密码技术笔记

adamanteye

1. 总结

这篇笔记主要来自结城浩-图解密码技术.

2. 对称密码

对称密码也称共享密钥密码,用相同的密钥进行加密和解密.

2.1. 一次性密码本

一次性密码本由维纳(G.S.Vernam)于 1917 年提出,1949 年,香农从数学上证明了一次性密码本是无条件安全的,理论上无法破译.

2.2. AES

3. 非对称密码

也称公钥密码.用公钥加密,用私钥解密.

3.1. RSA

RSA 得名于三位开发者的首字母组合.

RSA 可以被用于公钥与密码签名.

公钥	(E, N)
私钥	(D, N)
加密	密文 $=$ 明文$^E \bmod N$
解密[1]	明文 $=$ 密文$^D \bmod N$

表 1　RSA 的加密与解密

生成一对 RSA 公钥和私钥的过程如下:

1. 求N

   重复生成伪随机数,直到找到 2 个大素数p, q.

   Miller–Rabin 素性测试是常用的概率性素数检测算法.

   $$N = pq$$

2. 求中间结果L

   $$L = \operatorname{lcm}(p-1, q-1)$$

3. 求E

   要求E满足

   - $1 < E < L$
   - $\gcd(E, L) = 1$

   重复生成伪随机数,检查是否满足最大公约数的要求

4. 求D

   - $1 < D < L$
   - $ED \equiv 1 \pmod L$

3.2. 椭圆曲线密码(ECC)

3.3. 安全性

3.3.1. 暴力破解

RSA　没有对大整数进行质因数分解的高效算法

ECC　椭圆曲线上的乘法运算的逆运算是困难的

对非对称密码可以被中间人攻击,中间人截获通信发起方的公钥,替换为自己的公钥,之后可伪装通信发起方.

4. 单向散列函数

也称为消息摘要函数,哈希函数.

单向散列函数承担以下功能:

- 确认完整性

MD 结构　循环执行压缩函数

MD4, MD5, SHA-1, SHA-2 等传统单向散列函数算法都是基于 MD 结构的.

海绵结构　吸收阶段,挤出阶段

Keccak 使用的结构,一种变体是双工结构.

4.1. SHA-3

Secure Hash Algorithm-3 在 2012 年被确定为 Keccak 算法.

为了配合 SHA-2 的散列值长度, SHA-3 中规定了 4 种版本:

- SHA3-224
- SHA3-256
- SHA3-384

[1] 明文需要小于N,假如大于N,取模后必定无法得到正确的明文.

- SHA3-512

4.2. 攻击

弱碰撞 知道散列值,寻找另一条消息

强碰撞 知道消息,寻找另一条散列值相同的消息

洪水攻击[2] 提交一堆准备好的频繁碰撞的键,进行拒绝服务攻击.应对方法为带密钥哈希算法.

5. 消息认证码

消息认证码(Message Authentication Code)承担以下功能:

- 确认完整性
- 认证

消息认证码有这些缺陷:

- 无法对第三方证明
- 无法防止否认

而数字签名可以解决这些缺陷.

5.1. HMAC

HMAC 是用单向散列函数构造消息认证码的方法(RFC 2104).

5.2. 应用例子

SWIFT 环球银行金融协会(Society for Worldwide Interbank Financial Telecommunication)

银行间通过 SWIFT 传递交易消息,其中使用了消息认证码.

IPsec 使用消息认证码认证通信内容,校验完整性.

6. 数字签名

数字签名是将非对称密码反过来用实现的.

	私钥	公钥
非对称密码	接受者解密	发送者加密
数字签名	签名者生成签名	验证者验证签名

表 2 非对称密码对比数字签名

7. 证书

信任需要起点.

8. 密钥

9. 随机数

10. SSL/TLS

SSL 是 1994 年由网景(netscape)设计的协议,于 1995 年发布了 3.0 版本,在 2014 年, SSL 3.0 协议被发现存在可能导致 POODLE 攻击的安全漏洞,不再安全.

1999 年, IETF 在 SSL 3.0 基础上设计了 TLS 1.0,作为 RFC 2246 发布. 2006 年, TLS 1.1 以 RFC 4346 发布,加入了 AES 对称密码算法. TLS 1.2 新增了 HMAC-SHA256 以及对 GCM, CCM 认证加密的支持,移除了 IDEA 和 DES.

[2] 什么是哈希洪水攻击