第一章：概述

1. 无线通信的分类

(1) 按通信距离划分：采用分组交换协议

① 无线个域网 (PAN:Bluetooth)
② 无线局域网 (LAN:WLAN)
③ 无线城域网 (MAN:Wimax)
④ 无线广域网 (WAN:3G/B3G)

(2) 按应用类型划分：移动通信、无线网络

2. 信息安全

(1) 信息安全模型

(2) 信息安全框架：三个方面

① 机密性：保证机密信息不被窃听，或窃听者不能了解信息的真实含义。
② 完整性：保证数据的一致性，防止数据被非法用户篡改。
③ 可用性：保证合法用户对信息和资源的使用不会被不正当地拒绝。

(3) 安全攻击常见类型，分类：主动和被动

(4) 安全服务的类型及概念

(5) 安全机制

3. 古典密码学

(1) 古典密码的基本加密方法：密码术（Cryptology）

① 置换：改变明文字母排列顺序
② 代换：明文的字母由其他字母或数字或符号代替

(2) 古典加密破解者使用的方法：暴力破解（穷举攻击）

(3) 多表代换密码的概念

① 使用两个或两个以上的密码表
② 交替使用

(4) 维吉尼亚密码

① 以移位代换为基础的周期代换密码；
② m 个移位代表由 m 个字母组成密钥字；
③ 字母 a b c d… x y z 分别由数字 0 1 2 3 …24 25 表示；
④ 加密时：明文字母 Pi 在密钥 Ki 的作用下向后移位 d（Ki），得到密文字母 Ci，
⑤ 解密时：密文字母 Ci 在密钥 Ki 的作用下向前移位 d（Ki），得到明文字母 Pi。
⑥ 维基尼亚表：26x26 矩阵表示 26 种排列组合

第二章 密码学

1. 乘积密码概念

乘积密码就是以某种方式连续执行两个或多个密码，以使得所得到的最后结果或乘积从密码编码的角度比其任意一个组成密码都更强。（百度）

（ppt)由于语言的统计特性使得使用替换或置换进行加密并不安全，可以交替的使用多种加密方式: ①两种替换得到更复杂的替换结果；②两种置换得到更复杂的置换结

果；③替换后再进行置换得到的结果相对更复杂。

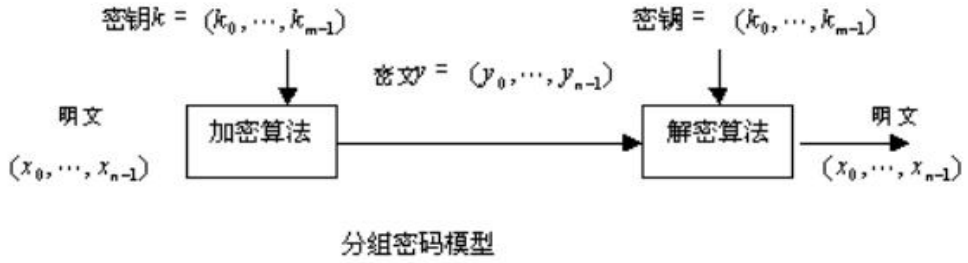
2. 对称密钥和非对称密钥的概念

(1) 对称密码算法（Symmetric cipher）：加密密钥和解密密钥相同，或实质上等同，即从一个易于推出另一个。又称传统密码算法、秘密密钥算法或单密钥算法。

(2) 非对称密码算法（Asymmetric cipher）：加密密钥和解密密钥不同，从一个很难推出另一个。又叫公钥密码算法。其中的加密密钥可以公开，称为公开密钥，简称公钥；解密密钥必须保密，称为私人密钥，简称私钥。

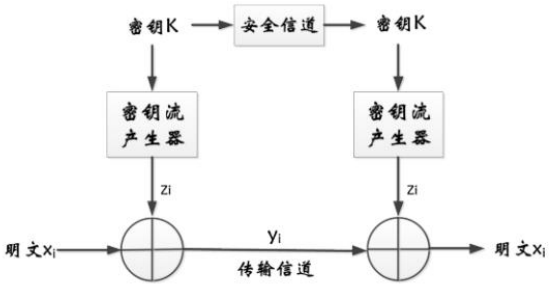
3. 分组加密和流加密的概念

(1) 分组密码（Block cipher）：将明文分成固定长度的组，用同一密钥和算法对每一块加密，输出也是固定长度的密文。分组密码是将明文消息编码表示后的数字（简称明文数字）序列，划分成长度为 n 的组（可看成长度为 n 的矢量），每组分别在密钥的控制下变换成等长的输出数字（简称密文数字）序列。分组密码模型如下：



分组密码模型

(2) 序列密码（Stream cipher）：又称流密码，序列密码每次加密一位或一字节的明文。流密码模型如下：



4. Kercheff 原则

科克霍夫假设：密码分析者知道双方使用的密码系统，包括明文的统计特性、加解密体制等，唯一不知道的是密钥。即使密码系统的任何细节已为人悉知，只要密钥未泄漏，它也应是安全的。

5. 穷举攻击（暴力破解）的概念

对密码进行逐个推算，直到找出真正的密码为止的一种攻击方式。理论上可破解任何一种密码，问题在于如何缩短破解时间。

6. 攻击类型

唯密文攻击（cybertext only attack）：
- 密码分析者知道一些消息的密文（加密算法相同），并且试图恢复尽可能多的消息明文，并进一步试图推算出加密消息的密钥（以便通过密钥得出更多的消息明文。

已知明文攻击（known plaintext attack）：
- 密码分析者不仅知道一些消息的密文，也知道与这些密文对应的明文，并试图推导出加密密钥或算法（该算法可对采用同一密钥加密的所有新消息进行解密。

旁路攻击（side channel）
- 通过收集“外面”的信息来破解密码，而不是直接处理“里面”的东西。
- 检测加解密过程所消耗的能量，所释放的辐射来计算过程时间。

重放攻击（replay attack）
- 攻击者捕获了一些类型的数据并重新提交它，寄希望于欺骗接收设备误以为这些是合法信息。
- 时间戳和序列号是对付重放攻击的两个对策。

统计式攻击
- 利用明文的已知统计规律进行破译的方法。密码破译者对截获的密文进行统计分析，总结出其统计规律，并与明文的统计规律进行对照比较，从中提取出明文和密文之间的对应或变换信息。

选择明文攻击（chosen plaintext attack）：
- 密码分析者不仅知道一些消息的密文以及与之对应的明文，而且可以选择被加密的明文（这种选择可能导致产生更多关于密钥的信息），并试图推导出加密密钥或算法（该算法可对采用同一密钥加密的所有新消息进行解密）。（暂时控制加密机）

选择密文攻击（chosen ciphertext attack）：
- 密码分析者能够选择不同的密文并能得到对应的明文，密码分析的目的是推导出密钥。（暂时控制解密机）

7. 无条件安全和计算安全的概念

(1) 无条件安全：（ppt）一次一密。

（百度）一个加密算法是无条件安全的，如果算法产生的密文不能给出惟一决定相应明文的足够信息。此时无论敌手截获多少密文、花费多少时间，都不能解密密文。Shannon 指出，仅当密钥至少和明文一样长时，才能达到无条件安全。也就是说除了一次一密方案外，再无其他的加密方案是无条件安全的。

(2) 计算上安全：（ppt）破译的代价超出信息本身的代价；破译的时间超出信息自身的生命周期。

（百度）

理论上，除一文一密外，没有绝对安全的密码体制，通常，称一个密码体制是安全的是指计算上安全的，即：密码分析者为了破译密码，穷尽其时间、存储资源仍不可得，或破译所耗资材已超出因破译而获得的获益。

8. 混淆和扩散的概念

(1) 混淆：使密文与明文之间的关系复杂。
- 通过使用一个复杂的，非线性的代换操作（S box）
- 在理想密码系统中，密文的所有统计特性都与所使用的密钥独立。

(2) 扩散：扩散增加明文的冗余度。
- 增加明文与密文之间的相关性：将每一位明文数字的影响尽可能地散布到多个输出密文数字中去，以更隐蔽明文数字的统计特性。
- 一个好的算法设计是：改变输入的 1 位，输出的一半为数会发生改变。

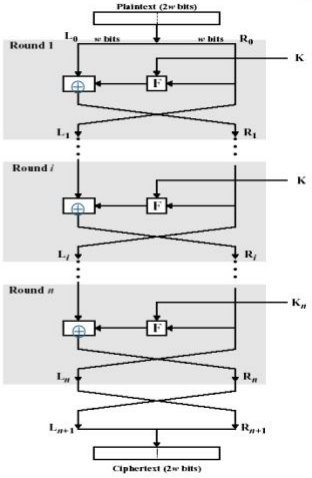
9. DES 算法 教材 78

(1) **Feistel 架构** 教材 76 页

- 多轮迭代
- 先代换（异或）
  后置换（左右两部分交换）。
- 每轮迭代输入分为两部分L_{i-1}和R_{i-1}。
- 第i轮：

$$L_i = R_{i-1}$$

$$R_i = L_{i-1} \oplus F(K_i, R_{i-1})$$



(2) 基本参数：密钥长度，明文长度

DES 是一种对称密钥算法，密钥长度为 56bits（加上奇偶校验，通常写成 64bits）。分组加密算法，64 bits 为一个分组。

(3) 三重 DES 教材 136 页

10. AES 算法 教材 109 页

(1) 基本架构：Rijndael 算法，采用置换组合结构，将处理的数据看成一个 4*4 的字节矩阵，每轮所有的数据都参与运算。

(2) 基本参数：密钥长度（128/192/256 bits），明文长度（128 bits）

(3) **工作模式**

概念：分组加密只处理固定长度的明文

▪ DES 处理的明文长度为 64 位 ▪ 在现实中我们需要处理任意长度的明文

五种常见的 教材 136 页

① ECB 模式：ECB 加密有可能保存数据的结构特征

② CBC 模式：用途：大数据量的明文加密，认证。

③ CFB 模式：用途：流加密，认证

④ OFB 模式：反馈过程与明文独立，因此可以先计算。在有噪声干扰的信道上进行流加密。

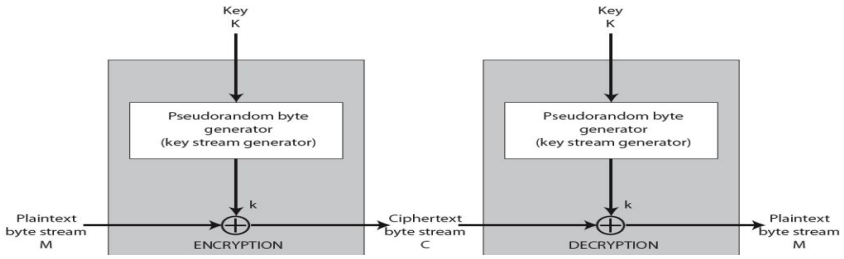
⑤ CTR 模式

11. 流加密教材 179 页 一位一位处理，好像流一样。

(1) 架构

① 密钥流：伪随机序列，伪随机数是使用一个确定性的算法计算出来的，似乎是随机的数序。因此伪随机数实际上并不随机。

② 明文与密钥流逐位 XOR



(2) 需注意的问题

① 密钥流周期要长。

② 统计上随机

③ 密钥流的随机性与密钥长度有关

如果设计得当，则流密码的安全性与分组密码相当，且实现简单，运算速度快。相同密钥不能加密不同明文，即同一密钥不能用两次。

12. 公钥密码

(1) 单向函数、单向陷门函数

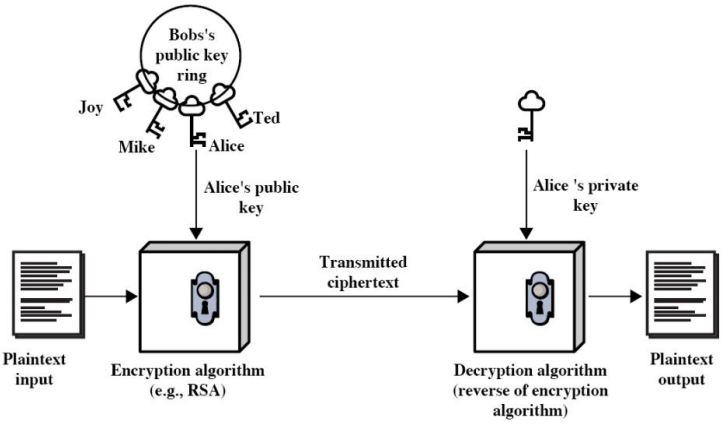
① 单向函数：▪函数值计算很容易 ▪逆计算是不可行的。

② 单向陷门函数：▪函数值计算很容易 ▪若知道某种附加的信息，则逆计算是可行的，否则不可行

❖ **单向函数**
- $Y = f(X)$ 容易
- $X = f^{-1}(Y)$ 不可行

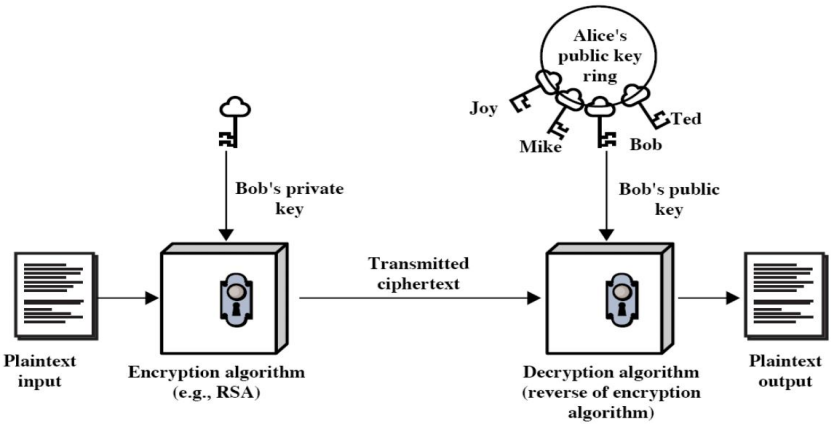
❖ **单向陷门函数**
- $Y = f_k(X)$ 给定k和X, 容易
- $X = f_k^{-1}(Y)$ 给定k和Y，容易
- $X = f_k^{-1}(Y)$ 给定Y但k未知，不可行

(2) 如何利用公钥密码算法进行加密



(a) Encryption

(3) 如何利用公钥密码算法进行认证



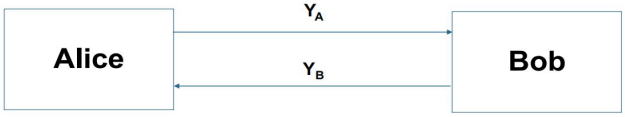
(b) Authentication

(4) RSA 算法教材 199 页

- **找素数**
  - 选取两个随机素数p, q
- **计算模n和Euler函数 $\phi(n)$**
  - $n=pq$
  - $\phi(n)=(p-1)(q-1)$
- **随机选择加密密钥e，使e和$(p-1)(q-1)$互素，利用欧几里德扩展算法找**
  - $ed \equiv 1 \mod \phi(n)$
  - $d=e^{-1} \mod \phi(n)$
- **发布**
  - 发布(e, n)，这是公钥k_e
  - d保密，(d, n)是私钥 k_d

(5) Diffie-Hellman 密码交换协议教材 214 页

- **基于计算离散对数的难度的基础上的。**



随机生成秘密参数X_A：$X_A<q$

计算Y_A：$Y_A=a^{X_A} \mod q$

$K = (Y_B)^{X_A} \mod q$

随机生成秘密参数X_B：$X_B<q$

计算Y_B：$Y_B=a^{X_B} \mod q$

$K = (Y_A)^{X_B} \mod q$

公开素数q和本原根a

例子:

素数q = 97, 本原根 $\alpha = 5$

A和B的秘密参数分别是：$X_A = 36$，$X_B = 58$

计算：$Y_A = 5^{36} \mod 97 = 50$

$Y_B = 5^{58} \mod 97 = 44$

A计算K

$K = (Y_B)^{X_A} \mod 97 = 44^{36} \mod 97 = 75$

B计算K

$K = (Y_A)^{X_B} \mod 97 = 50^{58} \mod 97 = 75$

攻击者可以得到的信息：

$q = 97, \alpha = 5, Y_A = 50, Y_B = 44$

(6) 关于公钥密码学的几点认识

① 公钥算法是基于数学函数而不是基于替换和置换。

② 公钥算法是非对称的，它使用两个独立的密钥，加密和解密各使用不同的密钥。

③ 两个密钥必须保密其中一个。

④ 若知道算法、其中一个密钥去推导另一个密钥是不可行的。

(7) 关于公钥密码学和对称密码学的比较：三个问题

① 问题 1：从密码分析的角度上看，公钥密码是否比传统密码更安全？▪ 密码的安全性依赖于密钥数量的空间大小和破译密文所花费的计算量。从密码分析角度看，不存在谁比谁更安全的问题。

② 问题 2：公钥密码比传统密码要先进，可以取代传统密码？▪ 公钥密码算法所需计算量大，所以应用领域有限，主要用于身份认证和签名，无法取代现有的传统密码。

③ 问题 3：传统密码密钥分配是很麻烦的事，公钥密码的密钥分配则很简单？▪ 使用公钥算法也需要处理密钥分配问题，其过程并不比传统密码更简单，也不比之更有效。

13. 密钥管理 教材 307 页

(1) 范围：密钥的生存周期、密钥的产生、密钥的分配、密钥管理的其他阶段（使用、存储、更新、备份、销毁）

密钥管理

- 在一种安全策略指导下密钥的产生、 存储、分配、删除、归档及应用。
- 处理密钥自产生到最终销毁的整个过程中的有关问题包括系统的初始化、密钥的产生、存储、备份/恢复、装入、分配、保护、更新、泄露、撤销和销毁等内容。
- 所有的密码技术都依赖于密钥的保密。
- 密钥的管理本身是一个很复杂的课题而且是保证安全性的关键点。
- 密钥管理方法因所使用的密码体制对称密码体制和公钥密码体制而异。

所有的密钥都有生存期

- 密钥的生命周期：授权使用该密钥的周期。一个密钥主要经历以下主要阶段：
  - 产生、登记、存储、分发、注入、应用、更换和销毁
- 原因：
  - 1 拥有大量的密文有助于密码分析一个密钥使用得太多了会给攻击者增大收集密文的机会.
  - 2 假定一个密钥受到危及或用一个特定密钥的加密/解密过程被分析则限定密钥的使用期限就相当于限制危险的发生.密钥的生存期。

(2) 密钥分配的方法

① 无中心的密钥分配模式

② 中心化密钥分配模式

③ 公钥密码体制的密钥分配

(3) 基于公钥算法的密钥分配

① 流程如下：

- A用B的公钥加密A的身份和一个一次性随机数N_1后发给B。
- B解密的N_1，并用A的公钥加密N_1和另一个一次性随机数N_2后发给A。
- A用B的公钥加密N_2后发给B。
- B选取一个会话密钥Ks，用B的私钥加密后再用A的公钥加密，发送给B。
- A用A的私钥和B的公钥解密得Ks 。

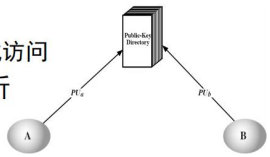
② 公钥的分配问题

1) 公开发布

- 使用者将自己的公钥发送给接收者或广播给所有人。
  - 例如：PGP用户将PGP公钥附在发送消息后或直接通过新闻组及邮件列表散布。
- 缺点：易于伪造
  - 任何人都可以创建一个密钥，并宣称是A的并进行散布。
  - 在伪装被发现之前，假冒者一直可以伪装成用户A。

2) 公开可访问的目录

- 在一个公开目录上注册密钥可以获得更大程度的安全性
- 目录必须是可信任的：
  - 包含〔姓名，对应的公钥〕
  - 用户可以在目录上安全的进行注册
  - 用户可以随时替换公钥
  - 目录定期发布
  - 目录可以通过网络方式访问
- 仍然容易被伪装和窃听



3) 公钥机构(Public-Key Authority)

- 通过严格控制目录的公钥发布来提高安全性
- 要求用户可靠知道维护公钥目录机构的公钥
- 用户通过与目录的交互以安全的得到需要的公钥
  - 要求：用户需要得到公钥时可以实时访问目录。
- 用户A和用户B通信的时候要求相互认证以保证公钥的时效性（不是过期的）。
- 缺陷：
  - 瓶颈问题：每次通信都需要访问公钥机构
  - 目录仍然容易被篡改

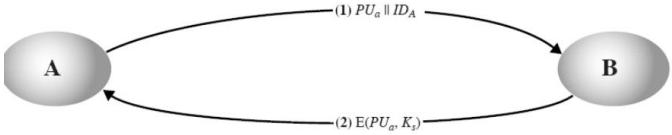
4) 公钥证书

- 提供一种跟公钥机构一样安全可靠的机制，但不需要直接访问公钥机构。
- 公钥证书
  - 将用户的身份和用户的公钥绑定在一起
  - 通常还需要其他信息，例如有效期限，使用的权限等
  - 所有的内容由可信的第三方或者证书机构签发

③ 使用公钥加密分配对称密码体制的密钥教材 313 页

简单的密钥分配（Merkle's）

- Alice生成一临时公/私钥对，并将她的公钥和标示ID_A发给Bob
- Bob生成会话密钥Ks，并用 Alice的公钥加密发给A
- A解密后得到会话密钥Ks，双方用Ks进行安全通信



Simple Use of Public-Key Encryption to Establish a Session Key

14. 消息认证 教材 264 页

1. 泄露(Disclosure)
2. 传输分析(Traffic analysis)

} 机密性

3. 伪装(Masquerade)
4. 内容篡改(Content modification)
5. 顺序修改(Sequence modification)
6. 计时修改(Timing modification)
7. 发送方否认(Source repudiation)

} 消息认证 数字签名

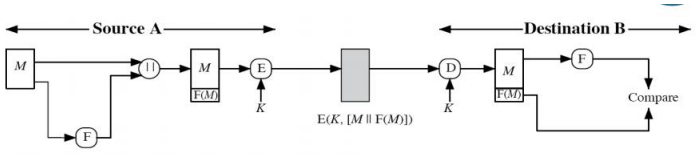
8. 接收方否认(Destination repudiation) 特定的数字签名机制

(1) 消息认证的概念，和数字签名的区别

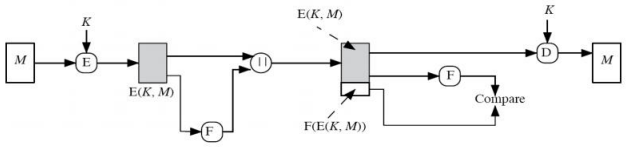
消息认证：数据完整性 ▪验证收到的消息确实来自声明的发送方且未被修改
▪消息认证也可以验证消息的顺序和时间

数字签名：不可否认性 ▪一种认证技术，包含了防止发送方否认的方法

(2) 利用校验和进行消息认证的方法：两种方式，一个安全一个不安全



(a) Internal error control

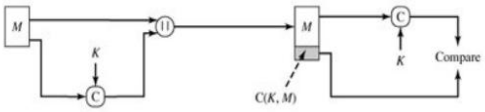


(b) External error control

(3) 消息认证码的定义

❖ Message Authentication Code (MAC)：利用共享密钥生成一固定长度的字段（记为MAC）

❖ MAC = C (K, M)
- M：输入消息
- C：MAC函数
- K：共享密钥
- MAC：消息认证码



- 可以确认：
  - 消息不被修改
  - 消息来源于宣称的发送方
  - 消息的发送顺序未被改变（要求消息中包含序列号）

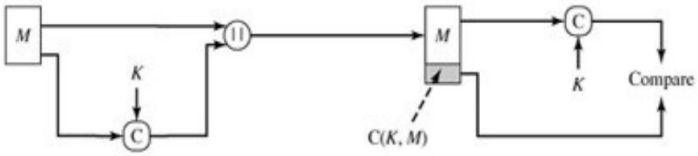
消息认证码生成函数与加密函数的区别、

- 与加密函数的区别：
  - MAC不需要解密，即MAC函数无需可逆性
  - MAC函数为多对一的映射关系

(4) 攻击者攻击的目标：不再是获得秘钥 K，而是寻找可生成相同认证码的消息。

(5) 如何利用消息认证码进行消息认证

- MAC = C (K, M)
  - M：输入消息
  - C：MAC函数
  - K：共享密钥
  - MAC：消息认证码



15. 散列函数

(1) 基本概念

① 单向散列函数（HASH 函数）：将一个长度可变的消息 M 转换为一个固定长度的输出，称之为散列码或摘要。

② 与 MAC 的区别：没有使用密钥，函数输入参数只有一个，可以检测出消息是否发生变化

(2) 利用散列函数构造 MAC 码的方法 **教材 272 页**

(3) 设计要求（弱碰撞性、强碰撞性）

1. H 可应用于任意大小的数据块
2. H 产生一固定长度的输出
3. 对于任意给定的x，H(x)的值都是容易计算的。
4. H是单向的，即给定h，找到任何一个满足h = H(x)的x在计算上不行
5. H有弱抗碰撞性：即给定x，找到任何一个满足H(x) = H(y)的 y，y ≠ x 在计算上是不可行的。
   - 满足性质4和5的函数称为弱单向函数
6. H有强抗碰撞性，找到任何两个满足H(x) = H(y)的x和y在计算上是不可行的。
   - 满足性质4、5和6的函数称为强单向函数

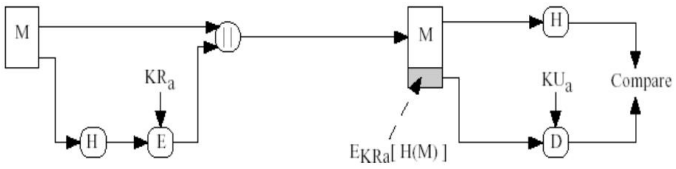
单向的特性是认证所必需的。 弱抗碰撞性对于防止伪造是必需的。强抗碰撞性对于抵抗生日攻击是非常重要的。

16. 数字签名

(1) 基本概念：只有信息的发送者才能产生的别人无法伪造的一段数字串，这段数字串同时也是对信息的发送者发送信息真实性的一个有效证明。

(2) 数字签名的常见方法

- 先对消息M作一个摘要H(M)
- 然后发送方用自己的私钥对H(M)进行加密，得到签名$E_{KRa}(H(M))$
- 连同消息M一起，发送出去
- B收到复合的消息之后，把签名提取出来
- B用A的公钥对签名解密得到H'
- B计算所收到消息的摘要H(M')
- 如果H'=H(M')，则消息确实是A产生的

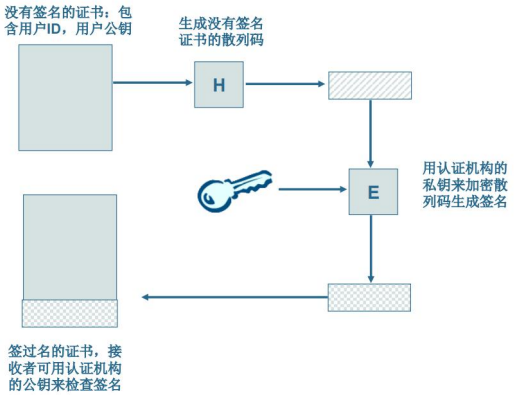


17. 公钥证书

(1) 基本概念：是一种数字签名的声明，它将公钥的值绑定到持有对应私钥的个人、设备或服务的身份。大多数普通用途的证书基于 X。509v3 证书标准。

(2) 公钥证书的产生过程及验证方法

① 产生



② 验证

- 验证证书的过程是迭代寻找证书链中下一个证书和它相应的上级CA证书。
- 在使用每个证书前，必须检查相应的CRL(对用户来说这种在线的检查是透明的)。
- 用户检查证书的路径是从最后一个证书(即用户已确认可以信任的CA证书)所签发的证书有效性开始，检验每一个证书，一旦验证后，就提取该证书中的公钥，用于检验下一个证书，直到验证完发送者的签名证书，并将该证书中包括的公钥用于验证签名。
  - 验证证书链中每一个CA证书
  - 上级CA签名的有效性
  - 证书有效期
  - 是否作废：CRL、OCSP

18. 身份认证 教材 330 页

(1) 认证方式：单向、双向

(2) 认证协议的安全目标

(3) 重发攻击的概念及如何抗重发攻击的常见方法

第三讲

1. 链路加密和端到端加密

(1) 在采用链路加密的网络中，每条通信链路上的加密是独立实现的。通常对每条链路使用不同的加密密钥。当某条链路受到破坏就不会导致其他链路上传送的信息被析

出。加密算法常采用序列密码。链路加密的最大缺点是在中间结点都暴露了信息的内容。在网络互连的情况下，仅采用链路加密是不能实现通信安全的。

(2) 端到端加密是在源结点和目的结点中对传送的 PDU 进行加密和解密，其报文的安全性不会因中间结点的不可靠而受到影响。端到端加密的层次选择有一定的灵活性。端到端加密更容易适合不同用户的要求。端到端加密不仅适用于互连网环境，而且同样也适用于广播网。

(3) 分层加密的概念和适用范围：加密的东西越多，自然是越安全，传输范围越小；加密的越少，安全性相对来说差一些，传输范围越广

2. EAP 协议基本概念：可扩展认证协议，看第七章！

3. 802.1X 认证协议：局域网接入控制协议

▪基于端口的访问控制协议 (Port Based Network Access Control Protocol)

▪目的：解决无线局域网用户的接入认证问题

IEEE 802.1x 协议的体系结构：

•客户端 Supplicant System

•认证系统 Authenticator System

•认证服务器 Authentication Server System

(1) 端口控制概念

① 端口概念：▪物理端口：网口

▪逻辑端口： MAC 地址，IP 地址，识别用户的标示

② 802.1X 中的端口是逻辑端口。

▪控制端口 (controlled port)：在认证通过的状态下才打开，用于传输网络服务数据。

▪非控制端口 (uncontrolled port)：始终处于连通状态，用于传输认证协议数据。

③ 端口控制状态：决定客户端能否接入网络

▪强开 (Force Authorized)：端口处于连接状态

▪强关 (Force Unauthorized)：端口处于关闭状态

▪自动 (Auto)：激活 802.1X ，初始设置端口为未授权状态，并通过端口认证来确定端口的闭合。

•用户尝试接入时处于非授权状态**(unauthorized)**。

•用户通过认证后端口切换到授权状态**(authorized)**

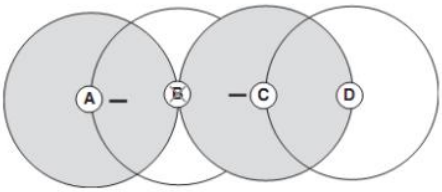
第四讲

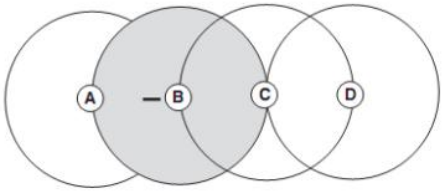
1. 隐藏终端和暴露终端

(1) "隐藏终端"（Hidden Stations）：在通信领域，基站 A 向基站 B 发送信息，基站 C 未侦测到 A 也向 B 发送，故 A 和 C 同时将信号发送至 B，引起信号冲突，最终导致发送至 B 的信号都丢失了。"隐藏终端"多发生在大型单元中（一般在室外环境），这将带来效率损失，并且需要错误恢复机制。当需要传送大容量文件时，尤其需要杜绝"隐藏终端"现象的发生。

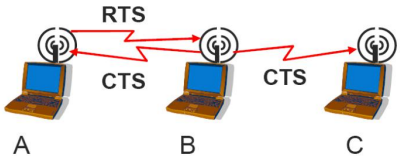
(2) 暴露终端是指在发送节点的覆盖范围内而在接收节点的覆盖范围外的节点，暴露终端因听到发送节点的发送而可能延迟发送。但是，它其实是在接收节点的通信范围

之外，它的发送不会造成冲突。这就引入了不必要的延时。



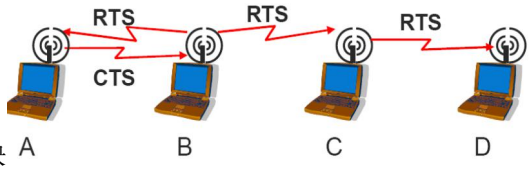


1. 节点A欲发送一数据包给节点B, 首先A发送一RTS给B;
2. B发送CTS;
3. A收到CTS后发送数据;
4. C监听到CTS，知道有节点在发送数据，A和B数据传输时间C不会发数据包。



隐藏终端问题解决

1、发送者发送 RTS。
2、接收者返回 CTS。
3、邻居节点：
如果收到 CTS则保持安静，不能传输数据。
如果只收到 RTS 而没收到 CTS,可以传输数据。



暴露终端问题解决

(3) 隐藏终端和暴露终端问题的解决方法：

解决隐藏终端问题的思路是使接收节点周围的邻居节点都能了解到它正在进行接收，目前实现的方法有两种：一种是接收节点在接收的同时发送忙音来通知邻居节点，即 BTMA 系列；另一种方法是发送节点在数据发送前与接收节点进行一次短控制消息握手交换，以短消息的方式通知邻居节点它即将进行接收，即 RTS/CTS 方式。这种方式是目前解决这个问题的主要趋势，如已经提出来的 CSMA/CA、MACA、MACAW 等。还有将两种方法结合起来使用的多址协议，如 DBTMA。

对于隐藏发送终端问题，可以使用控制分组进行握手的方法加以解决。一个终端发送数据之前，首先要发送请求发送分组，只有听到对应该请求分组的应答信号后才能发送数据，而是收到此应答信号的其他终端必须延迟发送。

在单信道条件下使用控制分组的方法只能解决隐发送终端，无法解决隐藏接收终端和暴露终端问题。为此，必须采用双信道的方法。即利用数据信道收发数据，利用控制信道收发控制信号

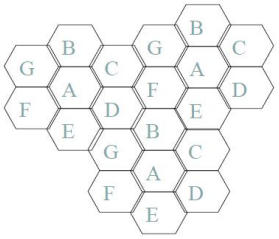
2. 频分和时分的概念

(1) 频分：将用于传输信道的总带宽划分成若干个子频带，每一个子信道传输 1 路信号。

(2) 时分：将提供给整个信道传输信息的时间划分成若干时间片(简称时隙)，并将这些时隙分配给每一个信号源使用，每一路信号在自己的时隙内独占信道进行数据传输。

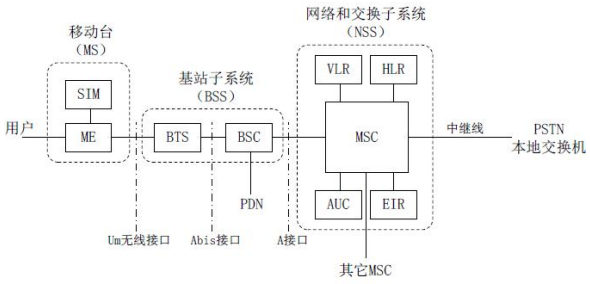
3. 蜂窝架构

❖蜂窝拓扑结构图

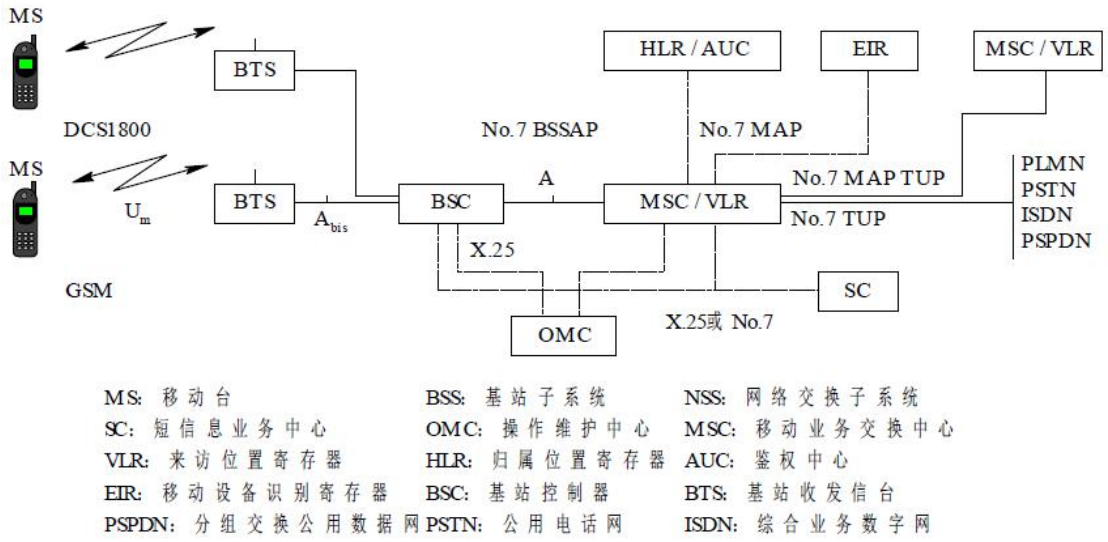


- 使用蜂窝拓扑可以有效实现频率复用。

❖典型蜂窝网络GSM的组成



4. GSM 系统架构



GSM系统整体结构框图

5. 越区切换（ handoff ）过程

当某移动终端离开一个小区时，就会询问所有邻近的基站收到该电话的信号的强弱。该基站随后将控制权转交给获得最强信号的小区。该电话随即被告之它有新的管理者，并且如果正在进行通话，它会被要求切换到新的信道。

6. GSM 系统的编号

(1) **MSISDN**：Mobile Subscriber Integrated Services Digital Network (**MSISDN**) number：移动用户的 MSISDN 号码相当于固定网的用户电话号码，是供用户拨打的公开号码。

(2) **IMSI**：International Mobile Subscriber Identity：国际移动用户识别。每个 GSM 移动用户都有一个 IMSI， 而且具有全球惟一性和永久不变性 更换身份证或丢失 SIM 卡的情况除外。IMSI 用于 GSM 通信网的所有信令中，在用户的 SIM 卡、 系统的 HLR 和 VLR 中都有存储。

(3) **TMSI**：Temporary Mobile Station Identity：为加强系统的保密性而在 VLR 内分配的临时用户识别号。它在某一 VLR 区域内与 IMSI 唯一对应。

分配原则：包含四个字节、不能全为 1，全为 1 表示无效 TMSI。

(4) **IMEI**：International Mobile Equipment Identity：国际移动台设备识别码。惟一地标识一个移动台设备的编码，IMEI 编码最多由 15 位十进制数字组成。

(5) **MSRN**：Mobile Station Roaming Number：移动台漫游号码是当移动台由所属的 MSC／VLR 业务区漫游至另一个 MSC／VLR 业务区中时， 为了将对它的呼叫顺利发送给它而由其所属 MSC／VLR 分配的一个临时号码。MSRN 与 MSISDN 结构相同。

(6) **LMSI**：本地移动用户识别码：为了加速 VLR 对用户数据的查询，还可使用辅助性的本地移动用户识别码 LMSI，它是在位置更新时，VLR 暂分配给来访用户的一个唯一识别码。LMSI 虽属可选，但如果在每次呼叫基础上分配移动用户漫游号 MSRN 时，则需使用 LMSI。

长度：4 个字节，没有具体定义。

(7) **LAI**：Location Area Identity：位置区识别

(8) **CI**：在 LAI 后加上 CI(Cell Identify，小区识别码）

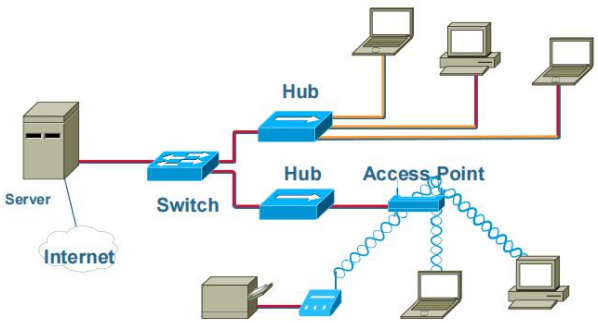
CI 长度：两字节

(9) **BSIC**：Base Station Identity Color：基站识别色。基站识别色码用于移动台识别使用相同载波的不同基站。

第五讲

1. **无线局域网的概念**

- **无线局域网是固定局域网的一种延伸。**
- **使用无线电波作为数据传送的媒介。传送距离一般为几十米。**
- **对用户来说是完全透明的，与有线局域网一样 。**



(1) **组成：IBSS、BSS、DS、ESS、STA（无线用户端）、AP（无线接入点）**

(2) **AD-HOC 模式和 Infrastructure 模式**

❖ **Ad-hoc Mode:**

- **一群使用无线网卡的Station，直接相互连接，资源共享，无需通过接入点（Access Point），该种模式通常无法连接Internet**

❖ **Infrastructure Mode**

- **所有Station通过接入点连接成网络实现资源共享**

(3) IBSS、BSS、DS、ESS 的概念

IBSS：独立基本服务集（适用于小型 WLAN 系统）

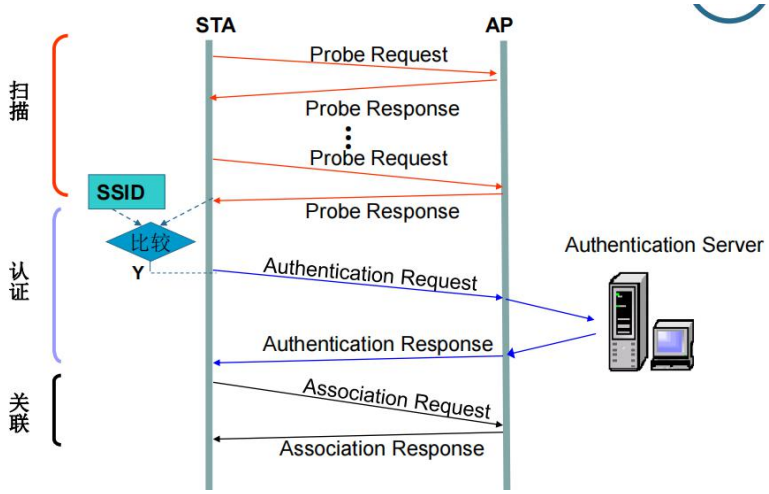
BSS：基本服务集（包括一组无线用户和一台连接到有线局域网的无线接入点）

DS：分配系统

ESS：扩展业务集（BSS+DS）

(4) 无线局域网的接入过程

STA (工作站）启动初始化、开始正式使用 AP 传送数据帧前，要经过三个阶段才能接入：1。 扫描(SCAN) 2。 认证(Authentication) 3。 关联(Association)



第一阶段 ： 扫描（ SCAN ） 阶段

❖ 若无线站点 STA 设成 Ad-hoc 模式：

STA先寻找是否已有 IBSS（与STA所属相同的SSID）存在，如有，则参加（join）；若无，则会自己创建一个IBSS，等其他站来 join。

❖ 若无线站点 STA 设成 Infrastructure 模式：

1、主动扫描方式（特点：能迅速找到）

STA 依次在11个信道发出 Probe Request 帧，寻找与STA所属有相同SSID的AP，若找不到有相同 SSID 的 AP，则一直扫描下去...

2、被动扫描方式（特点：找到时间较长，但STA节电）

STA被动等待AP 每隔一段时间定时送出的 Beacon 信标帧，该帧提供了AP及所在BSS相关信息： “我在这里”...

第二阶段 ： 认证（Authentication）阶段

当 STA 找到与其有相同 SSID 的 AP，在 SSID 匹配的 AP 中，根据收到的 AP 信号强度，选择一个信号最强的 AP，然后进入认证阶段。只有身份认证通过的站点才能进行无线接入访问。802.11提供几种认证方法，有简单有复杂，如采用802.1x/EAP认证方法时大致为：

1. STA向AP发送认证请求
2. AP向认证服务器发送请求信息要求验证STA的身份
3. 认证服务器认证完毕后向AP返回相应信息
4. 如果STA身份不符，AP向STA返回错误信息

如果STA身份相符，AP向STA返回认证响应信息

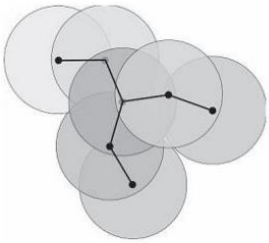
第三阶段 ： 关联（Association）阶段

当 AP 向 STA 返回认证响应信息、身份认证获得通过后， 进入关联阶段。

1. STA 向 AP 发送关联请求
2. AP 向 STA 返回关联响应

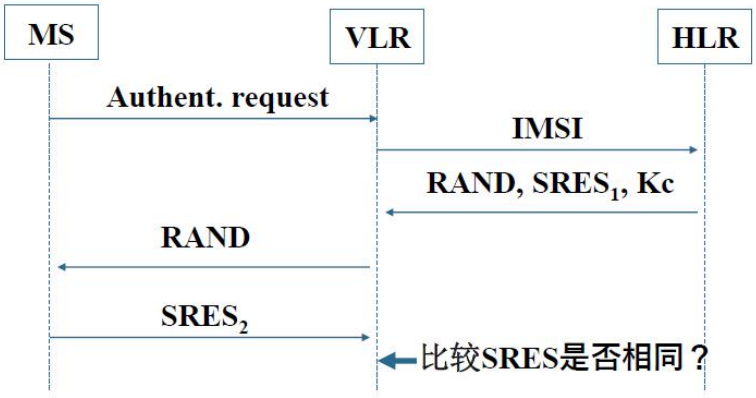
至此，接入过程才完成， STA 初始化完毕，可以开始向 AP 传送数据帧。

- **MANET 的基本概念**（移动自主网络）
  - 由一组带有无线收发装置的移动终端组成的一个多跳的临时性自治系统
    - 节点之间点对点通信
    - 节点是移动的，网络的拓扑结构不断变化
    - 节点负责转发通信，多跳路由

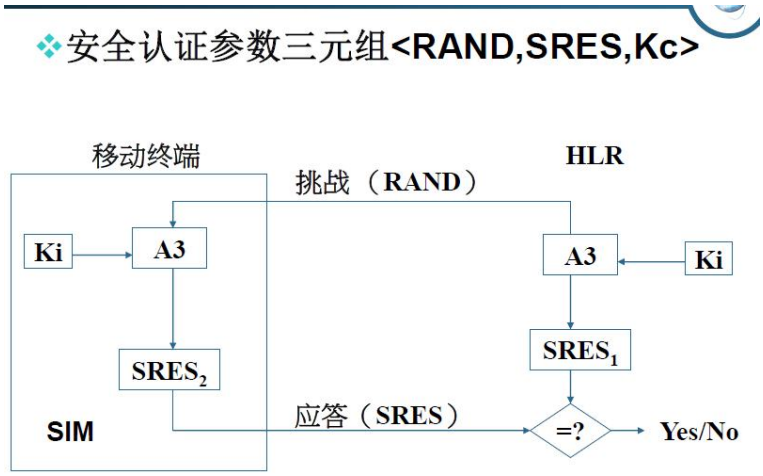


第六讲

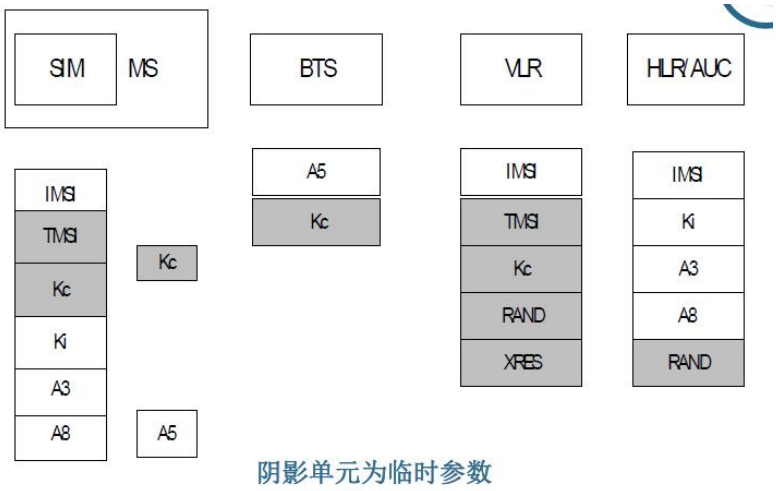
1. GSM 的身份认证流程



(1) 三元组概念



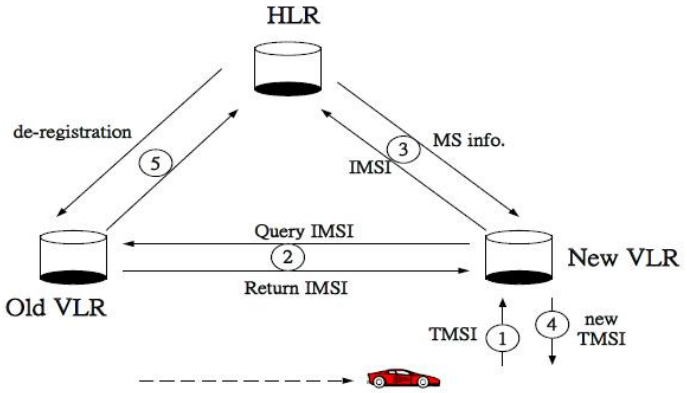
(2) 安全参数和算法分布



2. **GSM 的匿名保护**

- 使用 TMSI 替代用户 IMSI
  - 作为替代 IMSI 临时使用的用户号
  - 防止攻击者窃取用户识别号
- 在初始认证时使用 IMSI
- VLR 为每个用户生成一个 TMSI
  - VLR 执行 TMSI 的分配，管理，和更新工作

1. 首次通话交换时， IMSI发送给AC，分配得到一个TMSI。
2. 用户移动时，新的MSC会分配用户一个新的TMSI
3. TMSI在MS进行会话连接建立的时候。
4. 网络通过TMSI和MS进行通信
5. 在MS端，TMSI存放在SIM卡中用于下次使用。



3. GSM 安全机制存在的问题

(1) 只提供单向认证，难以防止中间人攻击和伪基站攻击；
(2) 加密只在空中接口部分进行，固网中不提供端到端的加密；
(3) 加密功能没有延伸到核心网络，基站之间的传输链路中用户信息和信令数据都以明文传输；
(4) 用户身份认证密钥不可变更，无法抗重放保护；
(5) 用户数据和信令数据缺乏完整性保护机制；
(6) 算法设计过程不公开；
(7) 用户出于漫游状态时，服务网络采用的认证参数与归属网络之间没有有效的联系；
(8) 无第三方仲裁功能，当网络实体间出现费用纠纷时，无法递交给第三方进行仲裁；
(9) 用户认证过程中 IMSI 可能以明文方式在无线信道上传输；
(10) 无法对系统的安全升级及安全功能的更新；
(11) 安全算法存在漏洞，可被破解；

4. 3GPP 的身份认证

(1) 身份认证和密钥分配（AKA 协议）

(2) 五元组概念

相互认证 (Mutual Authentication）

五元组认证向量：RAND ： 128 位随机数

XRES RAND ： 对应的应答， 32 位。

CK ： 加密密钥 128 位。

IK ： 完整性校验密钥 128 位。

AUTN ： 网络认证令牌 128 位。

第七讲

WEP 加密是共享密钥认证，而 TKIP、CCMP 和 802.1x 则是开放系统认证。

WEP(Wired Equivalent Privacy)叫做有线等效加密，是一种可选的链路层安全机制，用来提供访问控制、数据加密和安全性检验等功能，是无线领域第一个安全协议。 WEP 的实现在 802.11 中是可选项。

WEP 的密钥在 802.11（1999）以前的版本中规定为 64bits（40bits 静态 Key +24bits IV 初始向量），后来有些厂家将静态共享 Key 拓展到 104bits 再加上 24bits 初始化向量便构成 128bits 的 WEP 密钥。

1. WEP 的认证流程及安全问题

（1）**2 类认证：**

① 开放系统：没有认证，无任何安全性可言，任意 STA 都可以接入网络。

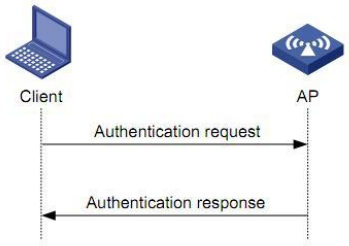
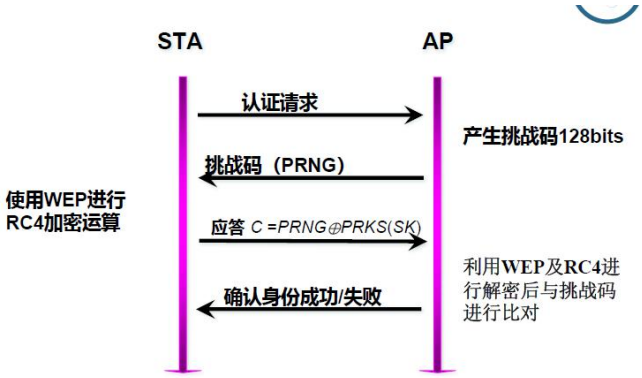


图1 开放系统认证过程

Note:

无论密码是否正确，AP 都会进行认证而且认证会通过，之后再进行关联，关联会通过。只是，如果密码不正确，将不能分配到 IP 地址。

② 共享密钥认证：通过共享 40bits 或 104bits 静态密钥来实现认证要求 4 个步骤：



1) 初始站点 STA 发送一个认证请求到接收端（通常是一个 AP）。
2) AP 送回一个明文文本检验消息--挑战码 PRNG128bits。
3) 该站点 STA 使用 RC4 加密消息并送回到 AP 再次向 AP 发出认证请求。
4) AP 进行 WEP 解密解密消息。如果与所发送的消息匹配，请求的站点就配置了正确的密钥，从而证明它被授权使用该网络。
5) 然后，这两个站点都可以自由地交换消息，每一次加密和解密都使用 RC4 方法，并且认证过程中都使用相同的密钥。

共享密钥认证需要客户端和设备端配置相同的共享密钥。共享密钥认证的安全性高于开放式系统认证，但是就技术而言，完全可以无视这种认证。

Note:

如果认证成功，则随即进行关联，关联通过后即可分配到 IP 地址。

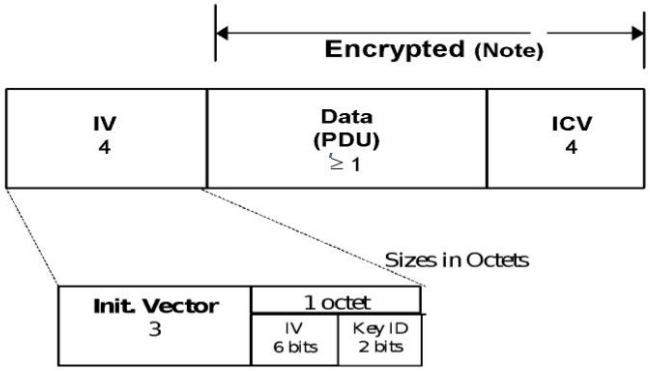
如果认证失败，客户端会尝试几次认证，如果最后仍然失败，而不会进行关联。

③ 共享密钥认证漏洞：

对于共享秘钥认证，攻击者可以捕获挑战码（PRNG）和 C，通过 PRNG⊕C 得到 PRKS（SK），攻击者就可应答成功挑战码，取得身份认证，伪装成合法用户。

2. WEP 加密机制流程

WEP 加密采用 RC4 流加密算法。RC4 是一种流加密算法，密钥长度可变。它加解密使用相同的密钥。



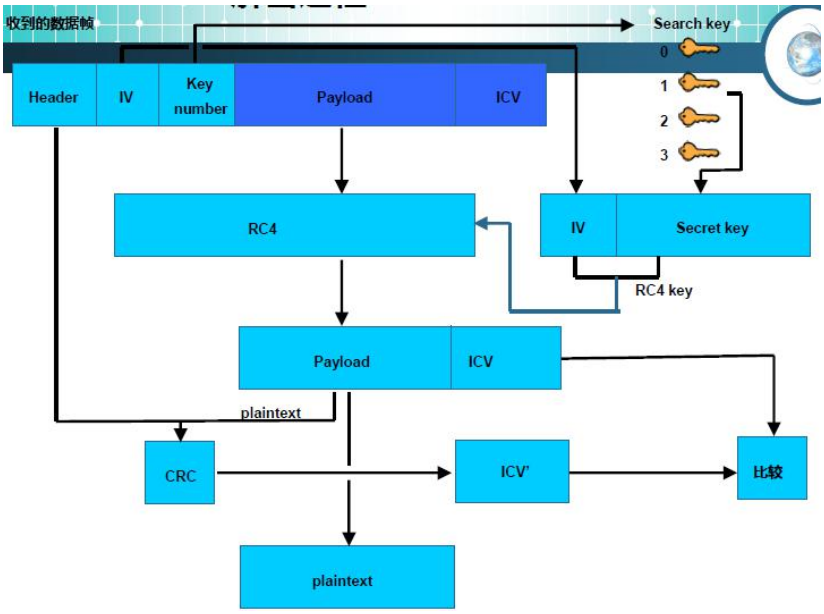
(1) WEP 加密过程：

① IV 是动态生成的 24bit 随机数，在数据帧中以明文的方式进行发送，它和 key 结合生成随机种子（seed），然后运用 CR4 算法生成秘钥流（keystream）。

② 对需要加密的明文进行 CRC-32 运算，生成 ICV（32 位），然后将这个 ICV 追加到 plaintext 的后面。

③ 将尾部有 ICV 的 plaintext 与密码流进行异或运算，得到加密数据。

④ 将 IV 添加到加密数据的前面，进行传送。

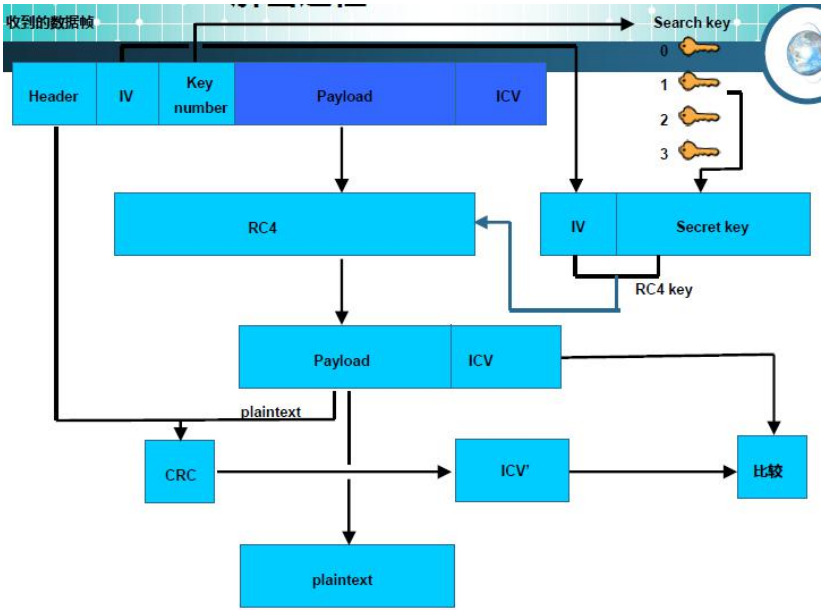


(2) WEP 解密过程：

① IV 和 key 结合生成随机种子（seed），然后运用 CR4 算法生成秘钥流（keystream）

② 将 keystream 和加密数据进行异或，得到 plaintext 和 ICV

③ 根据解密后得到的 plaintext 再计算一个 ICV 和包中的 ICV 进行比较，判断是否相等，这也算是一个可靠性的保证。-----数据帧的完整性校验（采用 CRC 校验防篡改）



3. WEP 加密机制安全问题

(1) WEP 加密是可选功能，在大多数的实际产品中默认为关闭，因此将用户数据完全暴露于攻击者面前。

(2) 密钥产生问题：

① 直接由用户写入 40 或 108 比特的密钥；

② 由用户输入一个口令，根据该口令通过某个密钥生成函数产生密钥。

③ 密钥分发问题：密钥为无线局域网所有用户共享，且很少变动，因而容易泄漏。

(3) 数据篡改：14-15 年试卷最后一题

- **RC4,CRC32算法:线性校验算法**
  - **线性算法特征：** $c(x \oplus y) = c(x) \oplus c(y)$
- **攻击方法**
  - **已知：初始向量iv,密文C。**
  - **未知：明文M，密钥K**
  - **C=RC4(iv,K)⊕{M,crc32(M)}**
  - **随意伪造新明文M'，令M'=M+Δ**
  - **C'= C⊕<Δ,crc32(Δ)>**

(4) 初始向量空间太小问题：容易造成重复使用。

WEP 协议使用了每个分组采用不同的初始向量以避免了密钥序列的重复。然而无论是 40bits 或 104 bits 长的密钥，其 IV 均为 24 bis，也就是说其密钥空间只有 2^{34} 大小，对于采用 CCK 调制速率高达 11 Mbps 的情形，可能在 1 小时以后就出现重复 IV。只要 IV 相同，与明文相异或的密钥序列必然相同。这样密钥便出现了两次，且该情况会频繁出现。更严重的是由于 WEP 在基本服务集(Basic Service Set，BSS)所有成员中共享基本密钥(Basie Key)，为避免密钥序列重复使用，WEP 需要随机选择初始向量 IV，这样便导致生日悖论。

由此可见，流加密算法本身的弱点及 802.11 标准中初始向量空间太小使密钥序列重复使用的机会大大增加，对于 WLAN 的安全是灾难性的结果。

$$C2 \oplus C1 = \{P1 \oplus RC4(iv \,||\, SK)\} \oplus \{P2 \oplus RC4(iv \,||\, SK)\} = P1 \oplus P2$$

iv空间: 24bits，
IV的生成方法：用计数器递增实现

(5) FMS 攻击：弱 IV 问题，通过收集特定 IV 格式 (弱的数据包来反向推导密钥）

▪Weak IV

•(B+3，N 1，X) 形式的 IV ，称 Weak IV

–B：欲破解的 secret key byte

–N：256

–X：为任意值

4. TKIP 协议

加密算法的改进	TKIP 加密机制	在现有的 WEP 基础上进行修改
	CCMP 加密机制	重新设计新的安全机制
认证机制的改进	WPA PSK 认证	
	802.1X 认证	

(1) 针对的 WEP 安全问题及相应的改进对策

① 问题：

（1）	无法检测消息是否被篡改
（2）	没有提供重放攻击保护
（3）	IV 长度太短，容易造成重复使用
（4）	存在 Weak IV，容易遭受 FMS 攻击
（5）	直接使用主密钥，没有提供密钥更新机制

② 对策：

目的	改进	针对的安全问题
数据完整性保护	添加基于密码学的消息完整性校验码 (MIC)，Michael 函数	(1)
IV 选择和使用	添加 IV 序列计号(24 变 48 位)，TSC 计数器，改变 IV 生成方式和功能；避免出现 Weak IV	(2)，(3)
密钥混合	添加分组密钥混合函数，使得每次加密使用的密钥都不同，临时密钥替代原有的 WEP 密钥和 IV	(4)
密钥管理	添加 Re-keying 机制，进行密钥分发、更新和生成临时密钥	(5)

5. CCMP 加密机制

(1) 设计要求：

① 被正确加密：密钥不能重复使用；Nonce 和 IV 不能重复使用

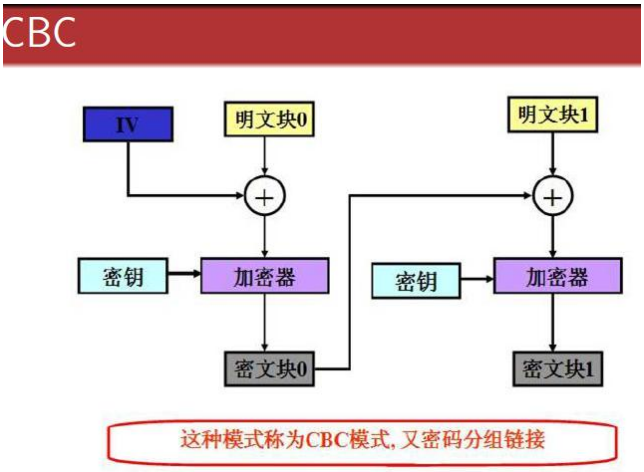
② 防止数据被篡改：防止发送地址和接收地址被篡改

③ 抗重发攻击

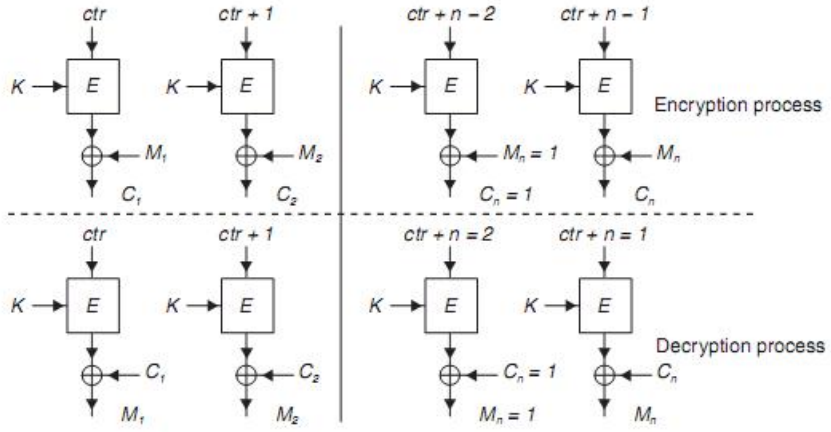
④ 降低成本：尽可能减少加密函数使用数量；尽可能减少软件开销；尽量借鉴已有的安全机制

(2) 设计细节：

① CBC-MAC 模式用于计算 MIC 码：这种模式是先将明文切分成若干小段，然后每一小段与初始块或者上一段的密文段进行异或运算后，再与密钥进行加密。



② CTR 模式用于进行加密：CTR 模式不常见，在 CTR 模式中， 有一个自增的算子，这个算子用密钥加密之后的输出和明文异或的结果得到密文，相当于一次一密。这种加密方式简单快速，安全可靠，而且可以并行加密，但是在计算器不能维持很长的情况下，密钥只能使用一次。



6. **WPA-PSK 基本概念**

(1) 存在的攻击方式：字典攻击

① 字典攻击：就是使用常见的单词、词组、数字、人名和相关的变形。由于用户在设置密码时为了方便记忆，会选择短的、有意义的英文字和数字作为密码。因此攻击者可以快速的进行反复猜测与比对，从而在短时间内获得密码。

② 特征：通过截获 4 步握手的数据包进行字典攻击；成功与否与所使用的字典有关；花费的时间与密码在字典中的位置有关。

(2) 实施一次字典攻击需要具备两个要素：

① 黑客了解认证方式（包括认证协议以及地址、端口等信息），如同小偷需要知

道库房在哪儿，房门挂着的是大铜锁还是密码锁，甚至虹膜、指纹识别，拿着一串金属钥匙想打开生指纹识别锁显然不现实。

② 黑客拥有比较全面的口令集，包含着各类常见的弱口令，或目标系统经常出现的组合口令，或目标系统曾经泄露的口令集，这样才有更多的尝试机会。通常一次字典攻击的实施还是很耗费时间的，特别是目标系统的口令不那么常见。

(3) 字典攻击预防：

① 口令的设置更加强壮（具有足够长度，含有字母、数字、符号等各种类型），更新更加频繁。这样可以减少被字典攻击猜测成功的几率。

② 采取针对字典攻击更为有效的入侵检测的机制，如某个客户端向系统频繁发起认证请求并失败时，系统应及时向管理员发出告警，发起分析和调查并在必要时更换新口令。

③ 采用更加健壮的加密算法和策略，使得常规的字典攻击难以生效

7. 802.1X 认证方式：

▪有线网络：物理位置固定，空间封闭。可以实现基于网络设备端口的控制管理。

▪无线网络：空间开放，终端可移动。

802.1X 认证：局域网接入控制协议，基于端口的访问控制协议，目的是解决无线局域网用户的接入认证问题。

(1) 基于端口控制：**看第三章**

(2) 采用 EAP 认证机制，可扩展。

802.1x 认证系统使用 EAP 协议来实现客户端、设备端和认证服务器之间的认证信息交换。

① **EAP 特点：**

▪协议封装简单，操作简单；

▪可以运行在任何链路层之上（ PPP 、 802.3 、 805.9 、802.11 等），具有良好的适用性；

▪EAP 采用高层认证技术，并且支持多种 IETF 安全协议标准（ TLS 、 IKE 等），从而降低了链路层运算资源在安全上的开销；

▪可方便的扩展支持未来的认证协议，具有良好的可扩展性；

▪可以运行于有损或无损媒体之上，包括无线媒体。

② **EAP 认证过程：**

1) 当用户有上网需求时打开 802。1X 客户端程序，输入用户名和口令，发起连接请求。此时客户端程序将发出请求认证的报文给交换机，启动一次认证过程。

2) 交换机在收到请求认证的数据帧后，将发出一个 EAP-Request/Identity 请求帧要求客户端程序发送用户输入的用户名。

3) 客户端程序响应交换机的请求，将包含用户名信息的一个 EAP-Response/Identity 送给交换机，交换机将客户端送来的数据帧经过封包处理后生成 RADIUS Access-Request 报文送给认证服务器进行处理。

4) 认证服务器收到交换机转发上来的用户名信息后，将该信息与数据库中的用户名表相比对，找到该用户名对应的口令信息，用随机生成的一个加密字 Challenge 对它进行加密处理（MD5），通过接入设备将 RADIUS Access-Challenge 报文发送给客户端，其中包含有

EAP-Request/MD5-Challenge。

5) 客户端收到 EAP-Request/MD5-Challenge 报文后，用该加密字对口令部分进行加密处理（MD5）给交换机发送在 EAP-Response/MD5-Challenge 回应，交换机将 Challenge，Challenged Password 和用户名一起送到 RADIUS 服务器进行认证。

6) 认证服务器将送上来的加密后的口令信息和其自己经过加密运算后的口令信息进行对比，判断用户是否合法，然后回应认证成功/失败报文到接入设备。如果认证成功，则向交换机发出打开端口的指令，允许用户的业务流通过端口访问网络。否则，保持交换机端口的关闭状态，只允许认证信息数据通过。

(3) 802.1X 三个实体

- 申请者：用户终端，发起 802.1X 认证过程。
- 认证者：接入点，透传认证数据。
- 认证服务器：实现用户认证