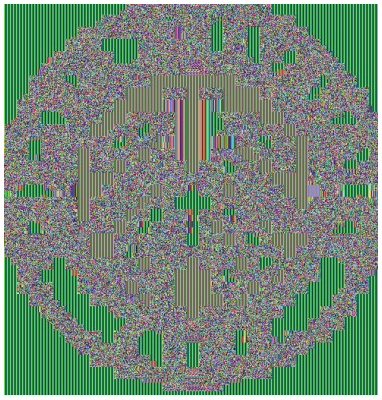
得到图像为 500×421，则可以进行转换：

```
convert -size 720x720 -depth 8 logo-ecb.rgba logo-ecb.jpg
convert -size 720x720 -depth 8 logo-cbc.rgba logo-cbc.jpg
```

最终得到图像：

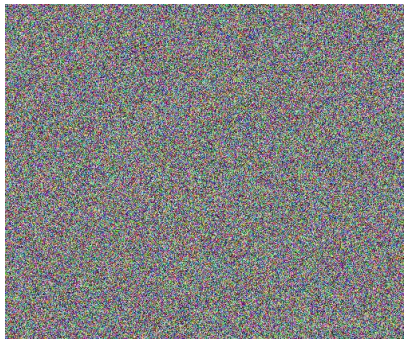
EBC 模式：

加密的 key 为：12345678



CBC 模式：

加密的 key 为：12345678



过程中所有的图片列表：