Syclover密码学入门（超级萌新向）

@r1ngs

前言

个人认为，密码学是一门数学和计算机科学交叉的学科，是信息安全专业的核心必修课。

前几天在知乎上刷到一个有趣回答：有哪些令人拍案叫绝的推理桥段？ - 大头郭师傅的回答 - 知乎

实际上，这里面的推理过程就是有的CTF（就是“亲爱的热爱的”电视剧里的比赛啦）密码学会考到的“脑洞题”的解题思路。

如果想要入坑CTF密码学的话，必须要至少掌握一门**编程语言**和学习一定的**数学知识**。

编程语言

很多萌新都选择在暑假入门学习C语言，但其实这对于CTF中的密码学来说帮助并不是很大。首先，C语言在入学的第一个学期老师就会教的，跟着老师走就行了。其次，就算学完了C语言，想要用C语言处理密码学里的大数运算是很困难或者说不容易的。

相比之下Python就方便很多了。事实上不管你是学习哪个方向的，Python都是非常重要的，必须学的。

学习Python的话首推廖雪峰的在线教程：Python 2.7教程。推荐学习Python 2.7而不是3.6，虽然这两者的差别也不是很大。

切记学习编程语言千万**不能浮躁**，不能说“我觉得这里的代码我看懂了”，“我觉得应该没有bug”这样想当然而不去动手操练。

廖雪峰的教程的话，学习到模块那一节就可以了，实际上这可能已经会花费你大半个暑假的时间了（可能还不止）。但如果真的能做到的话，开学一定会有很大的优势。

编写Python的IDE的话，推荐VScode、sublime、pycharm，这三者都是免费使用的（后两者社区版）。在配置环境等等的时候可能会遇到很多坑，在解决问题的过程你也许就会同时学到很多计算机的基础知识，如果出现什么错误的话，先要动手去百度或者谷歌，实在解决不了的话再来群里问学长学姐们。

数论

密码学里所用到数学方面的知识并不是萌新们认为的高中的函数求导、解析几何这种数学，而是和离散数学有关的一个数学分支：数论

数论主要研究的是整数之间性质，学习初等数论的话可以看这本书《密码编码学与网络安全——原理与实践》中和数论有关的章节（网上是能找到扫描版的，学校图书馆里面也有，数论章节内容比较少），主要搞懂：同余、模运算性质、逆元、欧拉定理、中国剩余定理这几个概念、公式的推导和证明就行了，然后可以用上面学的python写几个demo验证这几个数学公式是否正确。

当然，数论是一门非常深奥的学科，这里说的知识只是一点皮毛而已，如果要深入学习的话，还可以了解一下sagemath，这是一个非常强大的数学工具，集成了许多python和数学有关的库，可以让我们非常简单的处理一些抽象的数学运算，但是不推荐萌新学习，因为学习的资料太少。

密码学

接着就可以学习一点简单的密码学知识了，首先是古典密码学，古典密码学就是古代的时候常常用来加密信息的方式，现代已经很少使用，因为它们都不够安全，可以被现代计算机很容易的暴力破解。

古典密码学上面没有必要花费太多时间，了解一下常见的就行了，比如凯撒密码，维吉尼亚密码、栅栏密码。很多古典密码都是有在线加解密网站的，这里推荐两篇入门的CTF中Crypty（密码类）入门必看、密码学（Crypto）一些在线解密网站。在遇到类似题目的时候再根据题目描述去查阅就行了。

其中还涉及到了一些编码的知识，注意区别一下编码和密码。编码是每个CTF选手都必须掌握的。比如如何将需要加密的英文信息编码成参与数学运算的数字。

然后可以了解一下最著名最常考的RSA加密方式：李永乐老师11分钟讲RSA加密算法

光看这个视频肯定是不够的，结合视频上讲的和学习到的数论知识，推导一下RSA算法的正确性，搞懂公钥、私钥是什么，以及是怎么计算的，用的是什么算法，最后再思考如何用代码实现，虽然这可能有点难度。

然后就可以了解一下RSA的攻击手法了，现在常考的RSA的攻击手法都基本上来源于斯坦福大学应用密码学和计算机安全教授Dan Boneh发表的论文：

Twenty Years of Attacks on the RSA Cryptosystem

尽管国内有翻译作，但还是鼓励萌新们读英文文档，搞懂攻击的原理。只需要了解一下模不互素，共模攻击，小公钥指数这些简单的就行了。这些攻击手法的exp在ctf-wiki上有（其实也可以跟着ctf-wiki学习啦= =），可以对应类似的题目去试试怎么解密出明文来。

再然后的话就可以结合实际的情况，看看书，看看bugku的题目，更进一步的学习啦，□□永远欢迎热爱学习热爱技术的同学。

最后再唠叨一句，不论是学习什么，都要**记笔记！记笔记！记笔记！**（markdown、markdown、markdown） 作者：@r1ngs