

密码学

1. 密码学定义

1.1 密码学的目的

- 机密性：消息不泄露给非授权实体
- 完整性：消息未被篡改
- 认证性：消息来源或实体本身被正确标识
- 不可否认性：用户不能在事后否认信息的生成
- 可用性：资源随时可以提供服务

1.2 密码学的分类

- 密码编码学
- 密码分析学
- 被动攻击（监听，危害机密性）
- 主动攻击

1.3 攻击

- 唯密文攻击：已知一定密文
- 已知明文攻击：已知一定明密文对
- 选择明文攻击：能选择特定的明文得到对应密文
- 选择密文攻击：能选择特定的密文得到对应明文

1.4 柯克霍夫原则

- 密码分析者已知密码算法及其实现的全部资料
- 确保密码的安全性完全依赖于密钥

2. 密码学基础

2.1 信息论

- 熵
 - 集 X 中事件出现的不确定性
 - $H(X) = -\sum p(x_i) \log_2 p(x_i)$
 - $H(XY) = H(X, Y) = -\sum \sum p(x_i y_i) \log_2 p(x_i y_i)$
 - $H(X|y_i) = -\sum p(x_i|y_i) \log_2 p(x_i|y_i)$
 - $H(X|Y) = \sum p(y_i) H(X|y_i)$
 - $H(X|Y) \leq H(X) + H(Y)$
- 计算安全性

- 破解的成本大于信息价值
- 破解的时间大于信息生命周期
- 无条件安全性
 - $H(P) = H(P|C)$

3. DES

- Feistel 结构
- 块长度: 64bit
- 密钥长度: $64\text{bit} = 56\text{bit} + 8\text{bit}$ (校验位)
- 加密轮数: 10
- S 盒: 唯一的非线性部件
- 互补性: $y = E_k(x)$ 则 $\bar{y} = E_{\bar{k}}(\bar{x})$ (选择明文攻击降低一半的时间复杂度)
- 结构
 - $L_i = R_{i-1}$
 - $R_i = L_{i-1} \oplus F(R_{i-1}, K_i)$
 - 第 16 轮左右不交换
- 轮函数
 - E 扩展 ($32\text{bit} \rightarrow 48\text{bit}$)
 - 轮密钥加
 - S 盒代换 ($48\text{bit} \rightarrow 32\text{bit}$)
 - P 盒置换
- 密钥编排
 - PC1
 - 循环左移
 - PC2 ($56\text{bit} \rightarrow 48\text{bit}$)

4. AES

- SPN 结构
- 块大小: 128bit
- 密钥长度: 128bit, 192bit, 256bit
- 加密轮数: 10, 12, 14
- 结构
 - 字节代换 (非线性)
 - 行移位 (左移)
 - 列混合 (最后一轮无)
 - 轮密钥加 (开始与结束都有)
- 密钥编排

- $W[i] = W[i - 4] \oplus W[i - 1], i \neq 4k$
- $W[i] = W[i - 4] \oplus T(W[i - 1]), i = 4k$
- T 函数使用了字节代换的 S 盒

5. 其他加密算法

5.1 商密

- SM2: 椭圆曲线
- SM3: Hash
- SM4: 广义 Feistel
- ZUC: 流密码

5.2 Hash

- MD: 密钥长度 128bit
- ZUC: 密钥长度 128bit
- SHA-0/1: 密钥长度 160bit

6. 分组密码工作模式

- ECB
 - 无法隐藏数据结构
 - 有填充、密文扩展
 - 无错误传播
- CBC
 - IV
 - 有填充
 - 有密文错误传播 (2 组)
- CFB
 - 无填充
 - 加解密均使用加密函数
 - 有密文错误传播 ($n+1$ 组)
- OFB
 - 无填充
 - 加解密均使用加密函数
 - 难以防御密文篡改
- CTR
 - 无填充
 - 加解密均使用加密函数
 - 无错误传播

7. 流密码

7.1 特征多项式

- 使 $p(x)|(x^L - 1)$ 最小的 L 为 $p(x)$ 的周期/阶
- 阶为 $2^n - 1$ 时 $p(x)$ 为本原多项式 (m 序列)
- LFSR 例子: $p(x) = x^3 + x + 1 \iff a_{n+4} = a_{n+3} \oplus a_{n+1}$

7.2 概念

- 同步流密码: 状态与明文无关 (OFB)
- 自同步流密码: 状态与明文有关 (CFB)

7.3 需求

- 周期极大
- 良好统计特性
- 抗线性分析

7.4 伪随机公设

- 0 与 1 的个数差 ≤ 1
- 长为 i 的游程占总游程数的 $\frac{1}{2^i}$, 等长游程中 0 与 1 的个数相同
- 异相自相关函数为常数 ($t \neq 0$) (自相关函数 $R(t) = \sum_{k=1}^T (-1)^a_k (-1)^{a_{k+t}}, 0 \leq t \leq T - 1$)

8. Hash

8.1 基本属性

- 压缩性: 定长输出
- 有效性: 容易计算
- 安全属性
 - 抗原像性 (2^n)
 - 抗第二原像性 (2^n)
 - 抗碰撞性 ($2^{\frac{n}{2}}$)

8.2 HMAC

- $HMAC = H(K \oplus opad || H(K \oplus ipad || M))$ oi!
- 填充: 在数据串左边填充原数据的长度, 其左边用 0 补齐

9. RSA

9.1 安全性

- $|p - q|$ 要大
- $p - 1, q - 1$ 要有大素因子
- e 不能太小
- 不同用户要使用不同 n

9.2 CRT-RSA

- 原式: $M = C^d \pmod{n}$
- 使用中国剩余定理:
 $M_1 \equiv C^d \equiv (C \pmod{p})^d \pmod{(p-1)} \pmod{p}$
 $M_2 \equiv C^d \equiv (C \pmod{q})^d \pmod{(q-1)} \pmod{q}$
- 解得: $M \equiv M_1 \cdot q \cdot q^{-1} + M_2 \cdot p \cdot p^{-1} \pmod{n}$

10. El Gamal

- $y \equiv g^x \pmod{p}$
- 公钥为 (y, g, p) , 私钥为 (x, g, p)
- 加密
 - $C_1 \equiv g^k \pmod{p}, k \in (0, 1]$
 - $C_2 \equiv y^k \cdot M \pmod{p}$
- 解密
 - $M \equiv \frac{C_2}{C_1^x} \pmod{p}$

11. ECC

- $y^2 \equiv x^3 + ax + b \pmod{p}$
- $4a^3 + 27b^2 \neq 0 \pmod{p}$
- $\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1}, & P \neq Q \\ \frac{3x_1^2 + a}{2y_1}, & P = Q \end{cases} \begin{cases} x_3 = \lambda^2 - x_1 - x_2 \pmod{p} \\ y_3 = \lambda(x_1 - x_3) - y_1 \pmod{p} \end{cases}$

12. ECC-El Gamal

- $E_p(a, b), P_A = xG$
- 加密
 - $C_1 = kG$
 - $C_2 = H(M) + kP_A$
- 解密
 - $H(M) = C_2 - xC_1$
- 1024 位的 RSA 安全强度与 160 位的 ECC 相近

13. 数字签名

13.1 信息安全 CIA

- 机密性
- 完整性
- 可用性

13.2 签名的安全模型

- 唯密钥攻击：已知公钥
- 已知消息攻击：知一定消息签名对
- 选择消息攻击：能选择特定的消息签名对

13.3 签名的攻击结果

- 存在性伪造：可生成一些消息的签名
- 选择性伪造：可生成特定消息的签名
- 一致性伪造：可生成任意消息的签名
- 完全破译：可获得私钥

13.4 签名认证方式

- 外部保密方法：先签名后加密（建议）
- 内部保密方法：先加密后签名

14. El Gamal 签名

- 签名

$$\begin{aligned} r &= g^k \pmod{p} \\ s &= (H(M) - xr)k^{-1} \pmod{p-1} \end{aligned}$$

- 验签

$$y^r r^s = g^{H(M)} \pmod{p}$$

- k 不能泄露
- 每次使用不同的 k

15. DSA 签名

- 签名

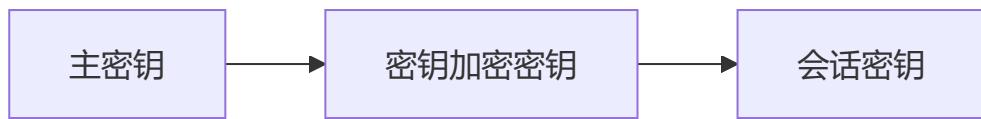
$$\begin{aligned} r &= g^k \pmod{p} \pmod{q} \\ s &= (H(M) + xr)k^{-1} \pmod{q} \end{aligned}$$

- 验签

$$r = g^{H(M)s^{-1}} \pmod{q} y^{rs^{-1}} \pmod{q} \pmod{p} \pmod{q}$$

16. 密钥分层管理

16.1 结构



16.2 好处

- 提高安全性
- 密钥管理自动化
- 提高效率

17. DH

- 中间人攻击
 - 使用数字签名防御