实验吧之CTF---Snake

原创

waterKxia 于 2016-10-07 15:02:23 发布 3223 收藏

分类专栏： 实验吧CTF 文章标签： 解密 密码 实验吧CTF安全杂项

本文链接：https://blog.csdn.net/moxiajuzi/article/details/52749562

题目： Snake

无

格式：CTF{}

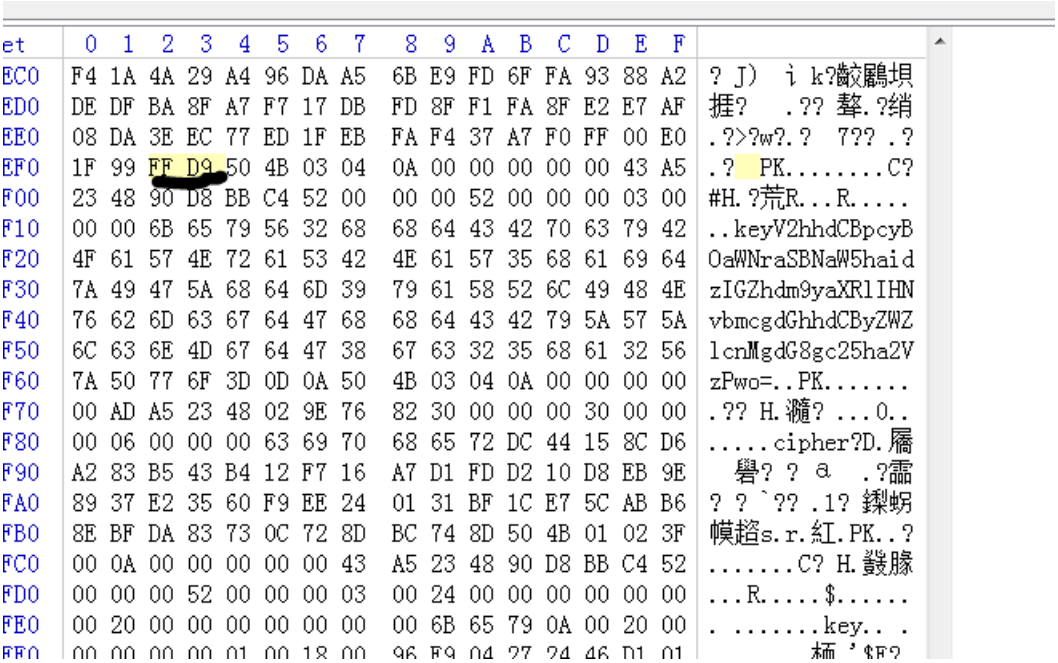
地址：http://www.shiyanbar.com/ctf/1851

解题步骤

1.下载文件

2.用winhex软件打开图片

3.因为是jpg文件所以文件头是FFD8，文件尾是FFD9。查看它们，发现此图片文件有文件尾FFD9，但不是在最后。



et	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
EC0	F4	1A	4A	29	A4	96	DA	A5	6B	E9	FD	6F	FA	93	88	A2	? J) ¤ k?骸鹂坝
ED0	DE	DF	BA	8F	A7	F7	17	DB	FD	8F	F1	FA	8F	E2	E7	AF	捱? .?? 聋.?绡
EE0	08	DA	3E	EC	77	ED	1F	EB	FA	F4	37	A7	F0	FF	00	E0	.?>?w?.? 7?? .?
EF0	1F	99	FF	D9	50	4B	03	04	0A	00	00	00	00	00	43	A5	.? PK.....C?
F00	23	48	90	D8	BB	C4	52	00	00	00	52	00	00	00	03	00	#H.?荒R...R.....
F10	00	00	6B	65	79	56	32	68	68	64	43	42	70	63	79	42	..keyV2hhdCBpcyB
F20	4F	61	57	4E	72	61	53	42	4E	61	57	35	68	61	69	64	OaWNraSBNaW5haid
F30	7A	49	47	5A	68	64	6D	39	79	61	58	52	6C	49	48	4E	zIGZhdm9yaXRlIHN
F40	76	62	6D	63	67	64	47	68	68	64	43	42	79	5A	57	5A	vbmcgdGhhdCByZWZ
F50	6C	63	6E	4D	67	64	47	38	67	63	32	35	68	61	32	56	lcnMgdG8gc25ha2V
F60	7A	50	77	6F	3D	0D	0A	50	4B	03	04	0A	00	00	00	00	zPwo=..PK.....
F70	00	AD	A5	23	48	02	9E	76	82	30	00	00	00	30	00	00	.?? H.癲? ...0..
F80	00	06	00	00	00	63	69	70	68	65	72	DC	44	15	8C	D6	.....cipher?D.屬
F90	A2	83	B5	43	B4	12	F7	16	A7	D1	FD	D2	10	D8	EB	9E	譽? ? a .?靄
FA0	89	37	E2	35	60	F9	EE	24	01	31	BF	1C	E7	5C	AB	B6	? ? `?? .1? 鑆蚜
FB0	8E	BF	DA	83	73	0C	72	8D	BC	74	8D	50	4B	01	02	3F	幙趙s.r.紅.PK..?
FC0	00	0A	00	00	00	00	00	43	A5	23	48	90	D8	BB	C4	52	.....C? H.髭膝
FD0	00	00	00	52	00	00	00	03	00	24	00	00	00	00	00	00	...R.....$.....
FE0	00	20	00	00	00	00	00	00	00	6B	65	79	0A	00	20	00	. .....key.. .
FF0	00	00	00	00	01	00	18	00	96	E9	04	27	24	46	D1	01	栖 '$F?

4.得出结论，该图片被隐写过，采用的是图种方式(采用一种特殊方式将图片与要隐藏的信息结合在一起)隐写。

5.解决办法就是将图片文件的扩展名(即:jpg)改为zip或rar

6.使它变成对应的压缩文件，再利用解压软件进行解压

7.打开文件夹发现有两个文件

一个名为cipher，另一个名为key

cipher为密文(最后解密)
key文件有一串base64加密过的密文对其进行解密
得到明文：
What is Nicki Minaj's favorite song that refers to snakes?
百度一下，得key:anaconda
8.因此cipher文件被一种加密方式加密，此加密方式还需要密钥
9.了解密码学的都知道，有公钥加密和私钥加密！！！
10.此题为公钥加密，而公钥加密最著名的就是AES
11.为此我百度了一下，发现：

形成过程

编辑

1997年4月15日，美国ANSI发起征集AES（advanced encryption standard）的活动，并为此成立了AES工作小组。

1997年9月12日，美国联邦登记处公布了正式征集AES候选算法的通告。对AES的基本要求是：比三重DES快、至少与三重DES一样安全、数据分组长度为128比特、密钥长度为128/192/256比特。

1998年8月12日，在首届AES候选会议（first AES candidate conference）上公布了AES的15个候选算法，任由全世界各机构和个人攻击和评论。

1999年3月，在第2届AES候选会议（second AES candidate conference）上经过对全球各密码机构和个人对候选算法分析结果的讨论，从15个候选算法中选出了5个。分别是RC6、Rijndael、SERPENT、Twofish和MARS。

Joan Daemen 与 Vincent Rijmen

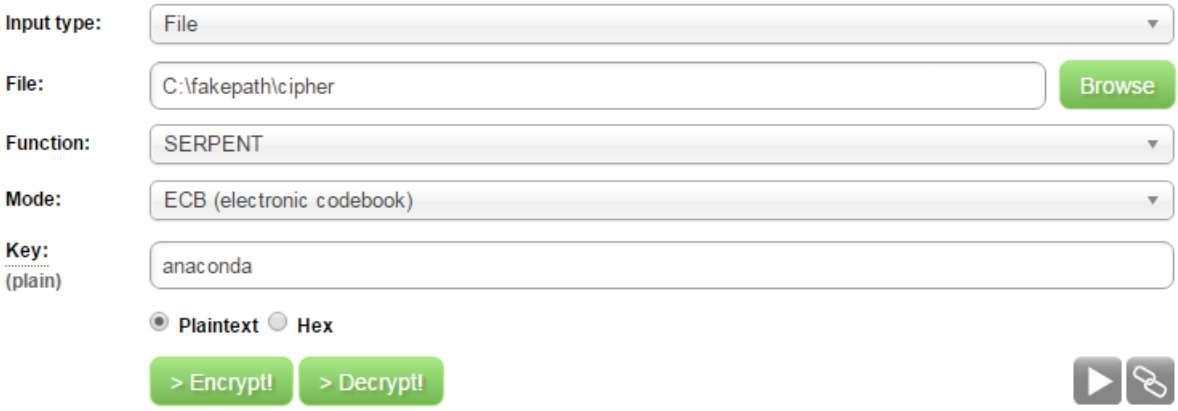
2000年4月13日至14日，召开了第3届AES候选会议（third AES candidate conference），继续对最后5个候选算法进行讨论。

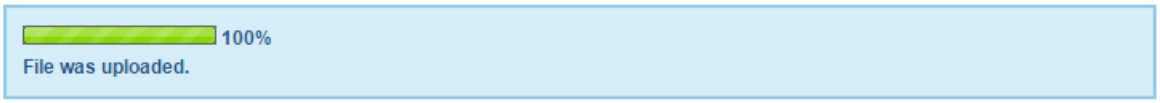
2000年10月2日，NIST宣布Rijndael作为新的AES。经过3年多的讨论，Rijndael终于脱颖而出。

Rijndael由比利时的Joan Daemen和Vincent Rijmen设计。算法的原型是Square算法，它的设计策略是宽轨迹策略（wide trail strategy）。算法有很好的抵抗差分密码分析及线性密码分析的能力。

图中被我标记的英文：SERPENT也是个密码算法
被我标记的原因是它作为英文单词的意思就是蛇==Snake
与题目有了联系
12.知道算法如何解决呢？
我多年游离于互联网，发现了一个非常有用的网站(集各种工具与web端)
地址：http://serpent.online-domain-tools.com/
这个是其下专门针对此密码的加解密地址
13.

这是输入数据后的界面，之后点击Decrypt!按钮！





Decrypted text:

00000000	43 54 46 7b 77 68 6f 5f 6b 6e 65 77 5f 73 65 72	C T F { w h o _ k n e w _ s e r
00000010	70 65 6e 74 5f 63 69 70 68 65 72 5f 65 78 69 73	p e n t _ c i p h e r _ e x i s
00000020	74 65 64 7d 00 00 00 00 00 00 00 00 00 00 00 00	t e d } . . . . .

[Download as a binary file] [?]

Inactive

得到flag：
CTF{who_know_serpent_cipher_existed}

很有趣：谁知道serpent密码的存在！！！
你知道了吗？？？