隐侠

DoraHacks 2018 Security Hack

但使安全Hacker在，不教黑帽度阴山

DoraHacks

RSA与SHA-256简介

公钥密码——对公钥密码的要求

1. 对于接受方B而言，产生一对密钥，在计算上是容易的。
2. 已知公钥和要发送的消息M，发送方A产生相应的密文在计算上是容易的：C=E(Pk,M)。
3. 接收方B使用其私钥，对接受到的密文解密以恢复明文在计算上是容易的:M=D(Sk,C)=D(Sk,E(Pk,M))。
4. 已知公钥Pk时，攻击者要确定私钥Sk在计算上是不可行的。
5. 已知公钥Pk和密文C，攻击者要恢复明文M在计算上是不可行的。
6. 加密和解密函数的顺序可以交换：M=D(Pk,E(Pk,M))=D(Sk,E(Pk,M))。

RSA加密算法

RSA算法是最常见的公钥密码算法，它既能用于加密，也能用于数字签名。

RSA的安全性基于大数分解的困难度。

- RSA加密：$C = m^e \bmod n$
- RSA解密：$M = c^d \bmod n$

公钥（e,n）私钥（d,n）

RSA加密算法

RSA算法是第一个可以同时用于加密和数字签名明的算法。

RSA加密算法中，只用到素数、互质数、欧拉函数、模运算等简单的数学知识。

算法涉及到的参量：p、q、n、Φ(n)、e、d

1. n。取两个非常大的、互异的质数p，q，计算N=p*q

2. Φ(n)。 n的欧拉函数， Φ(n)=n(1-1/p)(1-1/q)

3. e。随机选取整数e，要求e和Φ(n)互质，e即为加密密钥。

4. d。计算d，令（e*d）≡1 mod Φ(n)

DoraHacks

HASH函数

Hash函数：也称为单向散列函数（one-way hash function），就是把任意长的输入消息串转化成固定长的输出串，而且由输出串难以得到输入串的一种函数。

- 特点：

1. 散列值的长度和消息长度无关
2. 消息不同散列值也不同
3. 计算速度非常快
4. 具备单向性

SHA系列

安全散列算法（英语：Secure Hash Algorithm，缩写为SHA）是一个密码散列函数家族，是美国联邦信息处理标准所认证的安全散列算法。是可以通过计算，把一个数字消息处理成固定长度的的字符串（消息摘要）的算法。

SHA家族的五个算法，分别是SHA-1、SHA-224、SHA-256、SHA-384，和SHA-512，由美国国家安全局（NSA）所设计，并由美国国家标准与技术研究院（NIST）发布,是美国的政府标准。

SHA系列

	SHA-1	SHA-224	SHA-256	SHA-384	SHA-512
消息摘要长度	160	224	256	384	512
消息长度	$<2^{64}$	$<2^{64}$	$<2^{64}$	$<2^{128}$	$<2^{128}$
分组长度	512	512	512	1024	1024
字长度	32	32	32	64	64
步骤数	80	64	64	80	80

SHA-256简介

在区块链中，sha-256常参与到钱包地址的生成，在共识机制中也有sha-256的身影。

sha-256的生成：

1. 消息填充
2. 初始化
3. 处理512bit消息分组
4. 输出hash值

THANK YOU!

DoraHacks