

第二次编程作业实验报告

刘曼姝 1901210656 2019.10.24

一、 实验目的与要求：

使用基于 ECB 模式和其他模式的 SM4 算法加密北京大学校徽。

二、 实验设备、系统环境与软件：

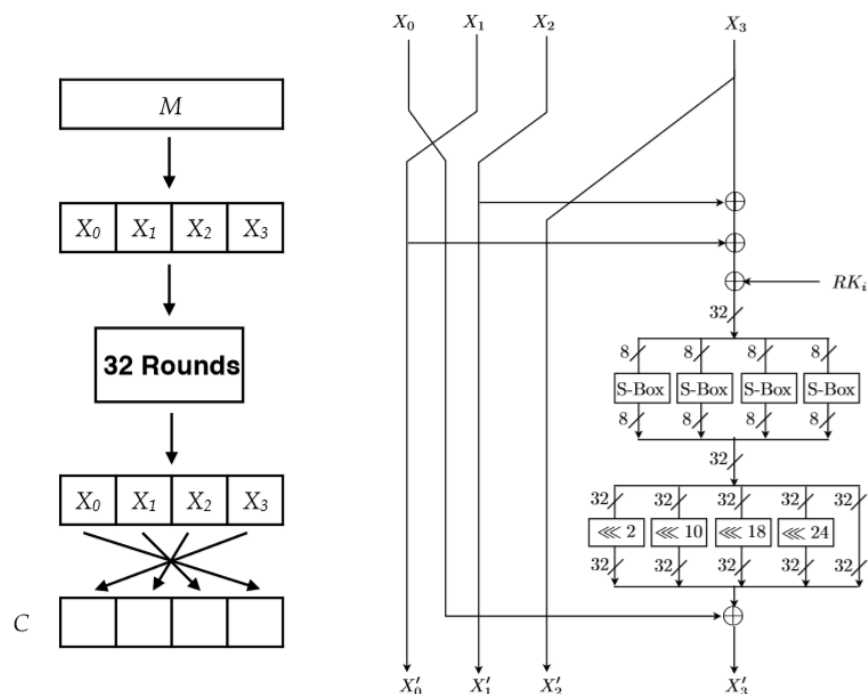
Windows 10 64 位操作系统的笔记本电脑，安装了 ActivePerl 5.20.2、Visual Studio 2019、GmSSL 2.5.4、Notepad++、ImageMagick-7.0.8-Q16。

三、 实验原理：

1、 SM4 算法

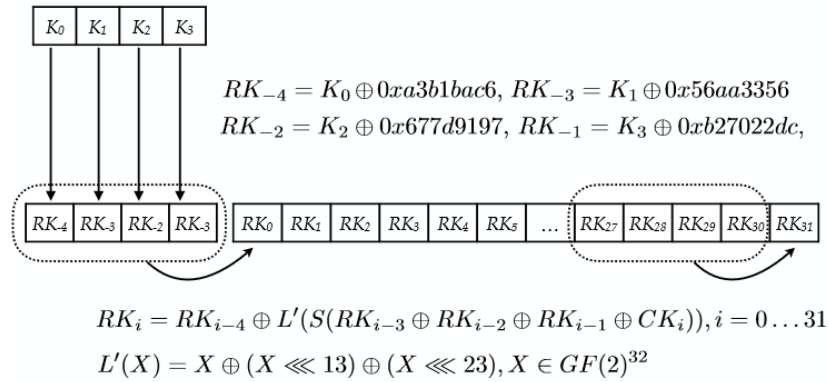
SM4 原名是 SMS4，是一种作为国家标准的分组密码算法。它采用 32 轮非平衡 Feistel 结构，具有 128bit 的密钥长度和分组长度。

其加密过程如下：



其中的 S-盒和密钥调度算法如下：

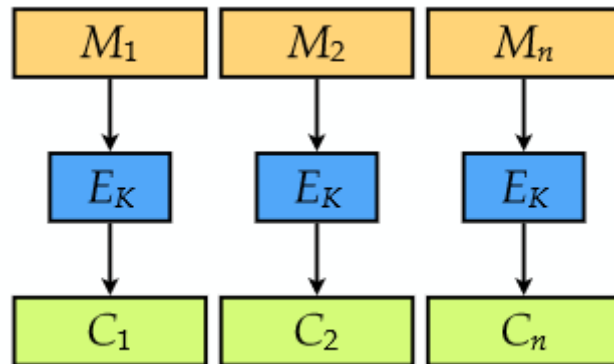
	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
00	d6	90	e9	fe	cc	e1	3d	b7	16	b6	14	c2	28	fb	2c	05
10	2b	67	9a	76	2a	be	04	c3	aa	44	13	26	49	86	06	99
20	9c	42	50	f4	91	ef	98	7a	33	54	0b	43	ed	cf	ac	62
30	e4	b3	1c	a9	c9	08	e8	95	80	df	94	fa	75	8f	3f	a6
40	47	07	a7	fc	f3	73	17	ba	83	59	3c	19	e6	85	4f	a8
50	68	6b	81	b2	71	64	da	8b	f8	eb	0f	4b	70	56	9d	35
60	1e	24	0e	5e	63	58	d1	a2	25	22	7c	3b	01	21	78	87
70	d4	00	46	57	9f	d3	27	52	4c	36	02	e7	a0	c4	c8	9e
80	ea	bf	8a	d2	40	c7	38	b5	a3	f7	f2	ce	f9	61	15	a1
90	e0	ae	5d	a4	9b	34	1a	55	ad	93	32	30	f5	8c	b1	e3
a0	1d	f6	e2	2e	82	66	ca	60	c0	29	23	ab	0d	53	4e	6f
b0	d5	db	37	45	de	fd	8e	2f	03	ff	6a	72	6d	6c	5b	51
c0	8d	1b	af	92	bb	dd	bc	7f	11	d9	5c	41	1f	10	5a	d8
d0	0a	c1	31	88	a5	cd	7b	bd	2d	74	d0	12	b8	e5	b4	b0
e0	89	69	97	4a	0c	96	77	7e	65	b9	f1	09	c5	6e	c6	84
f0	18	f0	7d	ec	3a	dc	4d	20	79	ee	5f	3e	d7	cb	39	48



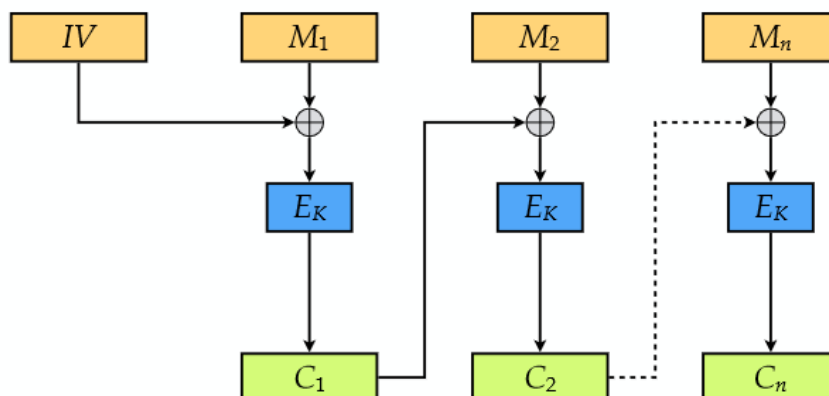
2、加密模式

加密模式分为以下 5 种：

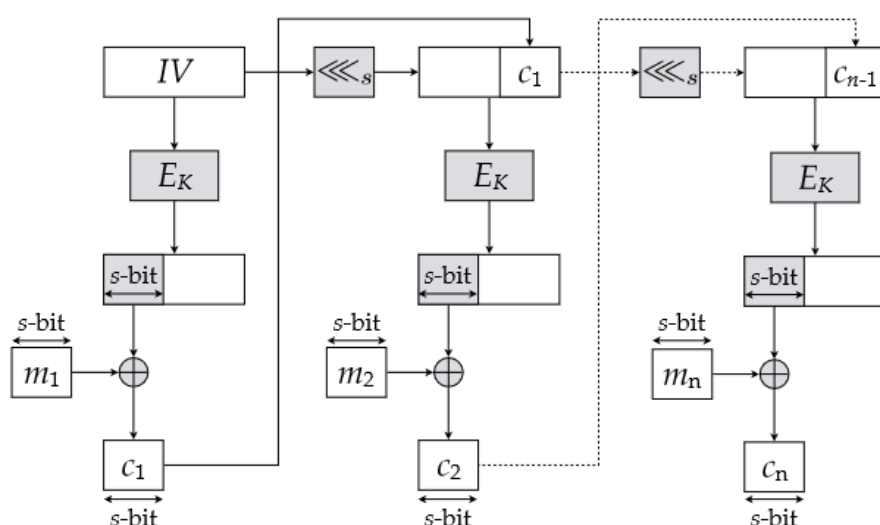
(1) ECB (Electronic Codebook) mode，电子密码本模式：



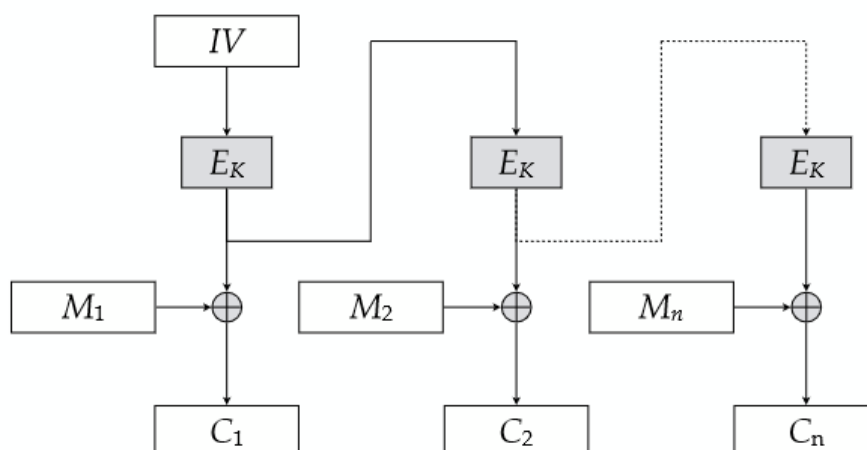
(2) CBC (Cipher Block Chaining) mode，密文分组链接模式：



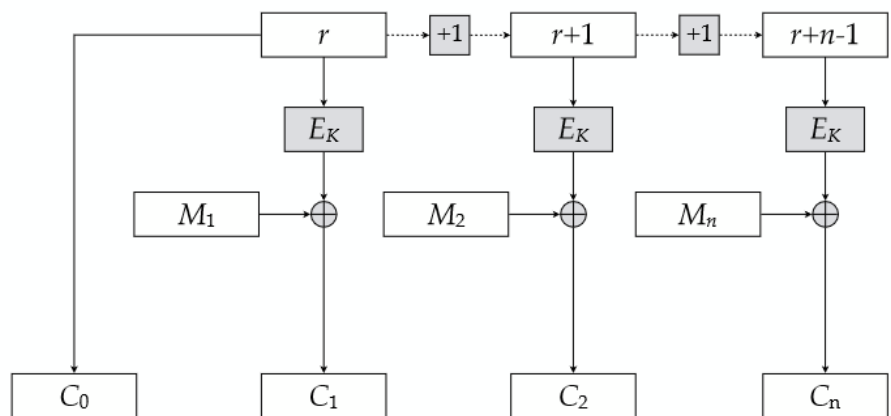
(3) CFB (Cipher Feedback) mode, 密文反馈模式:



(4) OFB (Output Feedback) mode, 输出反馈模式:



(5) CTR (Counter) mode, 计数器模式:



5 种加密模式的比较如图所示^[1]:

模式	名称	优点	缺点	备注
ECB 模式	Electronic CodeBook 电子密码本模式	<ul style="list-style-type: none"> 简单 快速 支持并行计算 (加密、解密) 	<ul style="list-style-type: none"> 明文中的重复排列会反映在密文中 通过删除、替换密文分组可以对明文进行操作 对包含某些比特错误的密文进行解密时, 对应的分组会出错 不能抵御重放攻击 	不应使用
CBC 模式	Cipher Block Chaining 密文分组链接模式	<ul style="list-style-type: none"> 明文的重复排列不会反映在密文中 支持并行计算 (仅解密) 能够解密任意密文分组 	<ul style="list-style-type: none"> 对包含某些错误比特的密文进行解密时, 第一个分组的全部比特以及后一个分组的相应比特会出错 加密不支持并行计算 	推荐使用
CFB 模式	Cipher-FeedBack 密文反馈模式	<ul style="list-style-type: none"> 不需要填充 (padding) 支持并行计算 (仅解密) 能够解密任意密文分组 	<ul style="list-style-type: none"> 加密不支持并行计算 对包含某些错误比特的密文进行解密时, 第一个分组的全部比特以及后一个分组的相应比特会出错 不能抵御重放攻击 	<ul style="list-style-type: none"> 现在已不使用 推荐用 CTR 模式代替
OFB 模式	Output-FeedBack 输出反馈模式	<ul style="list-style-type: none"> 不需要填充 (padding) 可事先进行加密、解密的准备 加密、解密使用相同结构 对包含某些错误比特的密文进行解密时, 只有明文中相对应的比特会出错 	<ul style="list-style-type: none"> 不支持并行计算 主动攻击者反转密文分组中的某些比特时, 明文分组中相对应的比特也会被反转 	推荐用 CTR 模式代替
CTR 模式	CounTeR 计数器模式	<ul style="list-style-type: none"> 不需要填充 (padding) 可事先进行加密、解密的准备 加密、解密使用相同结构 对包含某些错误比特的密文进行解密时, 只有明文中相对应的比特会出错 支持并行计算 (加密、解密) 	主动攻击者反转密文分组中的某些比特时, 明文分组中相对应的比特也会被反转	推荐使用

https://blog.csdn.net/qq_42940832

四、 实验步骤与设计思路:

1、 下载了一张 220x220 像素的北京大学校徽的图片, 格式为 “.png”, 命名为 “logo.png”:



2、 下载并安装 ImageMagick:

modules	2019/10/15 15:27	文件夹	
PerlMagick	2019/10/15 15:27	文件夹	
uninstall	2019/10/15 15:27	文件夹	
www	2019/10/15 15:27	文件夹	
ChangeLog.txt	2019/10/5 7:56	文本文档	75 KB
coder.xml	2019/10/5 7:56	XML 文档	1 KB
colors.xml	2019/10/5 7:56	XML 文档	2 KB
compare.exe	2019/10/5 8:08	应用程序	41 KB
composite.exe	2019/10/5 8:08	应用程序	41 KB
configure.xml	2019/10/5 7:58	XML 文档	1 KB
conjure.exe	2019/10/5 8:08	应用程序	41 KB
convert.exe	2019/10/5 8:08	应用程序	41 KB

3、 使用 ImageMagick 的 convert 命令，将 “logo.png” 转换为 rgba 格式的 “logo.rgba”，命令如下：

set path=C:\Program Files\ImageMagick-7.0.8-Q16;%path%;

magick convert -depth 32 C:\Users\0\Desktop\logo.png C:\Users\0\Desktop\logo.rgba

在桌面生成 “logo.rgba” 文件：



C:\Users\0\Desktop\logo.rgba - Notepad++

文件(F) 编辑(E) 搜索(S) 视图(V) 编码(N) 语言(L) 设置(T) 工具(O) 宏(M) 运行(R) 插件(P) 窗口(W) ?

change.log x logo.rgba x 四世同堂.txt x new 1 x logo-ecb.rgba x

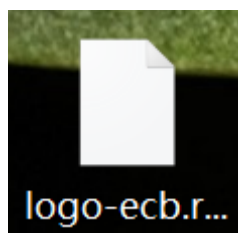
Address	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
00000000	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff
00000010	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff
00000020	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff
00000030	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff
00000040	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff
00000050	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff

4、使用 gmssl 的 ECB 模式的 SM4 算法对“logo.rgba”进行加密，密钥为“P@ssw0rd”，输出为“logo-ecb.rgba”文件，命令如下：

```
set path=C:\Windows\SysWOW64\apps;%path%;
```

```
gmssl enc -sms4-ecb -e -in C:\Users\0\Desktop\logo.rgba -out C:\Users\0\Desktop\logo-ecb.rgba -k P@ssw0rd
```

在桌面生成“logo-ecb.rgba”文件：



C:\Users\0\Desktop\logo-ecb.rgba - Notepad++

文件(F) 编辑(E) 搜索(S) 视图(V) 编码(N) 语言(L) 设置(T) 工具(O) 宏(M) 运行(R) 插件(P) 窗口(W) ?

change.log x logo.rgba x 四世同堂.txt x new 1 x logo-ecb.rgba x

Address	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
00000000	53	61	6c	74	65	64	5f	5f	62	e8	42	02	a9	7b	7e	dc
00000010	bf	9c	52	de	e6	c2	f7	ef	a4	53	34	5a	0d	c4	56	63
00000020	bf	9c	52	de	e6	c2	f7	ef	a4	53	34	5a	0d	c4	56	63
00000030	bf	9c	52	de	e6	c2	f7	ef	a4	53	34	5a	0d	c4	56	63
00000040	bf	9c	52	de	e6	c2	f7	ef	a4	53	34	5a	0d	c4	56	63
00000050	bf	9c	52	de	e6	c2	f7	ef	a4	53	34	5a	0d	c4	56	63

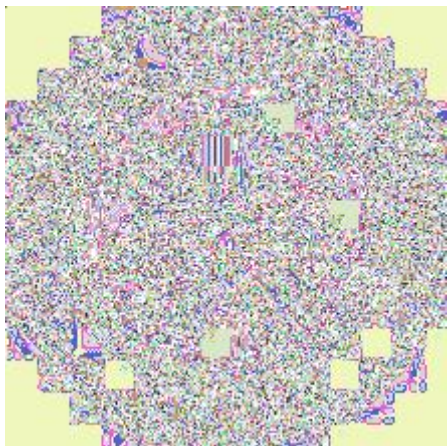
5、使用 ImageMagick 的 convert 命令，将“logo-ecb.rgba”转换回 png 格式的“logo-ecb.png”，命令如下：

```
magick convert -size 220x220 -depth 32 C:\Users\0\Desktop\logo-ecb.rgba
```

```
C:\Users\0\Desktop\logo-ecb.png
```

在桌面生成“logo-ecb.png”文件，即为基于 ECB 模式下的 SM4 算法加密后的北

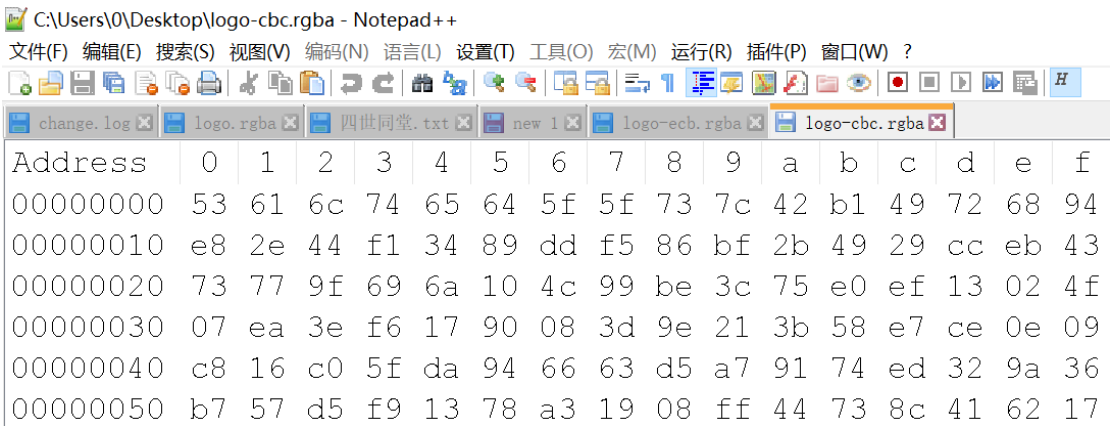
大校徽图片：



6、使用 gmssl 的 CBC 模式的 SM4 算法对 “logo.rgb a” 进行加密，密钥为 “P@ssw0rd”，输出为 “logo-cbc.rgb a” 文件，命令如下：

```
gmssl enc -sms4-cbc -e -in C:\Users\0\Desktop\logo.rgb a -out C:\Users\0\Desktop\logo-cbc.rgb a -k P@ssw0rd
```

在桌面生成 “logo-cbc.rgb a” 文件：

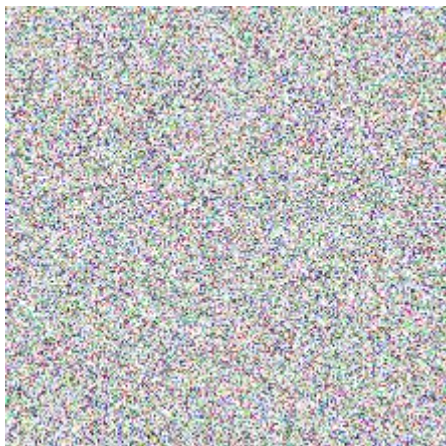


7、使用 ImageMagick 的 convert 命令，将 “logo-cbc.rgb a” 转换回 png 格式的 “logo-cbc.png”，命令如下：

```
magick convert -size 220x220 -depth 32 C:\Users\0\Desktop\logo-cbc.rgb a C:\Users\0\Desktop\logo-cbc.png
```

在桌面生成 “logo-cbc.png” 文件，即为基于 CBC 模式下的 SM4 算法加密后的北

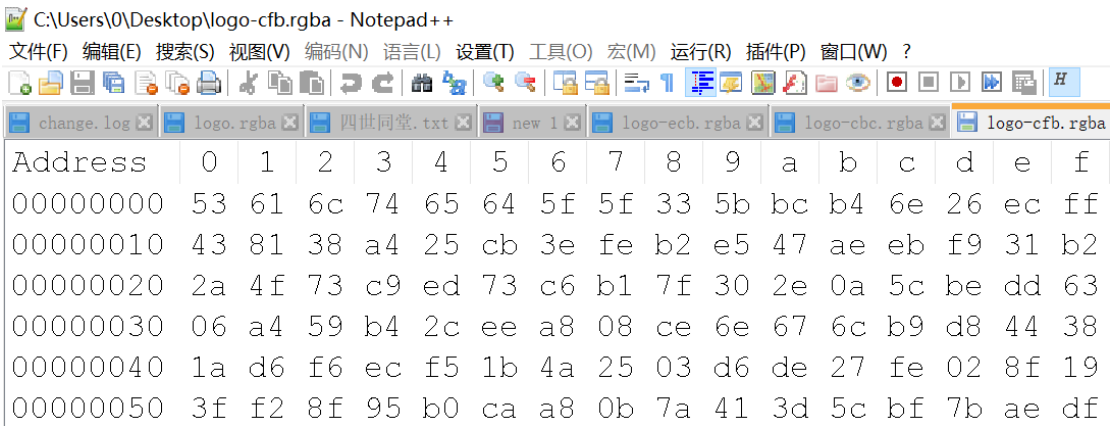
大校徽图片：



8、使用 gmssl 的 CFB 模式的 SM4 算法对 “logo.png” 进行加密，密钥为 “P@ssw0rd”，输出为 “logo-cfb.png” 文件，命令如下：

```
gmssl enc -sms4-cfb -e -in C:\Users\0\Desktop\logo.png -out C:\Users\0\Desktop\logo-cfb.png -k P@ssw0rd
```

在桌面生成 “logo-cfb.png” 文件：



9、使用 ImageMagick 的 convert 命令，将 “logo-cfb.png” 转换回 png 格式的 “logo-cfb.png”，命令如下：

```
magick convert -size 220x220 -depth 32 C:\Users\0\Desktop\logo-cfb.png C:\Users\0\Desktop\logo-cfb.png
```

在桌面生成 “logo-cfb.png” 文件，即为基于 CFB 模式下的 SM4 算法加密后的北

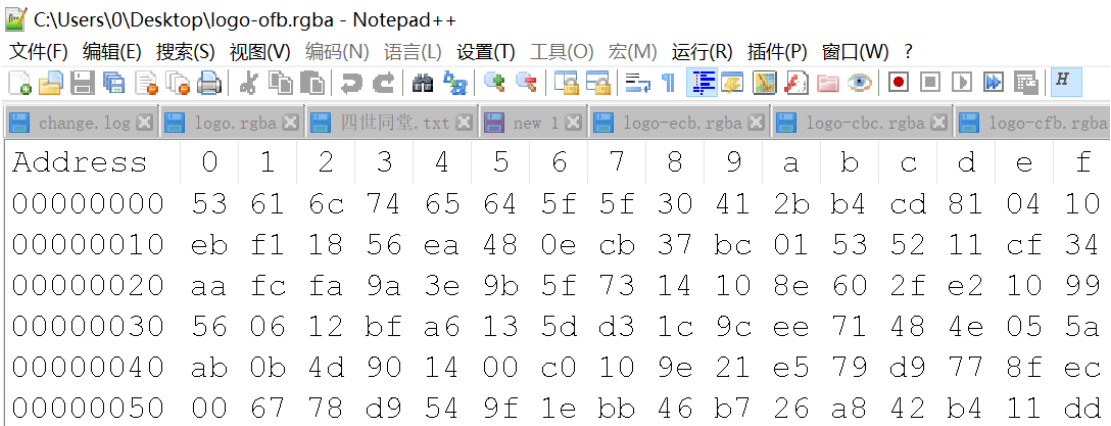
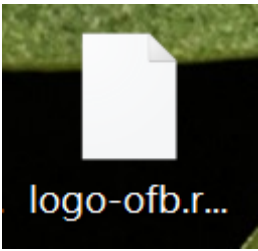
大校徽图片：



10、使用 gmssl 的 OFB 模式的 SM4 算法对“logo.rgb”进行加密，密钥为“P@ssw0rd”，输出为“logo-ofb.rgb”文件，命令如下：

```
gmssl enc -sms4-ofb -e -in C:\Users\0\Desktop\logo.rgb -out C:\Users\0\Desktop\logo-ofb.rgb -k P@ssw0rd
```

在桌面生成“logo-ofb.rgb”文件：



11、使用 ImageMagick 的 convert 命令，将“logo-ofb.rgb”转换回 png 格式的“logo-ofb.png”，命令如下：

```
magick convert -size 220x220 -depth 32 C:\Users\0\Desktop\logo-ofb.rgb C:\Users\0\Desktop\logo-ofb.png
```

在桌面生成“logo-ofb.png”文件，即为基于 OFB 模式下的 SM4 算法加密后的北大

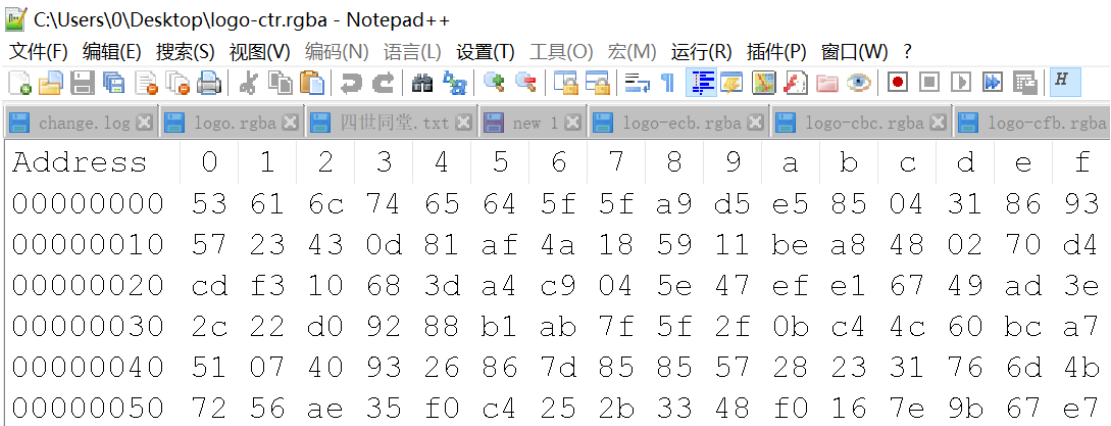
校徽图片：



12、 使用 gmssl 的 CTR 模式的 SM4 算法对“logo.rgba”进行加密，密钥为“P@ssw0rd”，输出为“logo-ctr.rgba”文件，命令如下：

```
gmssl enc -sms4-ctr -e -in C:\Users\0\Desktop\logo.rgba -out C:\Users\0\Desktop\logo-ctr.rgba -k P@ssw0rd
```

在桌面生成“logo-ctr.rgba”文件：



13、 使用 ImageMagick 的 convert 命令，将“logo-ctr.rgba”转换回 png 格式的“logo-ctr.png”，命令如下：

```
magick convert -size 220x220 -depth 32 C:\Users\0\Desktop\logo-ctr.rgba C:\Users\0\Desktop\logo-ctr.png
```

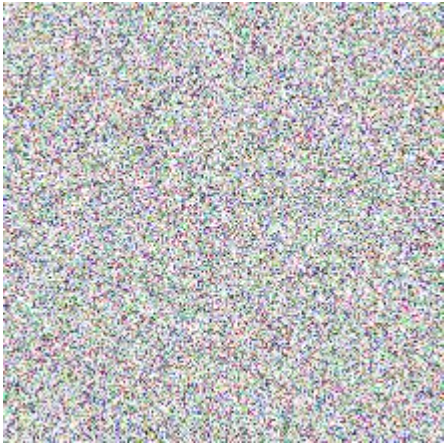
在桌面生成“logo-ctr.png”文件，即为基于 CTR 模式下的 SM4 算法加密后的北

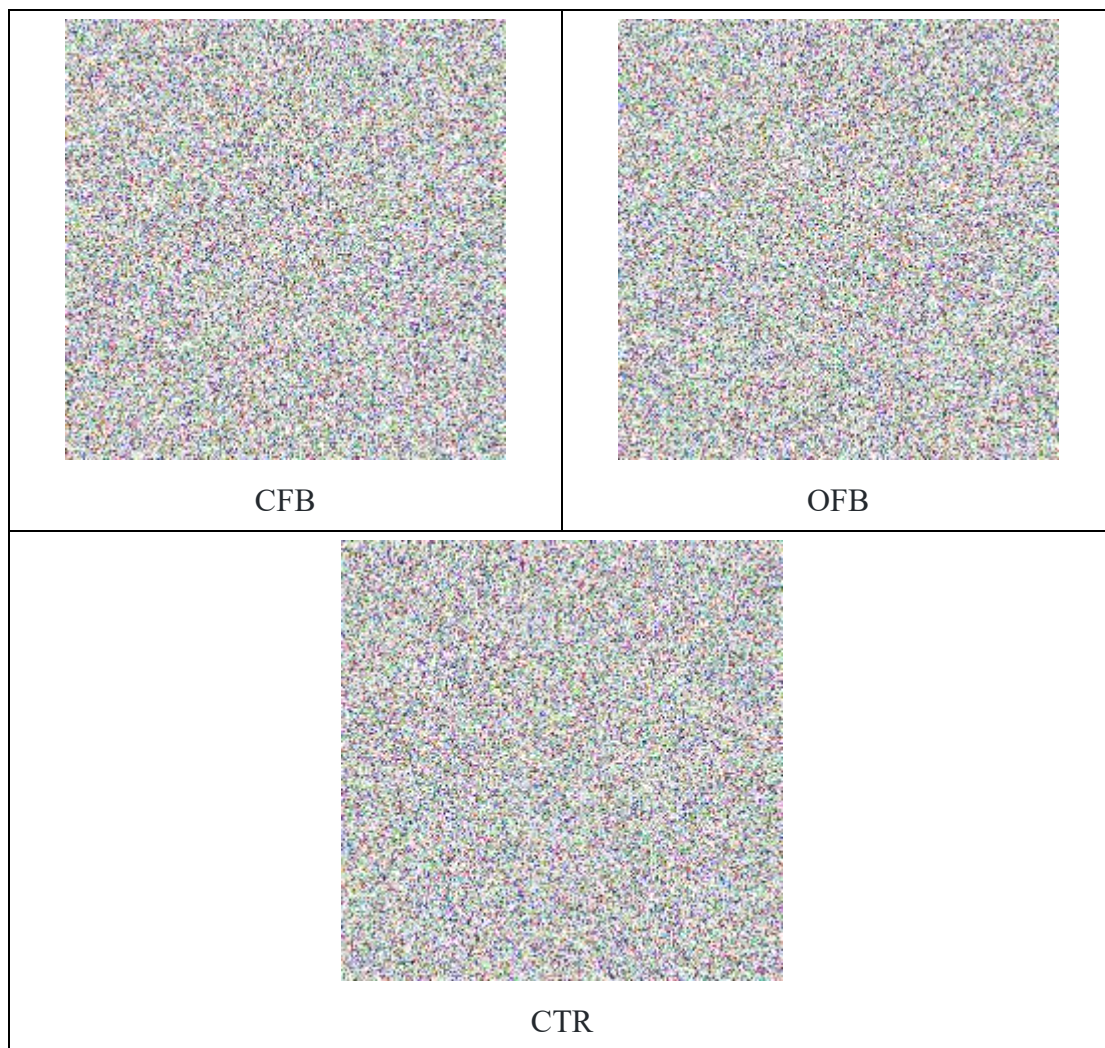
大校徽图片：



五、 实验结果分析：

由于 ECB 模式不能隐藏明文模式（尤其是对于随机性不强的明文），在密文中会出现明文消息的重复，加密消息块的相互独立成为被攻击的弱点，可以对明文进行主动攻击^[2]。而从实验结果可以看出，由于北京大学校徽图片像素明文随机性不强，故用 ECB 模式加密得到的结果明显差于其它的几个模式，如下表所示：

	
ECB	CBC



六、实验中的问题与总结：

本次实验我使用 GmSSL 和 ImageMagick，使用基于 ECB、CBC、CFB、OFB 和 CTR 这 5 种模式的 SM4 算法加密了北京大学校徽。

实验中我遇到了一个问题：是在直接使用 “convert...” 命令时参数无效：

```
C:\Windows\System32>convert -depth 32 C:\Users\0\Desktop\logo.png C:\Users\0\Desktop\logo.rgba
无效参数 - 32
```

这是因为此时运行的 “convert” 是 Windows 的分区自带的类型转换程序，正确的命令应该是：“magick convert...”，解决方法是加上“magick”即可^[3]：

```
C:\Windows\System32>magick convert -depth 32 C:\Users\0\Desktop\logo.png C:\Users\0\Desktop\logo.rgba
C:\Windows\System32>
```

【参考资料】

[1] https://blog.csdn.net/weixin_42940826/article/details/83687007 （对称加密算法常用的五种分组模式（ECB/CBC/CFB/OFB/CTR））。

[2] <https://www.cnblogs.com/yanzi-meng/p/9640578.html> （分组加密的四种模式（ECB、CBC、CFB、OFB））.

[3] <https://www.cnblogs.com/yourstars/p/5849818.html> （关于 ImageMagick 出现无效参数（invalid parameter）的解决方法）.