CTF中的Crypto

原创

数学家是我理想 于 2018-10-29 21:22:41 发布 9809 收藏 36

分类专栏： CTF 文章标签： CTF 密码学 Crypto

本文链接：https://blog.csdn.net/qq_37236745/article/details/83513506

密码学简介

密码学（Cryptography）一般可分为古典密码学和现代密码学。

古典密码学

古典密码学作为一种实用性艺术存在，其编码和破译通常依赖于设计者和敌手的创造力与技巧，并没有对密码学原件进行清晰的定义。古典密码学主要包含以下几个方面：

- 单表替换加密（Monoalphabetic Cipher）
- 多表替换加密（Polyalphabetic Cipher）
- 奇奇怪怪的加密方式

现代密码学

现代密码学则起源于 20 世纪中后期出现的大量相关理论，1949 年香农（C. E. Shannon）发表了题为《保密系统的通信理论》的经典论文标志着现代密码学的开始。现代密码学主要包含以下几个方面：

- 对称加密（Symmetric Cryptography），以 DES，AES，RC4 为代表
- 非对称加密（Asymmetric Cryptography），以 RSA，ElGamal，椭圆曲线加密为代表
- 哈希函数（Hash Function），以 MD5，SHA-1，SHA-512 等为代表
- 数字签名（Digital Signature），以 RSA 签名，ElGamal 签名，DSA 签名为代表

其中，对称加密体制主要分为两种方式：

- 分组密码（Block Cipher），又称为块密码
- 序列密码（Stream Cipher），又称为流密码

CTF中Crypto

CTF中脑洞密码题(非现代加密方式)一般都是各种古典密码的变形，一般出题者会对密文进行一些处理，但是会给留一些线索

1.常见编码

1. ASCII编码
2. Base64/32/16编码
3. shellcode编码
4. Quoted-printable编码
5. XXencode编码
6. UUencode编码
7. URL编码
8. Unicode编码
9. Escape/Unescape编码
10. HTML实体编码
11. 敲击码(Tap code)
12. 莫尔斯电码(Morse Code)

2.换位加密

1. 栅栏密码(Rail-fence Cipher)
2. 曲路密码(Curve Cipher)
3. 列移位密码(Columnar Transposition Cipher)

3.替换加密

1. 埃特巴什码(Atbash Cipher)
2. 凯撒密码(Caesar Cipher)
3. ROT5/13/18/47
4. 简单换位密码(Simple Substitution Cipher)
5. 希尔密码(Hill Cipher)
6. 猪圈密码(Pigpen Cipher)
7. 波利比奥斯方阵密码（Polybius Square Cipher)
8. 夏多密码(曲折加密)
9. 普莱菲尔密码(Playfair Cipher)
10. 维吉尼亚密码(Vigenère Cipher)
11. 自动密钥密码(Autokey Cipher)
12. 博福特密码(Beaufort Cipher)
13. 滚动密钥密码(Running Key Cipher)
14. Porta密码(Porta Cipher)
15. 同音替换密码(Homophonic Substitution Cipher)
16. 仿射密码(Affine Cipher)
17. 培根密码(Baconian Cipher)
18. ADFGX和ADFGVX密码(ADFG/VX Cipher)
19. 双密码(Bifid Cipher)
20. 三分密码(Trifid Cipher)
21. 四方密码(Four-Square Cipher)
22. 棋盘密码（Checkerboard Cipher)
23. 跨棋盘密码(Straddle Checkerboard Cipher)
24. 分组摩尔斯替换密码(Fractionated Morse Cipher)
25. Bazeries密码(Bazeries Cipher)
26. Digrafid密码(Digrafid Cipher)
27. 格朗普雷密码(Grandpré Cipher)
28. 比尔密码(Beale ciphers)
29. 键盘密码(Keyboard Cipher)

4.其他有趣的机械密码

1. 恩尼格玛密码

5.代码混淆加密

1. asp混淆加密
2. php混淆加密
3. css/js混淆加密
4. VBScript.Encode混淆加密
5. ppencode
6. rrencode
7. jjencode/aaencode
8. JSfuck
9. jother
10. brainfuck编程语言

详细的加密方式讲解将会在后面的文章给出

参考

https://www.cnblogs.com/mq0036/p/6544055.html
https://ctf-wiki.github.io/ctf-wiki/crypto/introduction/