CTF

——密码学（Cryptography）

大一的萌新们，你们好呀，这里是To1in，一个大二密码手（虽然菜菜），下面会给大家简单的介绍一下CTF以及我主学的方向密码学（简称Crypto）。

CTF（Capture The Flag）中文一般译作夺旗赛，在网络安全领域中指的是网络安全技术人员之间进行技术竞技的一种比赛形式。CTF起源于1996年DEFCON全球黑客大会，以代替之前黑客们通过互相发起真实攻击进行技术比拼的方式。发展至今，已经成为全球范围网络安全圈流行的竞赛形式，2013年全球举办了超过五十场国际性CTF赛事。而DEFCON作为CTF赛制的发源地，DEFCON CTF也成为了目前全球最高技术水平和影响力的CTF竞赛，类似于CTF赛场中的“世界杯”。

——百度百科

~~（群里有一位大三学长已经打defcon了，太强啦）~~

传统的CTF分为 web、pwn、re、misc以及crypto（具体信息请自行查询，文末会给出一些链接）。大家可以通过开学后组织的0xgame来对每个方向进行一些了解，从而选择自己喜欢、合适的方向~~（当然也可以全部都要）~~。当然了，大家也是可以在这个非常闲的暑假就开始自己的CTF历程（推荐网站会在文末给出）。

学习CTF是一个漫长的过程，所以在很长的一段时间里，你参加的比赛成绩都不会很理想，甚至基本每场都会爆0（指没有一题会做，学长在写这篇入门的时候还是这个样子的hhh）。但是，请不要放弃，相信会慢慢好起来的。加油，冲冲冲！

在平常的学习中，如果遇到有疑问的或者有不会的东西，都可以问学长们~~、学姐们（莫得学姐hhh）~~，当然也可以使用搜索引擎。建议先搜索引擎自行查找，再找学长们提问。

下面的部分就是介绍一下现在CTF中密码学的知识体系了：

密码学一般分为古典密码学和现代密码学：

- 古典密码学

  古典密码学主要通过字母的替换，顺序的替换进行加密。其主要包含以下几个方面：

  - 单表替换加密
  - 多表替换加密
  - 一些奇奇怪怪的加密方式
- 现代密码学

  现代密码学起源于 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：
    - 块密码：AES、DES……
    - 流密码：LFSR、LCG、RC4……
  - 非对称加密：
    - RSA、ECC、Elgmal……
    - 格密码
  - 协议：
    - 哈希函数

    - 数字签名

学习密码学需要什么基础：

- 数学基础：一些数论知识是必须的。密码学是数学的一个应用学科，最早的公钥密码算法RSA就是基于数论的，因此学习密码学通常还需要从数论开始学起，公钥密码往后发展的过程中，也逐步用到了线性代数与抽象代数的内容。
- 编程基础：python语言，因为其拥有丰富的第三方库，并且其数字没有上限，一般选择使用python编程。
- 英语基础：你有可能会遇到一些需要阅读纯英文文章才能解决的题目，需要有一定的耐心才能看明白。

推荐书籍：

深入浅出密码学 、An Introduction to Mathematical Cryptography

最后，欢迎学弟学妹们来学习密码学，虽然这个方向的难度相对大一些，但是在学习过程中，还是有很多乐趣的。

链接：

学长博客：

- huangx607087's Blog
- To1in's blog - welcome (tolinchan.xyz)
- Am473ur Blog
- Soreat_u's Blog (soreatu.com)

学习链接：

- 密码学简介 - CTF Wiki (x10sec.org)
- ……

HERE IS WHAT YOU WANT

0xGame{Welcom_to_Cryptogrphy_World_!}