SWRhapsody

Cryptography I 课程第一周总结

于2月 25, 2018由**SWRhapsody**发布

coursera 上 Cryptography I 课程的部分知识点的总结，总结可能存在部分错误。

部分基础概念：

1.Perfect Secrecy

Suppose a cryptosystem with `|K|=|C|=|P|`. The cryptosystem has perfect secrecy if and only if

- each key is used with equal probability `1/|K|`,
- for every plaintext `x` and ciphertext `y` there is a unique key `k` such that e_k`(x)=y`.

这里主要是有两个性质，一个是key在空间中要是均匀分布的，第二个是攻击者若是拥有2条不一样的明文和一条密文，他无法区别这条密文是由哪一条明文加密得到的，同时 `p(x|y)=p(x)` 。key的长度要大于等于明文的长度。

2.Negligible Functions

定义：A function μ is negligible iff $\forall c \in N\ \exists n_0 \in N$ such that $n \geq n_0, (n) < n^{-c}$

对于这个函数一开始完全没搞明白它的意义，后来找到了资料[1]

这是个函数用来衡量成功几率的，因为Perfect Secrecy的破解几率和计算量的多少没关系，但是部署一个这样的加密在很多时候不现实也没有必要，所以当前采用的大多是让攻击者在一定计算量内无法暴力破解的算法，这里假设攻击者的尝试次数是关于n的一个多项式 `poly(n)` （多项式拟合？），n是一个用于生成key的一个参数，一般来说n与key的长度有关。

这样攻击者会尝试 `poly(n)` 次，也就是说他每次尝试的成功几率是 `1/ploy(n)` 我们只要确保对于任何一个多项式他的成功几率都低于这个就可以了，所以只要存在一个n使等式成立就可以。

SWRhapsody

参考：

[1]https://crypto.stackexchange.com/questions/5832/what-exactly-is-a-negligible-and-non-negligible-function

分类： CRYPTOGRAPHY

0 条评论

发表评论

名称 *

电子邮件 *

网站

在想些什么?

发表评论

SWRhapsody

近期文章

携程Apollo YAML 反序列化

CVE-2020-5410

CodeQL部分源码简读

服务器与网关的不一致

CodeQL 部分使用记录

近期评论

文章归档

2020年8月

2020年6月

2020年5月

2020年3月

2020年1月

2019年12月

2019年11月

2019年8月

2019年7月

2019年5月

2019年4月

2019年1月

2018年11月

2018年10月

2018年9月

SWRhapsody

2018年2月

2018年1月

分类目录

Article Collection

Cheat Sheet

cryptography

Exercise

Exploit

HackTheBox

Penetration Test

Uncategorized