CTF_ CRYPTO(Cryptography)_密码学/密码分析学

原创

地热tan 已于 2022-02-21 10:56:18 修改 2724 收藏
文章标签： web安全 安全
于 2022-02-19 09:51:33 首次发布

本文链接：https://blog.csdn.net/weixin_44664189/article/details/122987422

> 奶奶曾说过，教会他人，是验证自己学习的最好方式。

一、 简介：

> 密码学：主要是研究编制密码 和 破译密码的学科
>
> 密码分析学：简单来说，就是密码的破解。

二、历史

> 事实上，密码和密码分析是同一枚硬币的正反两面：为了创建安全的密码，就必须考虑到可能的密码分析。

在古代，密码分析学一直是以敌国为主导的，没人在设计上考虑到安全性， 而一个合格的密码设计者应在设计之初就分析出这款密码的弱点，防范别的人破解。

三、密码分析

- **唯密文攻击**

已知的信息是，“密文”。

这种情况实际上是比较少见的，因为攻击者面对实际的情况多多少少会得知一些明文的数据格式或者能捕获到一些明文以及其对应的密文。

- **已知明文攻击**

已知的信息是，一段“明文”和对应的“密文”。

比较常见的例子是“可能词攻击”，攻击者处理一些特定的信息，他可能知道其中的一些信息，比如电子金融消息往往有标准化的文件头或者标志，一个完整的会计文件放在文件最前面的关键词应该是固定的。这样大大减小了破解的难度，而且在这种环境下我们要求加密一定不能是线性的，否则就可以通过一部分对应关系推出了全局的关系，保密性将不复存在。

- **选择明文攻击**

已知的信息是，制造或知道某一段“明文”和其加密之后的“密文”。

如果分析者能够通过某种方式获得信源系统，让发送方在发送的消息中插入一端由他选择的信息就可以实现选择明文攻击。一个例子就是**差分密码分析**。

- **选择密文攻击**

已知的信息是，制造或知道某一段“密文”和其解密之后的“明文”。

这种攻击主要攻击公开密钥密码体制，特别是攻击其**数字签名**。

- **选择文本攻击**

此时攻击者获得了更强的攻击能力，在攻击时不仅可以构造多个明文获取相应的密文，还可以构造多个密文获取相应的明文。也就是以上两种攻击的结合体。

- **唯密文攻击**：只知道密文，也就是 c_1, c_2, c_3 ，那只能通过统计特性分析其中有什么规律了
- **已知明文攻击**：得到了一些给定的明文和对应的密文，在这里可以是 $\{(p_1, c_1), (p_2, c_2), (p_3, c_3)\}$ 的任意非空子集。
- **选择明文攻击**：除了上面的基础，攻击者还可以任意创造一条明文比如 “Excited” ，并得到其加密后的密文。比如用一定的手段渗透Sharon的系统，但是不能直接攻破秘钥，于是只能以她的身份发 “Excited” ，然后用抓包或者别的方法得到她发送出来的加密的消息。
- **选择密文攻击**：除了已知明文攻击的基础，攻击者还可以任意制造或者选择一些密文，并得到其解密后的明文。比如用一定的手段在通信过程中伪造消息替换真实消息，然后窃取Sharon获得并解密的结果，有可能正好发现随手伪造的密文解密结果是有意义的，比如naive。
- **选择文本攻击**：可以制造任意明文/密文并得到对应的密文/明文，就是上面两者的结合。

是谁还说数学难？过来看看这个跨学科的密码学？用数学表示不简单多了嘛，嚯嚯嚯