第二届BMZCTF公开赛CRYPTO的simple

原创

沐一 · 林 于 2022-02-03 21:45:35 发布 195 收藏

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/122779060

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

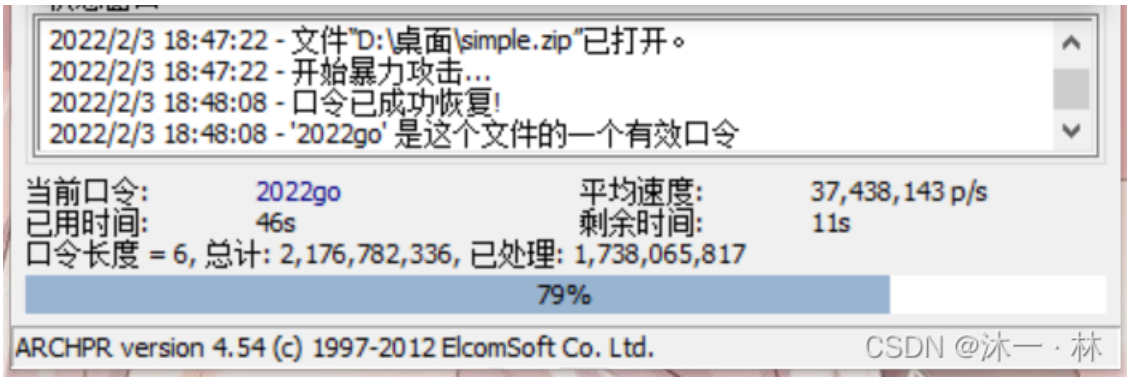
订阅专栏

第二届BMZCTF公开赛CRYPTO的simple

.

.

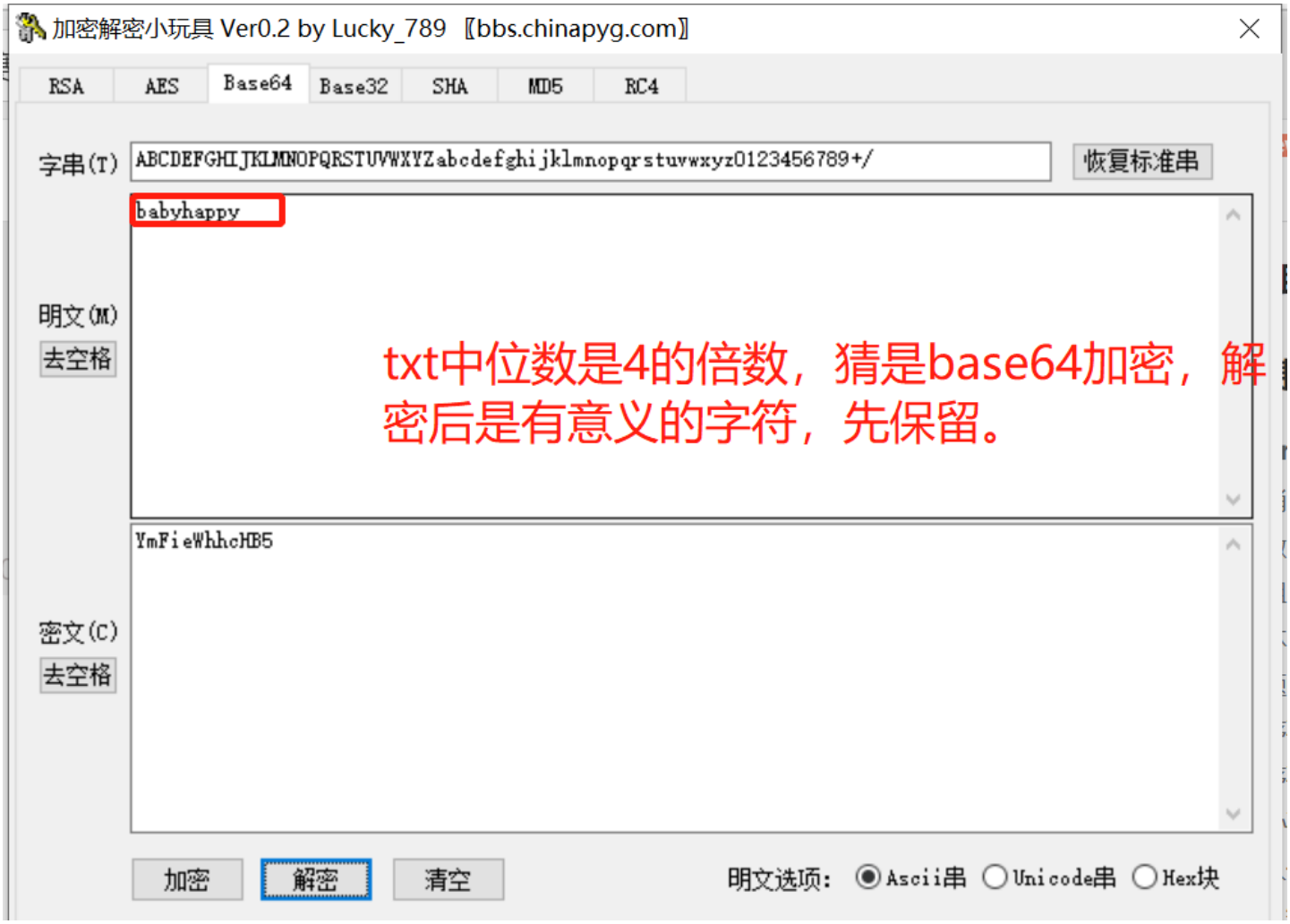
照例下载压缩包，解压，需要密码，直接 ARCHPR-4.5(密码8835)爆破：



.

.

解压后是两个附件，一个 txt，一个jpg：



Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
00009510	14	EC	7A	53	CA	64	0A	40	BD	B3	4A	E0	37	67	34	E0	ìzSÊd @½³Jà7g4à
00009520	B4	EC	52	ED	C0	A0	06	ED	19	A7	11	81	D2	8E	3A	53	´ìRíÀ í § ÒŽ:S
00009530	80	34	C4	46	53	8A	55	4E	F5	21	03	14	83	1D	32	69	€4ÄFSŠUNõ! ƒ 2i
00009540	5C	06	EC	CD	0A	BC	E7	15	26	DE	28	C7	E1	4A	E3	14	\ ìÍ ¼ç &Þ(ÇáJã
00009550	28	02	97	6F	7A	41	C0	E6	82	46	3A	83	48	05	C8	A9	(—ozAÀæ‚F:ƒH È©
00009560	14	E7	9C	D4	60	7E	54	F5	27	B5	30	1C	08	CF	4A	32	çœÔ`~Tõ'µ0 ÏJ2
00009570	71	93	4C	E9	9A	43	93	D3	A5	03	24	53	CD	3C	73	51	q"LéšC"Ó¥ $SÍ<sQ
00009580	AF	4A	78	3F	2F	14	08	7E	40	E9	4C	CF	34	9B	81	38	¯Jx?/ ~@éLÏ4› 8
00009590	A3	BE	3D	68	B8	AC	3C	1C	77	A6	93	9A	61	6D	BD	4D	£¾=h¸¬< w¦"šam½M
000095A0	2E	72	28	01	C0	E4	D2	3F	1D	0D	26	70	3A	D3	18	E4	.r(ÀäÒ? &p:Ó ä
000095B0	D0	31	FD	B9	39	A4	24	11	4D	2C	00	E0	F3	46	7B	9E	Ð1ý¹9¤$ M, àóF{ž
000095C0	D4	00	E0	78	A4	63	C7	4A	42	C3	B5	34	31	A0	00	B0	Ô àx¤cÇJBÃµ41 °
000095D0	FC	E9	85	B8	C0	A1	8F	38	A6	93	CD	3B	0C	3E	63	D0	üé…¸À¡ 8¦"Í; >cÐ
000095E0	7E	B4	52	6E	C0	1D	28	A0	2E	7F	FF	D9	3E	3E	55	32	~´RnÀ (. ÿÙ>>U2
000095F0	46	73	64	47	56	6B	58	31	39	2B	4B	6D	52	2B	4A	4C	FsdGVkX19+KmR+JL
00009600	70	71	30	6C	2F	49	4A	2B	72	56	6C	49	48	4E	32	54	pq0l/IJ+rVlIHN2T
00009610	2B	79	71	41	69	6B	4C	30	34	79	6A	41	3D	3D			+yqAikL04yjA==

jpg字节码最后好像是base64密文，后来解密后发现乱码，前面有一个通顺的babyhappy，后面有一个乱码的base64格式的密文，联系在一起就是RC4了。

.

.

RC4算法原理迟点在研究，照例用工具解密RC4：

.

.

最终flag：

> flag{You_Guess_It}

.

.

解毕！

敬礼！