攻防世界crypto高手题之banana-princess

原创

沐一 · 林 于 2021-09-10 21:50:04 发布 174 收藏 1

分类专栏： CTF 密码学 文章标签： ctf

本文链接：https://blog.csdn.net/xiao__1bai/article/details/120230019


CTF 同时被 2 个专栏收录

167 篇文章 6 订阅

订阅专栏


密码学

51 篇文章 1 订阅

订阅专栏

攻防世界crypto高手题之banana-princess

继续开启全栈梦想之逆向之旅~

这题是攻防世界crypto高手题的banana-princess

.

.

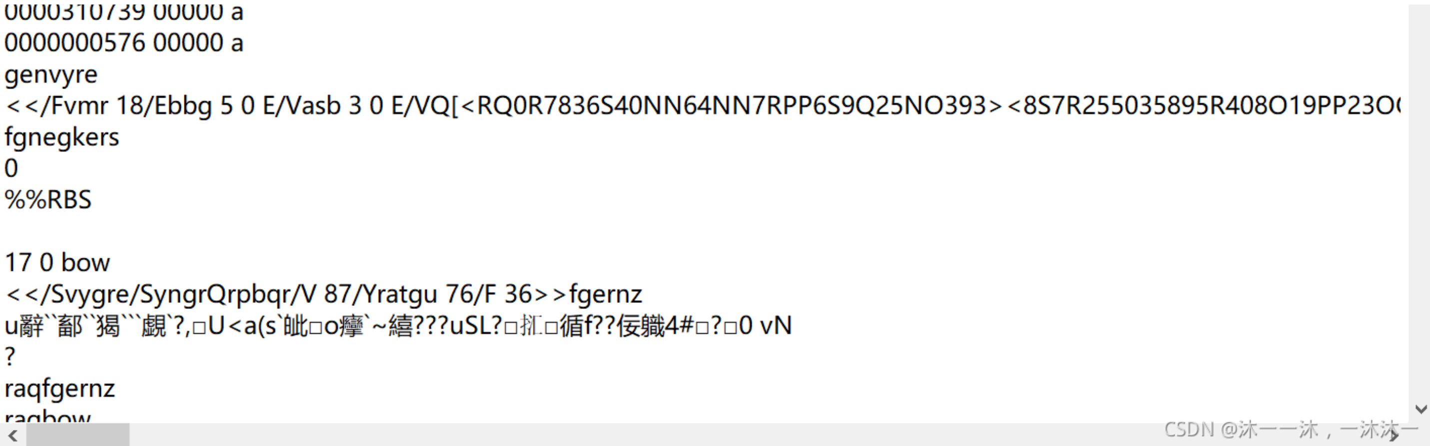
下载附件，是一个PDF文件，打不开，题目英文提示香蕉原则，好吧并没有什么用。(^ ~ ^)用记事本打开看一下内容：

.

（这里积累第一个经验）

前面排列到时挺规整的，不像是一个文件：

```
0000001224 00000 a
0000001444 00000 a
0000036608 00000 a
0000040339 00000 a
0000040400 00000 a
0000040618 00000 a
0000207067 00000 a
0000215381 00000 a
```

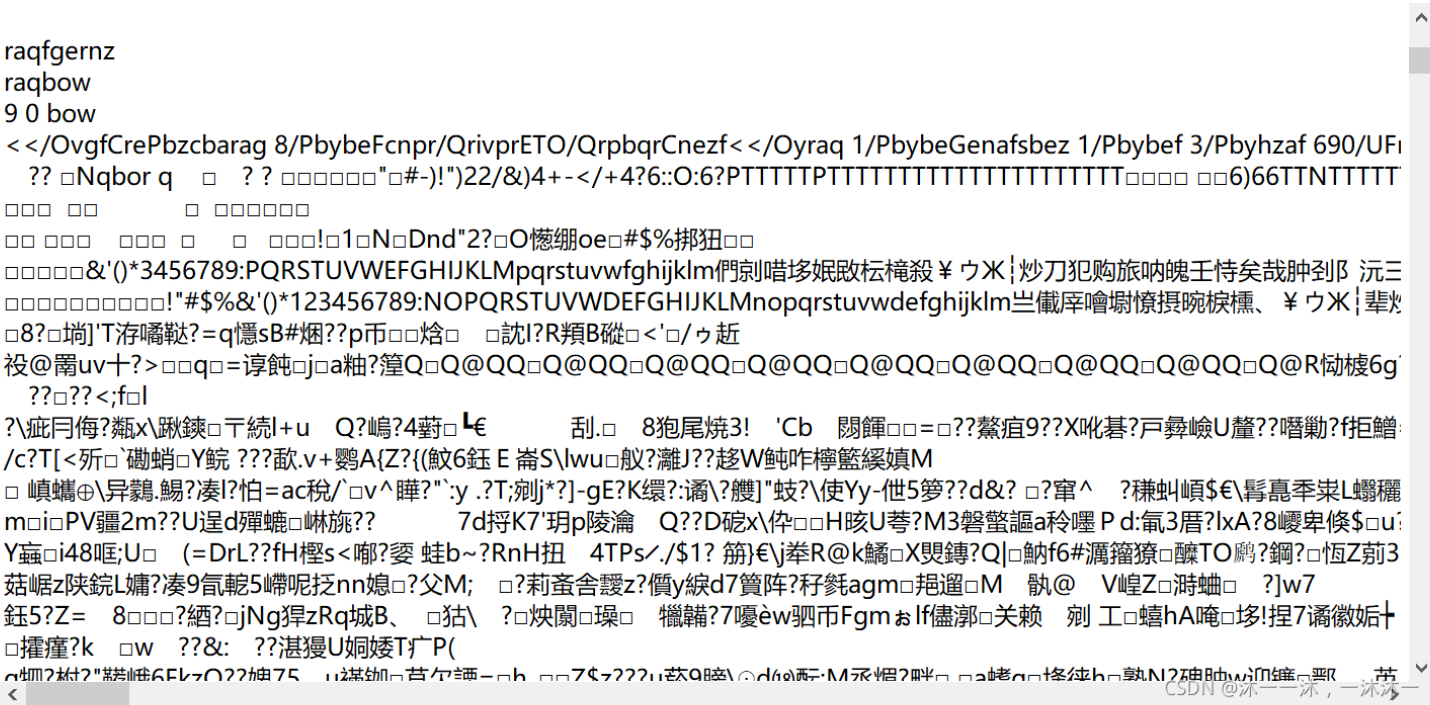

```
0000310739 00000 a
0000000576 00000 a
genvyre
<</Fvmr 18/Ebbg 5 0 E/Vasb 3 0 E/VQ[<RQ0R7836S40NN64NN7RPP6S9Q25NO393><8S7R255035895R408O19PP23O
fgnegkers
0
%%RBS

17 0 bow
<</Svygre/SyngrQrpbqr/V 87/Yratgu 76/F 36>>fgernz
?
raqfgernz
```

.

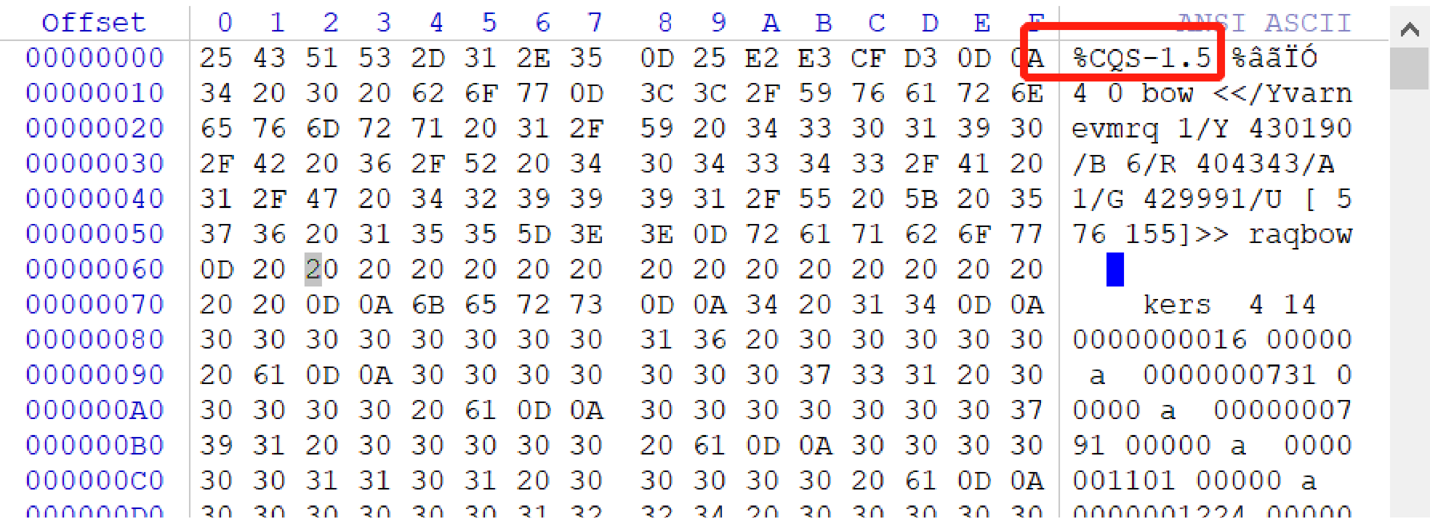
.

后面的乱码又像是文件了：


```
raqfgernz
raqbow
9 0 bow
<</OvgfCrePbzcbarag 8/PbybeFcnpr/QrivprETO/QrpbqrCnezf<</Oyraq 1/PbybeGenafsbez 1/Pbybef 3/Pbyhzaf 690/UF
```

这一下给我搞糊涂了，直接搜flag字眼，没有，肯定也没有，毕竟都高手题了，扔到winhex64中再看一下。

嗯~其实一开始我也看不出有什么不妥，红框那里是查了资料说与正常PDF有不同。



Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
00000000	25	43	51	53	2D	31	2E	35	0D	25	E2	E3	CF	D3	0D	0A	%CQS-1.5 %âãÏÓ
00000010	34	20	30	20	62	6F	77	0D	3C	3C	2F	59	76	61	72	6E	4 0 bow <</Yvarn
00000020	65	76	6D	72	71	20	31	2F	59	20	34	33	30	31	39	30	evmrq 1/Y 430190
00000030	2F	42	20	36	2F	52	20	34	30	34	33	34	33	2F	41	20	/B 6/R 404343/A
00000040	31	2F	47	20	34	32	39	39	39	31	2F	55	20	5B	20	35	1/G 429991/U [5
00000050	37	36	20	31	35	35	5D	3E	3E	0D	72	61	71	62	6F	77	76 155]>> raqbow
00000060	0D	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
00000070	20	20	0D	0A	6B	65	72	73	0D	0A	34	20	31	34	0D	0A	kers 4 14
00000080	30	30	30	30	30	30	30	30	31	36	20	30	30	30	30	30	0000000016 00000
00000090	20	61	0D	0A	30	30	30	30	30	30	30	37	33	31	20	30	a 0000000731 0
000000A0	30	30	30	30	20	61	0D	0A	30	30	30	30	30	30	30	37	0000 a 00000007
000000B0	39	31	20	30	30	30	30	30	20	61	0D	0A	30	30	30	30	91 00000 a 0000
000000C0	30	30	31	31	30	31	20	30	30	30	30	30	20	61	0D	0A	001101 00000 a
000000D0	30	30	30	30	30	30	31	32	32	34	20	30	30	30	30	30	0000001224 00000

```
000000D0  30 30 30 30 30 30 31 32  32 34 20 30 30 30 30 30  0000001224 00000
000000E0  20 61 0D 0A 30 30 30 30  30 30 31 34 34 34 20 30   a  0000001444 0
000000F0  30 30 30 30 20 61 0D 0A  30 30 30 30 30 33 36 36  0000 a  00000366
00000100  30 38 20 30 30 30 30 30  20 61 0D 0A 30 30 30 30  08 00000 a  0000
00000110  30 34 30 33 33 39 20 30  30 30 30 30 20 61 0D 0A  040339 00000 a
00000120  30 30 30 30 30 34 30 34  30 30 20 30 30 30 30 30  0000040400 00000
00000130  20 61 0D 0A 30 30 30 30  30 34 30 36 31 38 20 30   a  0000040618 0
00000140  30 30 30 30 20 61 0D 0A  30 30 30 30 32 30 37 30  0000 a  00002070
00000150  36 37 20 30 30 30 30 30  20 61 0D 0A 30 30 30 30  67 00000 a  0000
00000160  32 31 35 33 38 31 20 30  30 30 30 30 20 61 0D 0A  215381 00000 a
00000170  30 30 30 30 33 31 30 37  33 39 20 30 30 30 30 30  0000310739 00000
00000180  20 61 0D 0A 30 30 30 30  30 30 30 35 37 36 20 30   a  0000000576 0
00000190  30 30 30 30 20 61 0D 0A  67 65 6E 76 79 72 65 0D  0000 a  genvyre
000001A0  0A 3C 3C 2F 46 76 6D 72  20 31 38 2F 45 62 62 67   <</Fvmr 18/Ebbg
000001B0  20 35 20 30 20 45 2F 56  61 73 62 20 33 20 30 20   5 0 E/Vasb 3 0
000001C0  45 2F 56 51 5B 3C 52 51  30 52 37 38 33 36 53 34  E/VQ[<RQ0R7836S4
000001D0  30 4E 4E 36 34 4E 4E 37  52 50 50 36 53 39 51 32  0NN64NN7RPP6S9Q2
000001E0  35 4E 4F 33 39 33 3E 3C  38 53 37 52 32 35 35 30  5NO393><8S7R2550
000001F0  33 35 38 39 35 52 34 30  38 4F 31 39 50 50 32 33  35895R408O19PP23
00000200  4F 4F 50 34 4E 32 52 39  3E 5D 2F 43 65 72 69 20  OOP4N2R9>]/Ceri
00000210  34 32 39 39 38 31 3E 3E  0D 0A 66 67 6E 65 67 6B  429981>>  fgnegk
00000220  65 72 73 0D 0A 30 0D 0A  25 25 52 42 53 0D 0A 20  ers  0  %%RBS
00000230  20 20 20 20 20 20 20 20  20 20 20 20 20 20 0D 0A
00000240  31 37 20 30 20 62 6F 77  0D 3C 3C 2F 53 76 79 67  17 0 bow <</Svyg
00000250  72 65 2F 53 79 6E 67 72  51 72 70 62 71 72 2F 56  re/SyngrQrpbqr/V
00000260  20 38 37 2F 59 72 61 74  67 75 20 37 36 2F 46 20   87/Yratgu 76/F
```


.

.

正常PDF头：

Adobe Acrobat pdf %PDF-1.xx （1.xx是版本号）

```
Offset    0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F      ANSI ASCII
00000000  25 50 44 46 2D 31 2E 35  0D 25 E2 E3 CF D3 0D 0A  %PDF-1.5 §âãÏÓ
00000010  34 20 30 20 6F 62 6A 0D  3C 3C 2F 4C 69 6E 65 61  4 0 obj <</Linea
00000020  72 69 7A 65 64 20 31 2F  4C 20 34 33 30 31 39 30  rized 1/L 430190
00000030  2F 4F 20 36 2F 45 20 34  30 34 33 34 33 2F 4E 20  /O 6/E 404343/N
00000040  31 2F 54 20 34 32 39 39  39 31 2F 48 20 5B 20 35  1/T 429991/H [ 5
00000050  37 36 20 31 35 35 5D 3E  3E 0D 65 6E 64 6F 62 6A  76 155]>> endobj
00000060  0D 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
00000070  20 20 0D 0A 78 72 65 66  0D 0A 34 20 31 34 0D 0A     xref  4 14
00000080  30 30 30 30 30 30 30 30  31 36 20 30 30 30 30 30  0000000016 00000
00000090  20 6E 0D 0A 30 30 30 30  30 30 30 37 33 31 20 30   n  0000000731 0
000000A0  30 30 30 30 20 6E 0D 0A  30 30 30 30 30 30 30 37  0000 n  00000007
000000B0  39 31 20 30 30 30 30 30  20 6E 0D 0A 30 30 30 30  91 00000 n  0000
000000C0  30 30 31 31 30 31 20 30  30 30 30 30 20 6E 0D 0A  001101 00000 n
000000D0  30 30 30 30 30 30 31 32  32 34 20 30 30 30 30 30  0000001224 00000
000000E0  20 6E 0D 0A 30 30 30 30  30 30 31 34 34 34 20 30   n  0000001444 0
000000F0  30 30 30 30 20 6E 0D 0A  30 30 30 30 30 33 36 36  0000 n  00000366
00000100  30 38 20 30 30 30 30 30  20 6E 0D 0A 30 30 30 30  08 00000 n  0000
00000110  30 34 30 33 33 39 20 30  30 30 30 30 20 6E 0D 0A  040339 00000 n
00000120  30 30 30 30 30 34 30 34  30 30 20 30 30 30 30 30  0000040400 00000
00000130  20 6E 0D 0A 30 30 30 30  30 34 30 36 31 38 20 30   n  0000040618 0
```

```
00000140  30 30 30 30 20 6E 0D 0A  30 30 30 30 32 30 37 30  0000 n  00002070
00000150  36 37 20 30 30 30 30 30  20 6E 0D 0A 30 30 30 30  67 00000 n  0000
00000160  32 31 35 33 38 31 20 30  30 30 30 30 20 6E 0D 0A  215381 00000 n
00000170  30 30 30 30 33 31 30 37  33 39 20 30 30 30 30 30  0000310739 00000
00000180  20 6E 0D 0A 30 30 30 30  30 30 30 35 37 36 20 30   n  0000000576 0
00000190  30 30 30 30 20 6E 0D 0A  74 72 61 69 6C 65 72 0D  0000 n  trailer
000001A0  0A 3C 3C 2F 53 69 7A 65  20 31 38 2F 52 6F 6F 74   <</Size 18/Root
000001B0  20 35 20 30 20 52 2F 49  6E 66 6F 20 33 20 30 20   5 0 R/Info 3 0
000001C0  52 2F 49 44 5B 3C 45 44  30 45 37 38 33 36 46 34  R/ID[<ED0E7836F4
000001D0  30 41 41 36 34 41 41 37  45 43 43 36 46 39 44 32  0AA64AA7ECC6F9D2
000001E0  35 41 42 33 39 33 3E 3C  38 46 37 45 32 35 35 30  5AB393><8F7E2550
000001F0  33 35 38 39 35 45 34 30  38 42 31 39 43 43 32 33  35895E408B19CC23
00000200  42 42 43 34 41 32 45 39  3E 5D 2F 50 72 65 76 20  BBC4A2E9>]/Prev
00000210  34 32 39 39 38 31 3E 3E  0D 0A 73 74 61 72 74 78  429981>>  startx
00000220  72 65 66 0D 0A 30 0D 0A  25 25 45 4F 46 0D 0A 20  ref  0  %%EOF
00000230  20 20 20 20 20 20 20 20  20 20 20 20 20 20 0D 0A
00000240  31 37 20 30 20 6F 62 6A  0D 3C 3C 2F 46 69 6C 74  17 0 obj <</Filt
00000250  65 72 2F 46 6C 61 74 65  44 65 63 6F 64 65 2F 49  er/FlateDecode/I
00000260  20 38 37 2F 4C 65 6E 67  74 68 20 37 36 2F 53 20   87/Length 76/S
```


.

.

到这里我的思想就和别人不一样了，别人是思考`%CQS-1.5`和`%PDF-1.x`的关系。而我的第一反应是`%CQS-1.5`是一个没学过的文件头。。。。。毕竟没学过的文件头大把，，所以才有这么菜的自己。(哭~)

.

.

然后要问一个字母和另一个字母的关系，加密中能把一个字母加密后是另一个字母的目前学过的有培根，ROT13，24字母移动的凯撒密码。ROT13和凯撒是同一个类型，所以这里看看移动了多少位，发现都是移动了13位。那么这整个PDF文件的内容应该都是移动了13位才会有这种有规则数据和文件乱码数据的现象吧。

明文字母表	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
密文字母表	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

.

.

(这里积累第二个经验)

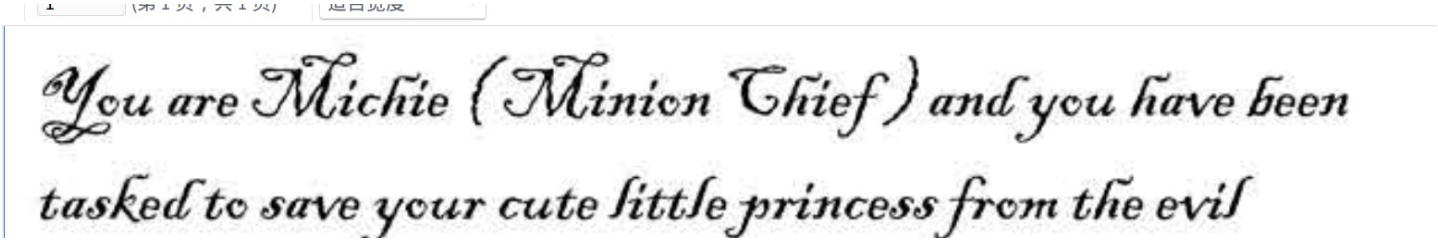
附上kali的字符移动13位的命令shell，这里tr命令的应用也是学到了知识，A-Za-z按顺序对应N-ZA-Mn-za-m，这连着的正则表达式之间不用空格也不用分号，无拘无束。

```
cat 1.pdf | tr A-Za-z N-ZA-Mn-za-m > 2.pdf
```

.

.

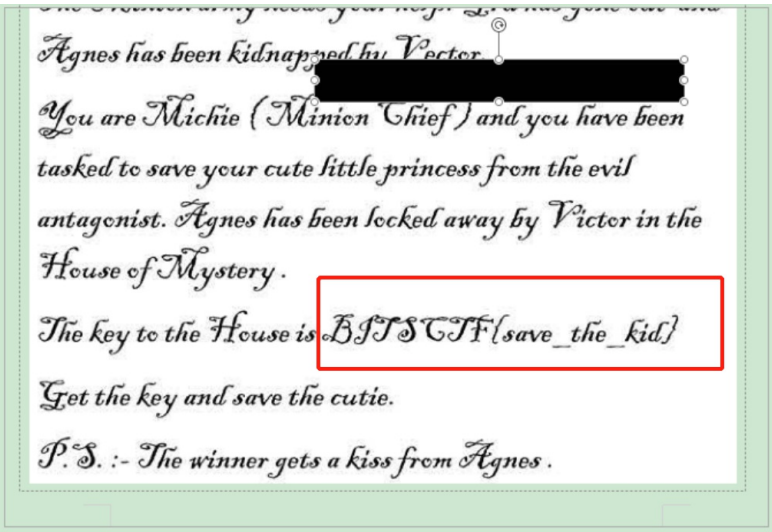
然后，转出来的PDF还自带黑格隐藏，一开始我都不记得怎么分离了，后来查资料说转html可以分离，因为这是两张图片重叠在一起而已。事实上用我的嗨格式永久VIP会员PDF转HTML、WORD、PPT都是可以分离的。



antagonist. Agnes has been locked away by Victor in the House of Mystery .

The key to the House is [redacted]

Get the key and save the cutie.

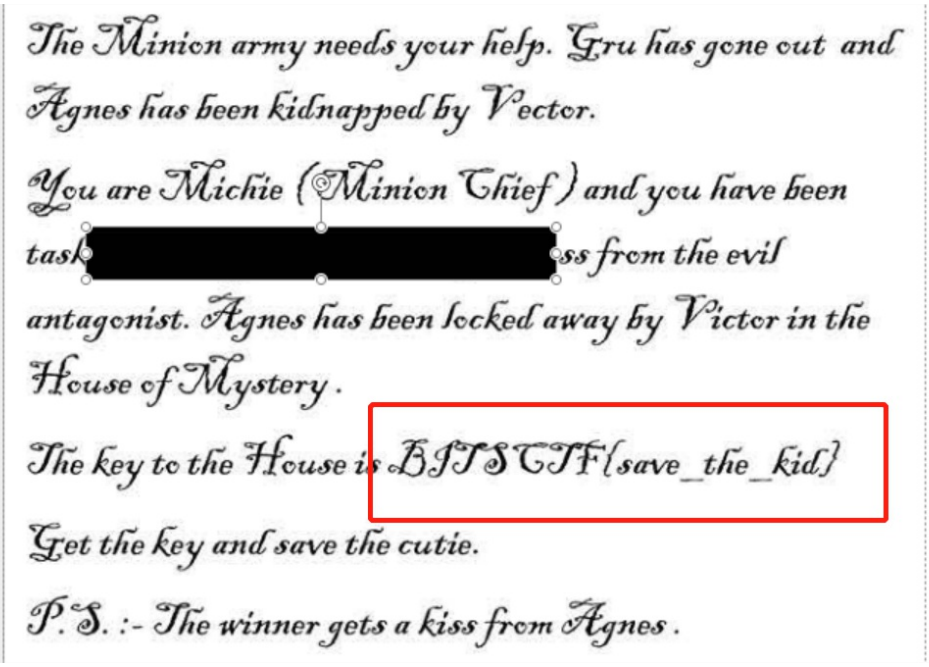

Agnes has been kidnapped by Vector.

You are Michie (Minion Chief) and you have been tasked to save your cute little princess from the evil antagonist. Agnes has been locked away by Victor in the House of Mystery .

The key to the House is BJTSCTF{save_the_kid}

Get the key and save the cutie.

P.S. :- The winner gets a kiss from Agnes .


The Minion army needs your help. Gru has gone out and Agnes has been kidnapped by Vector.

You are Michie (Minion Chief) and you have been tas[redacted]ss from the evil antagonist. Agnes has been locked away by Victor in the House of Mystery .

The key to the House is BJTSCTF{save_the_kid}

Get the key and save the cutie.

P.S. :- The winner gets a kiss from Agnes .

.

.

总结：

1：
（这里积累第一个经验） 前面排列到时挺规整的，不像是一个文件：
后面的乱码又像是文件了：
红框那里是查了资料说与正常PDF有不同。
.
.
到这里我的思想就和别人不一样了，别人是思考 `%CQS-1.5` 和 `%PDF-1.x` 的关系。而我的第一反应是 `%CQS-1.5` 是一个没学过的文件头。。。。。毕竟没学过的文件头大把，，所以才有这么菜的自己。(哭~)
.
.
然后要问一个字母和另一个字母的关系，加密中能把一个字母加密后是另一个字母的目前学过的有培根，ROT13，24字母移动的凯撒密码。ROT13和凯撒是同一个类型，所以这里看看移动了多少位，发现都是移动了13位。那么这整个PDF文件的内容应该都是移动了13位才会有这种有规则数据和文件乱码数据的现象吧。

2：
(这里积累第二个经验)
附上kali的字符移动13位的命令shell，这里tr命令的应用也是学到了知识，A-Za-z按顺序对应N-ZA-Mn-za-m，这连着的正则表达式之间不用空格也不用分号，无拘无束。
.
然后，转出来的PDF还自带黑格隐藏，一开始我都不记得怎么分离了，后来查资料说转html可以分离，因为这是两张图片重叠在一起而已。事实上用我的嗨格式永久VIP会员PDF转HTML、WORD、PPT都是可以分离的。

解毕！敬礼！