信息安全复习

第 1 章 引言

信息安全

计算机安全

网络安全

计算机安全的目标

保密性 Confidentiality

完整性 Integrity

可用性 Availability

真实性 Authenticity

可追溯性 Accountability

访问控制 Access Control

安全的 3 个方面

Security attack（安全攻击）：危及信息系统安全的行为

Security service（安全服务）：加强数据处理系统和信息传输安全性的处理过程或通信服

Security mechanism（安全机制）：检测、阻止、或从安全攻击中恢复的过程或设备

注：

Attack（攻击）-对系统安全的攻击，是行为

Threat（威胁）－破坏安全的潜在可能，是弱点被利用而可能带来的危险，是可能性

安全攻击

1. 被动攻击

- 明文窃听
- 流量分析

难于检测，重在预防

2. 主动攻击

- 伪装/假冒
- 重放
- 篡改
- 拒绝服务

难于预防，重在检测

安全服务

数据保密性 （加密：明文变密文）

数据完整性 （发现篡改假冒）

可用性

认证 （你是谁,你来自谁）

访问控制 （你能干什么，授权）

不可否认性 （防止对收发消息的抵赖）

安全机制

安全服务通过安全机制来实现安全策略

两类机制

（1）在特定的协议层次实现

（2）不属于特定的协议层次

网络安全模型

传输安全

系统安全

要素：

1. 安全变换
2. 共享秘密

体现形式	对应机制
黑客	门卫

病毒等恶意代码	监控程序

第 2 章 传统加密技术

密码学

明文：原始的消息

密文：加密后的消息

密钥：一段信息，是在明文转换为密文或将密文转换为明文的算法中输入的参数。通常分为对称密钥与非对称密钥。

加密：从明文到密文的变换过程

解密：从密文到明文的变换过程

密码体制(cryptographic system)或密码：加密方案

密码学（cryptology）

密码编码学（cryptography）：研究各种加密方案的领域

密码分析学（cryptanalysis）：在不知道任何加密细节的条件下解密消息的技术

对称密码模型

5 个基本要素

明文 plaintext

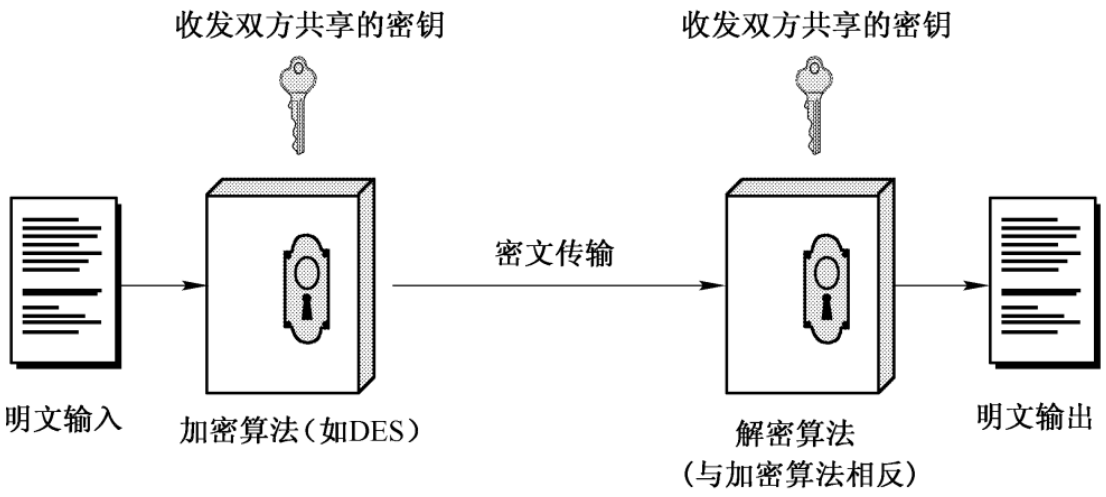
密文 ciphertext

密钥 key

加密算法 encryption algorithm

解密算法 decryption algorithm

简化的传统加密模型



保密系统的通信理论

1. 理论安全性

只有当密钥和明文一样长时才能完全保密，即 one time pad

2. 计算安全性

理论上并不完美，但在实践中难以攻破

满足任意一条：

- 破译密码的时间超出密文信息的有效生命周期
- 破译密码的代价超出密文信息的代价

密码编码学系统特征

运算类型

- 代替 substitution 明文元素映射为密文元素

- 置换 transposition 把明文元素重排

密钥数

- 对称密钥
- 非对称密钥

处理明文的方法

- 分组密码：每次处理输入的一组元素，相应地输出一组元素
- 流密码：连续地处理输入元素，每次输出一个元素

基本原则

算法公开

密钥的随机性

密码分析学

目标：恢复密钥，而不仅仅是单个明文

1. 唯密文攻击

只有一些密文

2. 已知明文攻击

知道一些过去的(明文及其密文)作参考和启发

3. 选择明文攻击

缴获有一台加密机（还能加密选择的明文）

少用但可能:

4. 选择密文攻击

有一台解密机（能解密选择的密文）

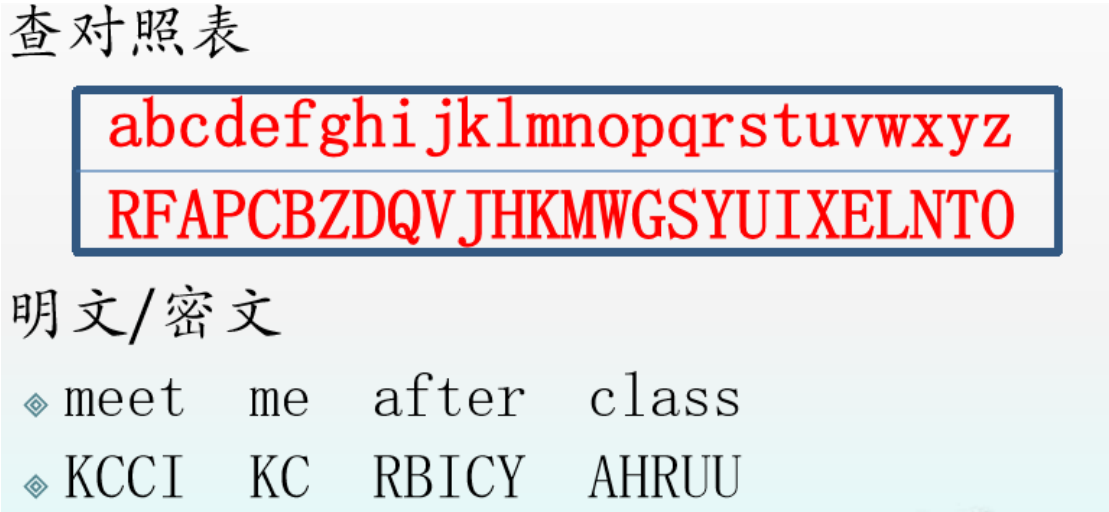
5. 选择文本攻击

有解密机、解密机

代替技术

Caesar 密码→移位密码

单表代替密码 Monoalphabetic Cipher（Substitution）



没有去除统计规律

减少代替密码中明文结构：

对明文中的多个字母一起加密

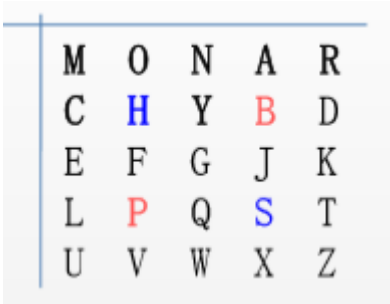
采用多表代替密码

Playfair 密码

简化 I 同 J（U 同 V）

规定：

加密：取对角线，同行取右，同列取下



M	O	N	A	R
C	H	Y	B	D
E	F	G	J	K
L	P	Q	S	T
U	V	W	X	Z

如 hs→BP, tm→LR

ar→RM，mu→CM

解密：同行取左，同列取上

多表密码 Polyalphabetic Cipher

使用多个(单)表，比如 Vigenère

根据密钥字母a-z，每个表移位0-25次：

key(repeat)	deceptive	deceptive	deceptive
Plaintext	wearedisc	overedsav	eyourself
Ciphertext	ZICVTWQNG	RZGVTWAVZ	HCQYGLMGJ

一次一密 one-time pad

唯一具有理论安全性的算法

置换技术

转轮机 Rotor

第 3 章 对称算法 DES

分组密码算法原理

明文被分为固定长度的分组，对每个分组用相同的算法和密钥加解密

一般为 64 或 128 比特

密文分组和明文分组同样长

用户要共享一个对称密钥

流密码算法(Stream Cipher)

每次可以加密一个比特或一个字节

适合远程终端输入等应用

流密码可用伪随机数发生器实现

共享一个生成密钥做为随机数种子，产生密钥流 keystream (不重复，或极大周期)

XOR (plaintext，key-stream)

One-time Pad

比较

基本区别

粒度：8 字节分组 vs. 1 比特或 1 字节

各自适应不同的应用数据格式

对相同的明文分组：分组密码总是相同的密 文分组；流密码却输出不同的密文比特

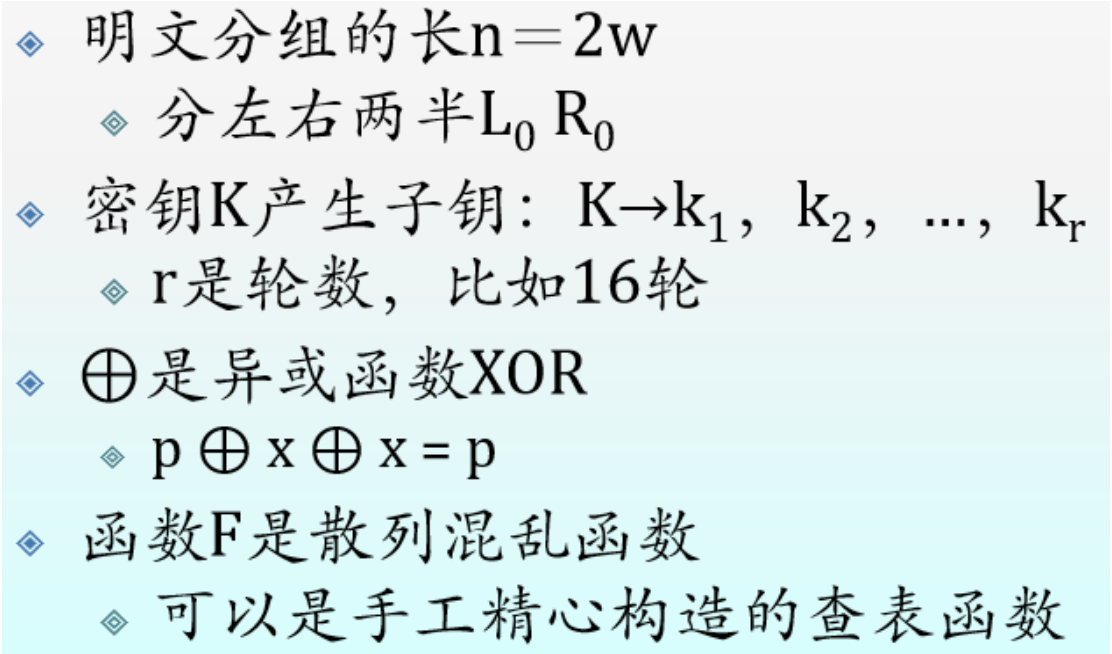
流密码速度一般快很多

分组密码多些，是主流

分组密码也可以用作流模式

Feistel(DES)加密框架

设计：用**乘积密码**逼近理想分组密码。依次使用 两个或以上的基本密码重复进行**代替和置换**，实现**混乱和扩散**。



Feistel 参数特性

分组大小

密钥大小

循环次数

一般仅几轮是不够的，得十几轮才好，如 16 轮

子钥产生算法--越复杂越好

轮函数 Round--关键

其他考虑

速度（尤其是软件实现的速度）

便于分析（使用简洁的结构）

Data Encryption Standard DES

参数

Feistel 体制分组密码

分组大小 64bit，密钥大小 56bit，轮数 16 轮

S-Boxes

DES 弱密钥 4 子密钥相同

半弱密钥 12 两个子密钥，互为加解密

可能的弱密钥 24 四个子密钥

差分分析

线性分析

3DES

三个递进思路：

用 2 个 key，加密 2 回

用 3 个 key，加密 3 回

用 2 个 key，加密 3 回

中间相遇攻击

由于 $C=E_{K2}(E_{K1}(P))$，故存在中间值 $X=E_{K1(}P)=D_{K2}(C)$

工作模式

工作模式是一项增强密码算法或者使算法适应具体应用的技术

五种工作模式

ECB: Electronic Codebook 电子密码本方式

报文被顺序分割分成 8 字节分组

各个分组独立加密，解密时需等齐整个分组

填充

优点：并行加密、随机存取

缺点：

Padding

相同的明文分组对应着相同的密文分组--暴露了统计规律

替换或乱序重排攻击

CBC: Cipher Block Chaining 密文分组链接方式

当前明文分组先和前一个密文异或，再加密

初始向量 IV －initialization vector IV 不必保密，但必须一致

优点

避免明密对应

还可以用做认证 authentication

缺点

等待缓冲区凑足 8 字节分组，否则需 padding

不能并行加密、随机存取

CFB: Cipher Feedback 密文反馈方式

IV 64bit，作为 b 位移位寄存器 R 的初始值

IV 不必保密，但是必须相同

明文 s(s<b)比特，与加密得到 R 的高位 s 比特异或，得密文 s 比特

s 比特的密文同时从 R 的低位进入，挤掉 R 的 高位的 s 比特

优点:流密码 stream cipher、也有校验的效果

OFB: Output Feedback 输出反馈方式

一种流方式应用

重复加密初始向量 IV，获得密钥流

IV 不必保密，但是双方得一致

明文与之 XOR

优点:比特错误不会扩散（如 C1 出错，卫星通信）

缺点:正是优点的反面。攻击者篡改密文位，则相应的明文位也取反。

CTR: Counter Mode 计数方式

一种流方式应用，但是可以非顺序存取

重复加密初始 counter＋＋，得密钥流

明文与之 XOR

优点：适合随机存取

注意：Counter 的初值须不能预测

AES

AES 要求

对称分组算法

支持标准密码本方式（ECB 模式）

要明显比 3DES 安全而且快速

密钥长度可变，128、192、256 等可选

计算上较小的时间、空间复杂性

便于软、硬件方式及各种场合实现

公开和免费许可

公开定义、公开评估、公正公开的选择

可同时供政府和商业使用

基本参数

分组大小 128bits，被分为 4 组×4 字节处理

密钥典型 128、192、256bits

非 Feistel 结构

设计出发点

安全，抵抗已知的攻击方法

代码紧凑，速度够快，适合软硬件实现

结构简单/简明/简洁

RSA

基本原理

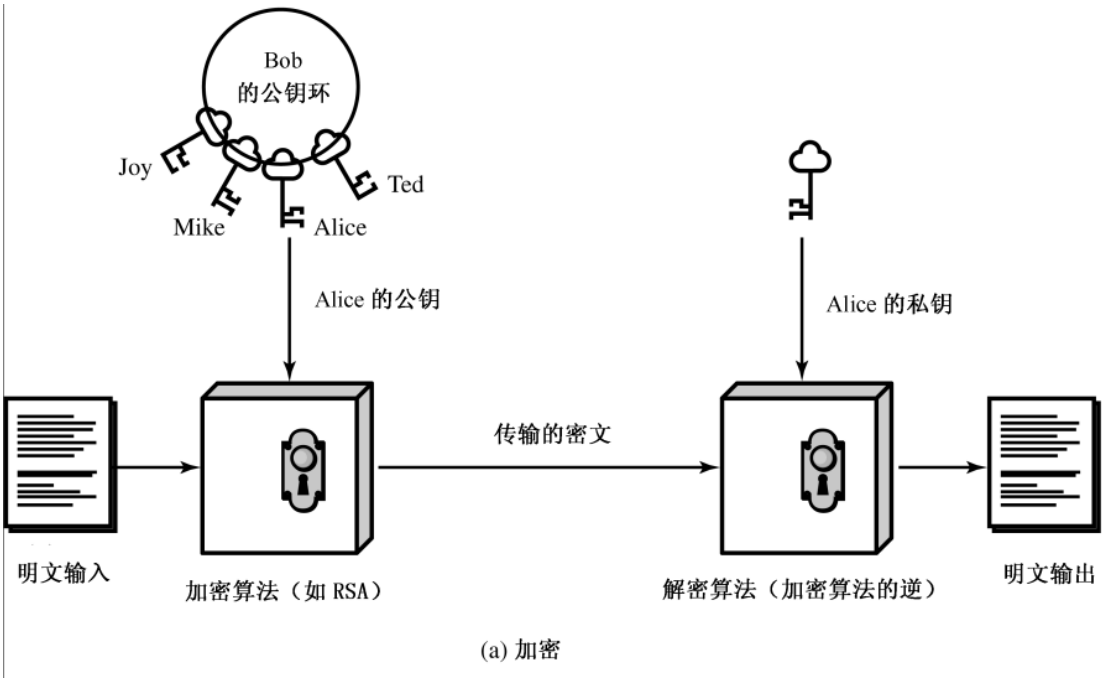
公钥算法提出的本身就是一个进步。

遵从公钥体制，能够简化密钥管理，能够 实现数字签名等安全特性。

和对称密钥不同，公钥体制的形式和结构 导致它必须基于某种数学结构，而不使用替代和置换等初等方法。

从形式上看，公钥算法将比对称算法更简 洁和易于理解。

公钥算法加密：



公钥算法：认证消息

公钥算法：认证身份

RSA 算法参数建立

找素数

选取两个 512bit 的随机质数 p, q

计算模 n 和 Euler 函数 $\Phi(n)$

n＝pq

ϕ(n)=(p-1)(q-1)

选取数 e，用扩展 Euclid 算法求数 d，使 ed≡1 mod ϕ(n)

发布

发布(e, n)，这是公钥 ke

d 保密，(d, n)是私钥 kd

RSA 加解密

加密：明文分组 m 做为整数须小于 n c=me mod n

解密 m=cd mod n

对称算法 vs. 公钥算法

安全性

速度

典型相差 1000 倍

密钥管理

对称算法需要额外安全信道

公钥：证书中心 CA

混合密码体制

公钥算法用于签名和认证

用公钥算法传输会话密钥

用会话密钥/对称算法加密批量(bulk)数据

第 10 章 公钥密钥管理 及其他公钥体制

公钥的分配方法

1. 自由扩散(临时索要公钥，PGP 的公钥环）

2. 公开目录(在线方式) ：性能瓶颈

3. 公钥授权(在线中心方式) ：单点故障和性能瓶颈

4. 公钥证书(离线中心方式，证书中心 CA)：证书作废列表

Diffie-Hellman 密钥交换协议

步骤

选取大素数 q 和生成元 g，这些参数公开

A 选择随机数 Xa，B 选择随机数 Xb

A 计算 Ya＝g^Xa mod q，B 计算 Yb＝g^Xb mod q

交换 Ya，Yb

A 计算 K＝Yb^Xa mod q，B 计算 K'＝Ya^Xb mod q

事实上，K＝K'

第 14 章 认证应用系统

LAN 上的安全：服务器、工作站、用户

Kerberos 动机

目标

- 安全性：防窃听，防假冒
- 可靠性：高可用性，分布式服务器结构
- 透明性：用户除了输入口令，不需知道认证细节
- 可伸缩性：可支持大量客户端和服务器，适应模块 化和分布式服务
- 鉴别 Authentication
- 授权 Authorization
- 记帐 Accounting

第 11 章消息认证和 Hash 函数

消息认证是验证消息完整性的一种机制，能 发现对消息的篡改或假冒。

- 使用对称算法可产生消息鉴别码 MAC
- 使用公钥算法可对消息进行签名

身份认证是鉴别通信对方的身份是否属实

Hash 函数是一个单向的消息摘要函数，在产生 MAC、签名中有重要用途