

xctf攻防世界 CRYPTO高手进阶区 banana-princess

原创

18947943 于 2022-02-11 10:27:17 发布 11429 收藏

分类专栏: [攻防世界crypto之路](#) 文章标签: [安全](#) [CRYPTO](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/18947943/article/details/122874668>

版权



[攻防世界crypto之路](#) 专栏收录该内容

26 篇文章 0 订阅

订阅专栏

1. 进入环境, 下载附件

题目给了个压缩包, 包含一个pdf文件, 尝试使用pdf阅读器打开, 提示文件已损坏。



2. 问题分析

我们将其放入winhex中, 并打开一个正常的pdf文件, 观察并对比其中的差异, 正常的如图:

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	36	0D	25	E2	E3	CF	D3	0D	0A	PDF	1.6 %âãÿÓ
00000010	33	32	20	30	20	6F	62	6A	0D	3C	3C	2F	46	69	6C	74	32	0 obj <</Filt
00000020	65	72	2F	46	6C	61	74	65	44	65	63	6F	64	65	2F	46	er/FlateDecode/F	
00000030	69	72	73	74	20	31	31	2F	4C	65	6E	67	74	68	20	31	irst 11/Length 1	
00000040	38	35	2F	4E	20	32	2F	54	79	70	65	2F	4F	62	6A	53	85/N 2/Type/ObjS	

给的文件如图:

offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI	ASCII
000000	25	43	51	53	2D	31	2E	35	0D	25	E2	E3	CF	D3	0D	0A	CCS-1.5	%äääiö
000010	34	20	30	20	62	6F	77	0D	3C	3C	2F	59	76	61	72	6E	4	U bow <</Yvarn
000020	65	76	6D	72	71	20	31	2F	59	20	34	33	30	31	39	30	evmrq	1/Y 430190
000030	2F	42	20	36	2F	52	20	34	30	34	33	34	33	2F	41	20	/B	6/R 404343/A
000040	31	2F	47	20	34	32	39	39	39	31	2F	55	20	5B	20	35	1/G	429991/U [5
000050	37	36	20	31	35	35	5D	3E	3E	0D	72	61	71	62	6F	77	76	155]>> raqbw
000060	0D	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20		
000070	20	20	0D	0A	6B	65	72	73	0D	0A	34	20	31	34	0D	0A	kers	4 14
000080	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	0000000016	000000

50 44 46 -> 43 51 53，将其转换成十进制，80 68 70 -> 67 81 83，发现字节之间的差值为13。猜测可能是ROT13加密。

密码描述

播报 编辑

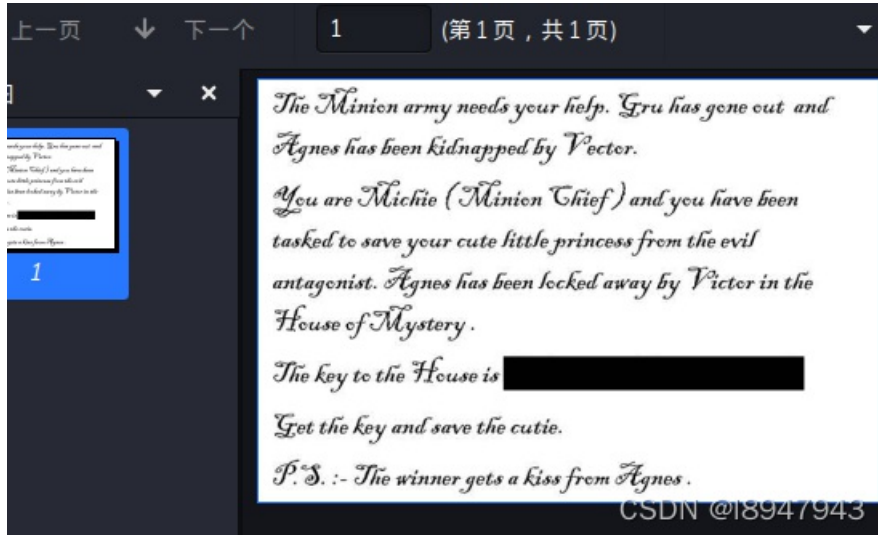
套用ROT13到一段文字上仅仅只需要检查字元字母顺序并取代它在13位之后的对应字母，有需要超过时则重新绕回26英文字母开头即可。A换成N、B换成O、依此类推到M换成Z，然后序列反转：N换成A、O换成B、最后Z换成M。只有这些出现在英文字母里头的字元受影响；数字、符号、空白字元以及所有其他字元都不变。因为只有在英文字母表里头只有26个，并且 $26=2 \times 13$ ，ROT13函数是它自己的逆反：^[1]

我们提取pdf中的数据，尝试将其按照ROT13再次进行偏移转换，即可复原。

将来pdf丢入kali中：（PS：kali中tr命令的使用：https://blog.csdn.net/weixin_40746176/article/details/104511547）

```
cat 9e45191069704531accd66f1ee1d5b2b.pdf | tr 'A-Za-z' 'N-ZA-Mn-za-m' > res.pdf
```

可以得到解密的pdf如图:



好家伙，还有马赛克，直接用pdf编辑器进行编辑，将其挪开，如图：

apped by Vector.

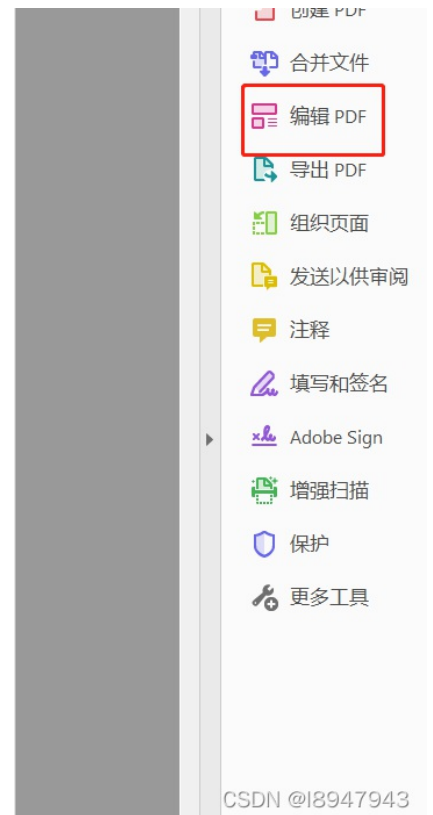
Minion Chief) and you have been

te little princess from the evil

is [REDACTED] e

is BITSTCTF{save_the_kid}

the cutie.



最终的答案为: `BITSTCTF{save_the_kid}`