思科认证辅导:信息安全(密码学基础)思科认证 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/590/2021_2022__E6_80_9D_E7_A7_91_E8_AE_A4_E8_c101_590392.htm 初学信息安全的朋友最初接触到的应该不例外的都是密码学，作为基础，我们应该掌握好其原理和机制，而针对算法的问题，我在以后的文章中会陆续提及，但对于一般的朋友来讲，不用过多深究各类算法，鉴于本人能力有限，涉及的面深度或广度均有所欠缺，仅供初学者们学习和交流所用。 密码学是一门研究秘密信息的隐写技术的学科 密码学技术可以使消息的内容对(除发送者和接收者以外)的所有人保密. 可以使接收者验证消息的正确性，是解决计算机与通信安全问题重要技术之一. 基本术语：密码技术（Cryptography）把可理解的消息变换成不可理解消息，同时又可恢复原消息的方法和原理的一门科学或艺术。 明文（plaintext ）--变换前的原始消息 密文（ciphertext ） --变换后的消息 密码（cipher ）--用于改变消息的替换或变换算法 密钥（key ）--用于密码变换的，只有发送者或接收者拥有的秘密消息 编码（encipher /encode）--把明文变为密文的过程 译码（decipher /decode)把密文变为明文的过程 基本概念：Encryption 把明文变成密文的加密函数 C = EK(P) Decryption 把密文变成明文的加密函数 P = EK-1(C) key 用于加密或解密的秘密参数, 选自密钥空间 K （一般情况下，可以把密码系统理解成可逆的密码算法、密钥空间，即：加密算法：EK. K in K : P -gt. P ） *通常密码系统是公开的， 只有密钥是秘密信息* 密码学算法大致分为: 私钥加密算法(private-key encryption algorithms ) ----分组密码,-----流密码

公钥加密算法(public-key encryption algorithms) 数字签名算法(digital signature algorithms ) 哈希函数（hash functions） 密码分析（又可称为攻击）: 密码分析学是指在没有加密密钥的情况下,攻击密文的过程 唯密文攻击 (ciphertext only ) --只知道算法与一些密文 --利用统计方法 --需要能够识别明文 gt. 唯密文攻击 (ciphertext only ) --只知道算法与一些密文 --利用统计方法 --需要能够识别明文 已知明文攻击（known plaintext ） ---- 知道一些明文/密文对 ----利用已知的明文密文对进行攻击 选择明文攻击（chosen plaintext ） ----能够选择明文并得到响应的密文----利用算法的结构进行攻击 选择密文攻击（chosen ciphertext ） ----能够选择密文并得到对应的明文 ----利用对算法结构的知识进行攻击 选择明文-密文对攻击（chosen plaintext-ciphertext ） ----能够选择明文并得到对应的密文或选择密文并得到对应的明文 ----利用对算法结构的了解进行攻击 穷密钥搜索 理论上很简单，对每个密钥进行测试 最基本的攻击方法，复杂度有密钥量的大小决定 假设可以对正确的明文能够识别 *无条件安全与计算安全 无条件安全（unconditional security） 由于密文没有泄露足够多的明文信息，无论计算能力有多大，都无法由密文唯一确定明文。 计算安全（computational security ） ----在有限的计算资源条件下，密文不能破解。 （如破解的时间超过地球的年龄） 更多优质资料尽在百考试题论坛 百考试题在线题库 思科认证更多详细资料 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com