通 信 安 全

L10—通信网安全通信协议

- 教师：崔爱娇

- 编号：ELEC3019
- 学时：32学时

概 要

通信网安全通信协议

- 安全通信协议概述
- 安全协议的概念与分类
- 安全协议的性质与设计
- 通信系统安全技术

概 要

通信网安全通信协议

- 安全通信协议概述
- 安全协议的概念与分类
- 安全协议的性质与设计
- 通信系统安全技术

通信网安全通信协议概述

安全通信协议：为实现安全通信目的而设计通信协议。

实质：通过信息的安全交换来实现某种安全目的。

网络安全通信协议：使用数据加密技术和访问控制技术解决网络安全中的信息交换问题。

基本要素包括：

- 保证信息交换的安全；
- 使用密码技术。核心技术；
- 严密的共同约定的逻辑交换规则。不严密，则易被攻击
- 使用访问控制等安全机制，也就是除了技术支持外，

还需要访问、操作、法规等诸多方面的安全机制来进一步保障安全性能目标的实现。解密失败、完整性检验无法通过就丢弃报文。

网络安全内涵

内涵发展：数据安全、用户安全、系统安全、人网安全

- 数据安全：机密性、完整性、可用性、有效性、可控性
- 用户安全：认证、授权、访问控制、防否认、可服务、私密、产权
- 数据安全+用户安全：安全策略、安全机制、安全服务
- 系统安全：可用、高效、高可靠、高生存（恢复、再生）
- 人网安全：环境安全、辅设安全、物理安全、网络安全、系统安全、数据安全、信息安全、公共与国家信息安全。

安全协议地位

◆地位：密码技术、安全协议、网络安全

◆密码技术：数学基础、密码体制、密码算法、密码分析

◆安全协议：安全协议设计+安全协议实现+协议漏洞分析

- 安全协议设计：安全目标+约束条件+选择密码体制；
- 安全协议实现：算法选择+算法语言+算法编程+系统融合
- 协议漏洞分析：安全分析+漏洞发现+漏洞补丁+安全审计

◆也叫密码协议，是通过保障信息安全交换以实现某种安全目的（网络）协议。

概 要

通信网安全通信协议

- 安全通信协议概述
- 安全协议的概念与分类
- 安全协议的性质与设计
- 通信系统安全技术

安全协议的概念与分类

- ◆ 协议：参与者为完成任务商定的规则集合。
- ◆ 协议任务：两个以上的参与者+任务目标+任务执行。
- ◆ 协议三要素：语法+语义+时序
- ◘ 通信协议：通信各方为信息通信商定的规则集合
- ◘ 通信协议语法：各方认可的通信信息和通信原语描述格式
- ◘ 通信协议语义：通信信息和通信原语中各项的具体含义。
- ◘ 通信协议时序：通信信息发送和通信原语执行的先后顺序。

安全协议的概念

- 安全协议：通信各方为保证信息交换安全协商的规则集合。
- 安全协议目标：信息交换安全=站点之间+站点内部
- 安全协议语法：安全交换数据格式+安全交换操作格式
- 安全协议语义：数据项和数据操作的具体含义
- 安全协议时序：数据交换和数据操作先后次序
- 安全协议主要技术：密码技术
- 安全协议同义语：密码协议或通信安全协议

安全协议分类

◆ 按功能分类：认证协议+密钥管理协议+防否认协议+信息安全交换协议。

- 认证协议：消息认证+源认证+身份认证
- 密钥管理协议：密钥分配+密钥交换+密钥保存+密钥更新+密钥共享
- 防否认协议：数字签名+数字证书+数字指纹
- 信息安全交换协议：如IPsec、S-MIME、sHTTP

安全协议分类

◆ 按层次分类：链路层安全协议+网络层安全协议+传输层安全协议+应用层安全协议。

- 链路层安全协议：如PPTP、L2TP、DiffServ等
- 网络层安全协议：如IPsec、IKE等
- 传输层安全协议：如SSL、TLS等
- 应用层安全协议：如S-MIME、sHTTP、PGP、SET等

概 要

通信网安全通信协议

- 安全通信协议概述
- 安全协议的概念与分类
- 安全协议的性质与设计
- 通信系统安全技术

安全协议的安全性质

- 安全协议的主要目的是保证通信中数据的机密性完整性，还要保证通信主体身份的识别与认证，以及不可否任性等安全性质。

- 通过协议消息的传递来达成通信主体身份的识别与认证，在此基础上为下一步的秘密通信分配会话密钥。因此，通信主体双方的身份认证是基础，是前提，认证过程中对关键信息的秘密性和完整性有要求。

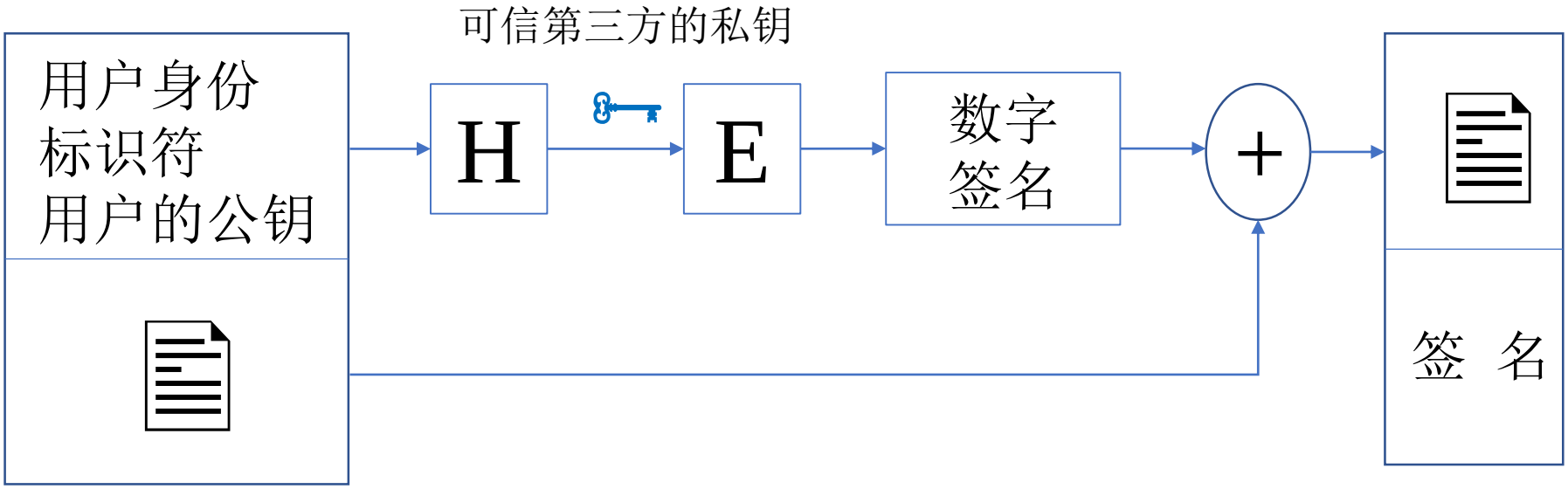
安全协议性质（1）—认证性

- 认证：对分布式系统中主体进行身份识别的过程。是其他安全性质的基础。
- 认证的作用：确保身份，获得对人或物的信任。抗假冒攻击的危险。证据证明其身份。
- 认证性：安全性的基础和前提，其他安全性依赖于此。
- 认证过程：协议中对身份或消息的识别与证实过程。
- 认证分类：身份认证（身份鉴别）+消息认证。

安全协议性质（1）—认证性

◆ 认证方法：

- 声称者使用仅为声称者和验证者知道的密钥封装的一个消息，如果验证者能够成功的解密消息或验证消息是正确的，则声称者的身份得到证明。
- 声称者使用其私钥对消息签名，验证者使用声称者的公钥验证签名，如果正确，则生成者的身份得到证明
- 声称者通过可信第三方来证明自己。



安全协议性质（2）—机密性

◆ 机密性：只有被授权的人才能查看信息。即时攻击者得到消息，无法查看消息的内容和有用的信息。

◆ 机密方法：加密+隧道+地址限定+目的端认证+密钥管理。

● 加密：密码体制+加密算法+密钥交换+前端加密机。

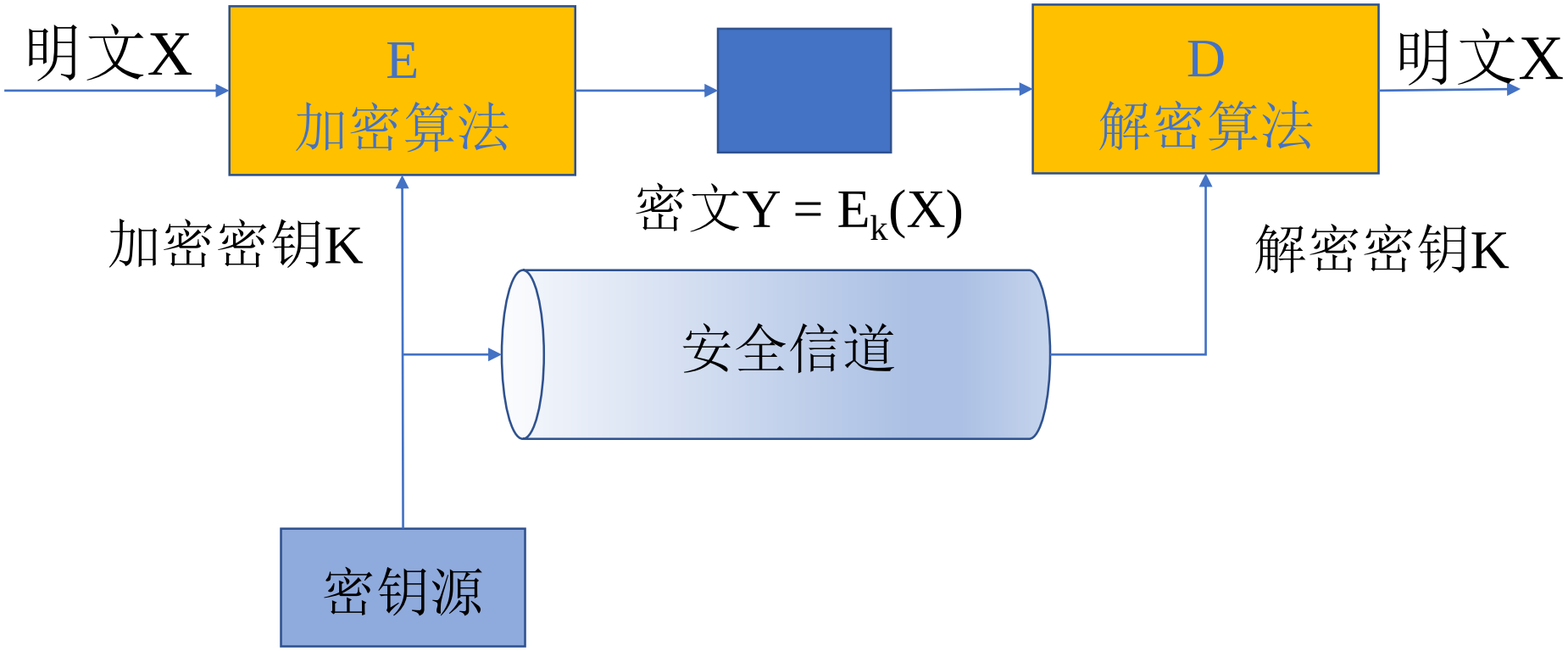
● 隧道：数据报加密 →进入隧道→退出隧道→报文解密。

● 地址限定：源地址认证+目的地址限定，例：限制下载地址

◆ 目的端认证：空包认证→有效报文连续认证

◆ 密钥管理 ： PKI等

安全协议性质（2）—机密性



一般的加密模型

安全协议性质（3）—完整性

◆ 完整性：协议消息不被添加、删除与篡改

◆ 完整方法：消息摘要+消息加密+消息签名+冗余封装

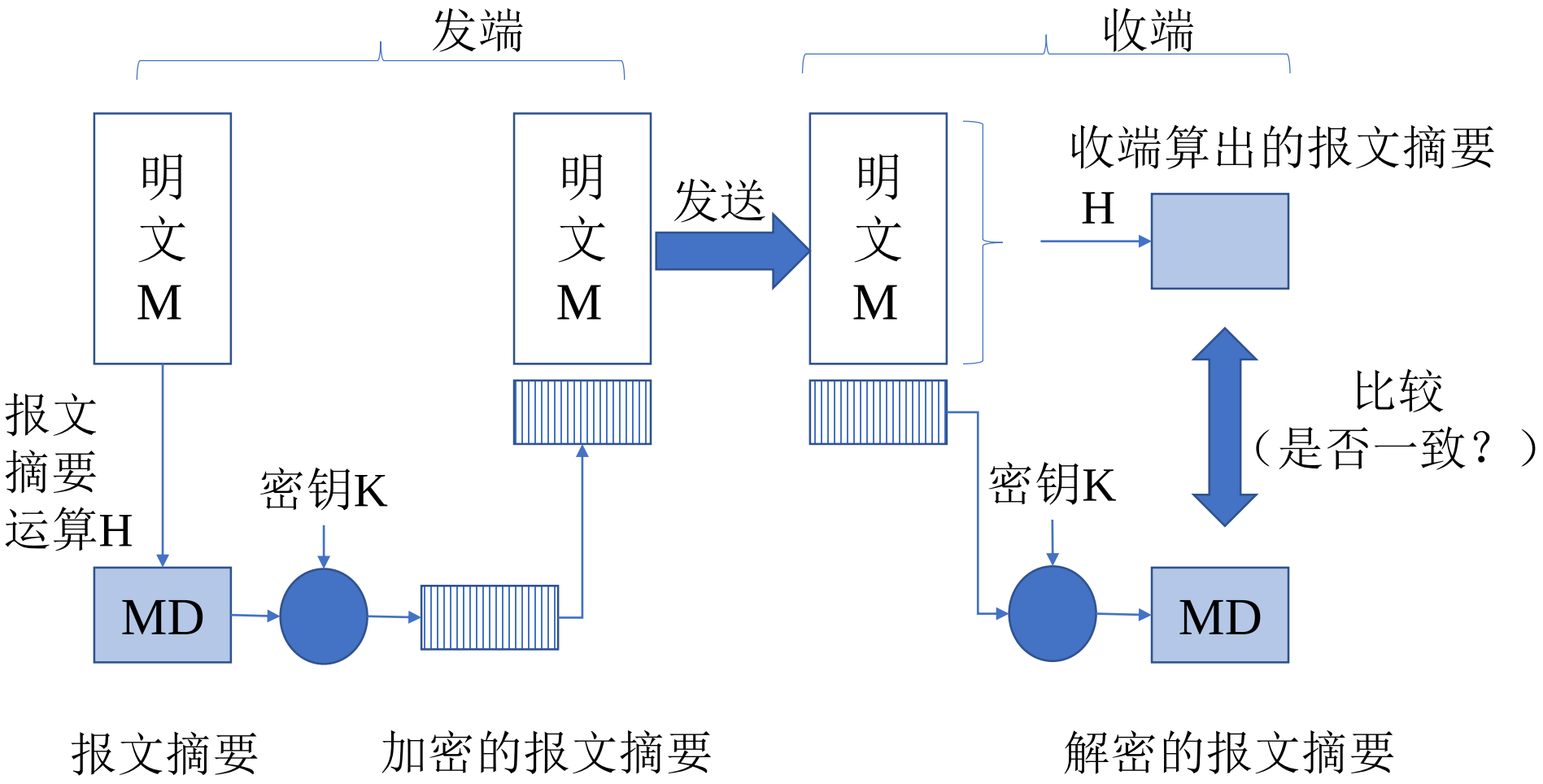
● 消息摘要：摘要算法协商：MD5+SHA-1，附加发送。

● 消息加密：数据报加密，消息摘要，摘要校验，报文解密。

● 消息签名：摘要与原文私钥加密+公钥解密，摘要校验。

● 封装和签名：用加密的方法或者hash函数产生一个明文的报文摘要附在传送的消息上，作为验证消息完整性的依据，称为完整性校验。

安全协议性质（3）—完整性



报文摘要的实现

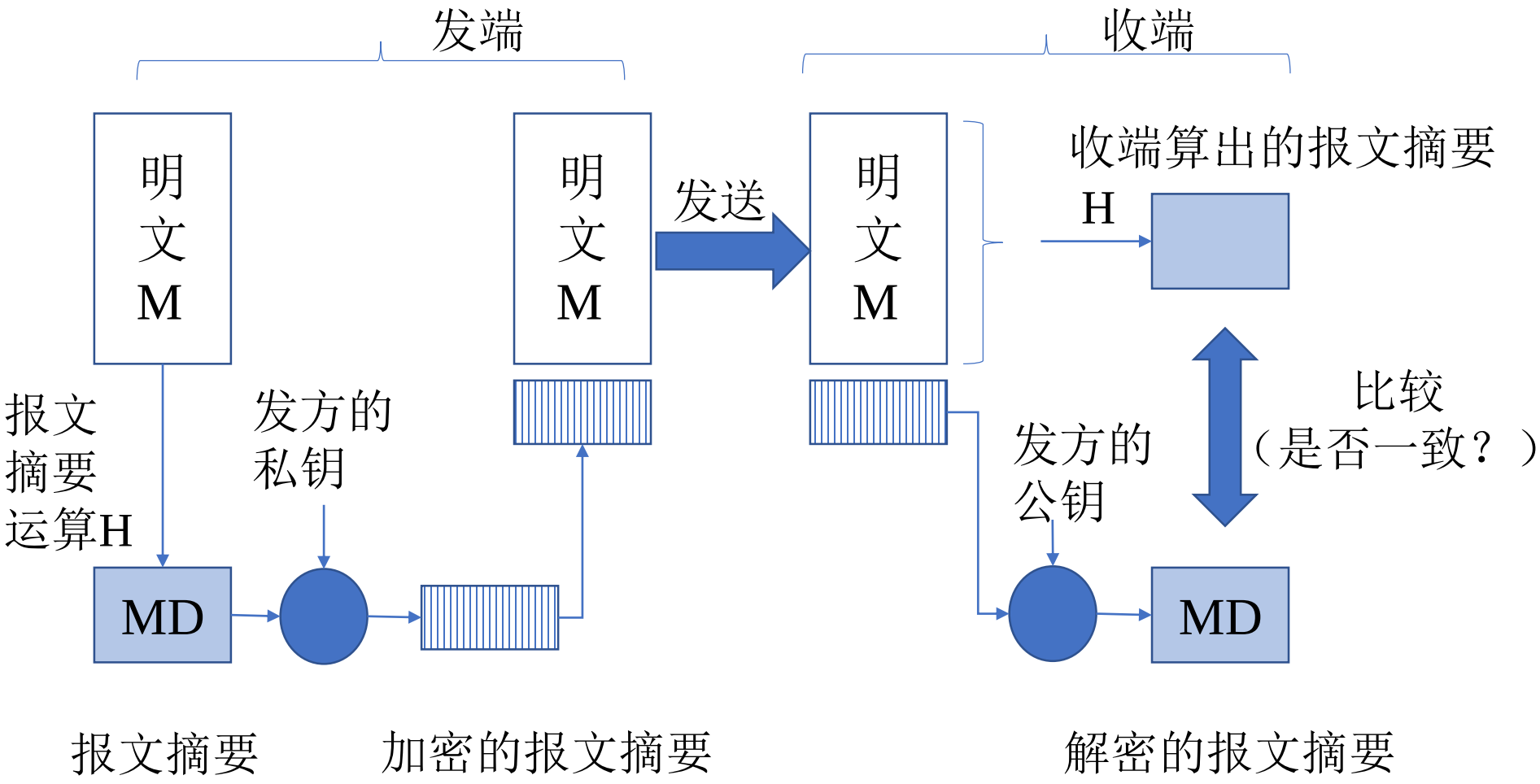
安全协议性质（4）—不可否认性

- ◆ 不可否认性：协议主体不能事后否认自己的行为。负责任，讲诚信。
- ◆ 不可否任性主体的目的：收集证据，事后向仲裁方呈现。
- ◆ 完整方法：消息签名+可信第三方TTP（Trusted Third Parties）

- ● 消息签名：A私钥签名→ B公钥加密正文与签名→ 消息发送→ 私钥解密正文与签名→ A公钥解密。

- ● 可信第三方： A发请求给TTP → TTP向A发送密钥→ A向B发送A证据E00与加密消息→ 若B同意，转发E00与B证据E0R给TTP → TTP验证后向B发送密钥→ TTP向A证实B接收。

安全协议性质（4）—不可否认性



数字签名的实现

安全协议的设计

- 缺陷分类
- 对安全协议的攻击
- 设计原则

安全协议缺陷（1）

- ◆ 分类：缺陷来源分类+根据缺陷攻击的分类

- □ 根据缺陷来源分类：设计缺陷+实现缺陷+执行缺陷

  - ➢ 设计缺陷：由于协议设计思想、设计策略、设计方法、安全目标疏漏造成的协议缺陷。

  - ➢ 实现缺陷：由于协议实现策略、算法选择、语言平台、实现流程、模块整合、实现完整性等不完善造成的协议缺陷。

  - ➢ 执行缺陷：策略缺陷+组织缺陷+制度缺陷+流程缺陷

安全协议缺陷（2）

- 根据缺陷攻击的分类：基本协议缺陷+并行会话缺陷+密钥/口令破解缺陷+旧消息缺陷+内部协议缺陷+密码体制缺陷

  - 基本协议缺陷：主要是设计原因造成的缺陷，没有防范攻击者。
  - 并行会话缺陷：主要是协议对并行会话协议缺乏防范。获得协议消息攻击。
  - 密钥/口令破解缺陷：主要是常用词口令，可猜测。暴力破解。
  - 旧消息缺陷：对消息的新鲜性没有考虑，攻击者消息重放。
  - 内部协议缺陷：协议的可达性存在问题，有一方不能完成动作导致的缺陷。
  - 密码体制缺陷：设计者不能满足机密性的要求。如位数32。

对协议安全的攻击（1）

- 攻击分类：按形式分类+按目标分类+按过程分类+按术语分类+按效果分类+按存储数据分类+每个CERT分类
  - 按形式分类：主动攻击+被动窃听
  - 按目标分类：机密性攻击+完整性攻击+可用性攻击+可控性攻击
    - 机密性攻击：拦截+Tempest+社交+重定向+推理+监听+病毒
    - 完整性攻击：认证攻击+会话劫持+异常输入（主要：溢出）
    - 可用性攻击：DoS+DDoS+前端攻击）
    - 可控性攻击：网络蠕虫+垃圾邮件+逻辑炸弹+DNS攻击。

对协议安全的攻击（2）

- 按过程分类：中断+拦截+篡改+伪造
- 按术语分类：窃听+陷门+蠕虫+病毒+DoS+IP欺骗+隐蔽信道+流量分析
- 按效果分类：泄露+DoS+系统崩溃+硬件损毁
- 按存储数据分类：浏览+泄漏+推理
- 美国CERT分类：溢出+非安全处理+参数检查不完整+非安全程序特征+木马+弱认证/加密+配置缺陷+程序实现缺陷

安全协议设计原则

- 基于缺陷：六类10条
  - A避免基本缺陷原则：消息清晰性+环境清晰性
    - 消息清晰性原则：1.消息独立完整+2.密文不依赖上下文+3.安全价值大于通信成本+4.先签名后加密
    - 环境清晰性原则：5.前提明确可验证，环境边界明确
  - B避免并行会话缺陷原则：“提问”方向明确可区分
  - C避免口令/密钥缺陷原则：响应鲜牛奶原则，只响应新鲜的请求
  - D避免旧消息缺陷原则：异步保险原则，尽量采用异步认证，避免同步
  - E避免内部缺陷原则：形式化验证所有状态，无死锁循环
  - F避免系统缺陷原则：使用好的秘密体制，按价值防护

概 要

通信网安全通信协议

- 安全通信协议概述
- 安全协议的概念与分类
- 安全协议的性质与设计
- 通信系统安全技术

第二代移动通信系统安全技术

◆ GSM的安全体系

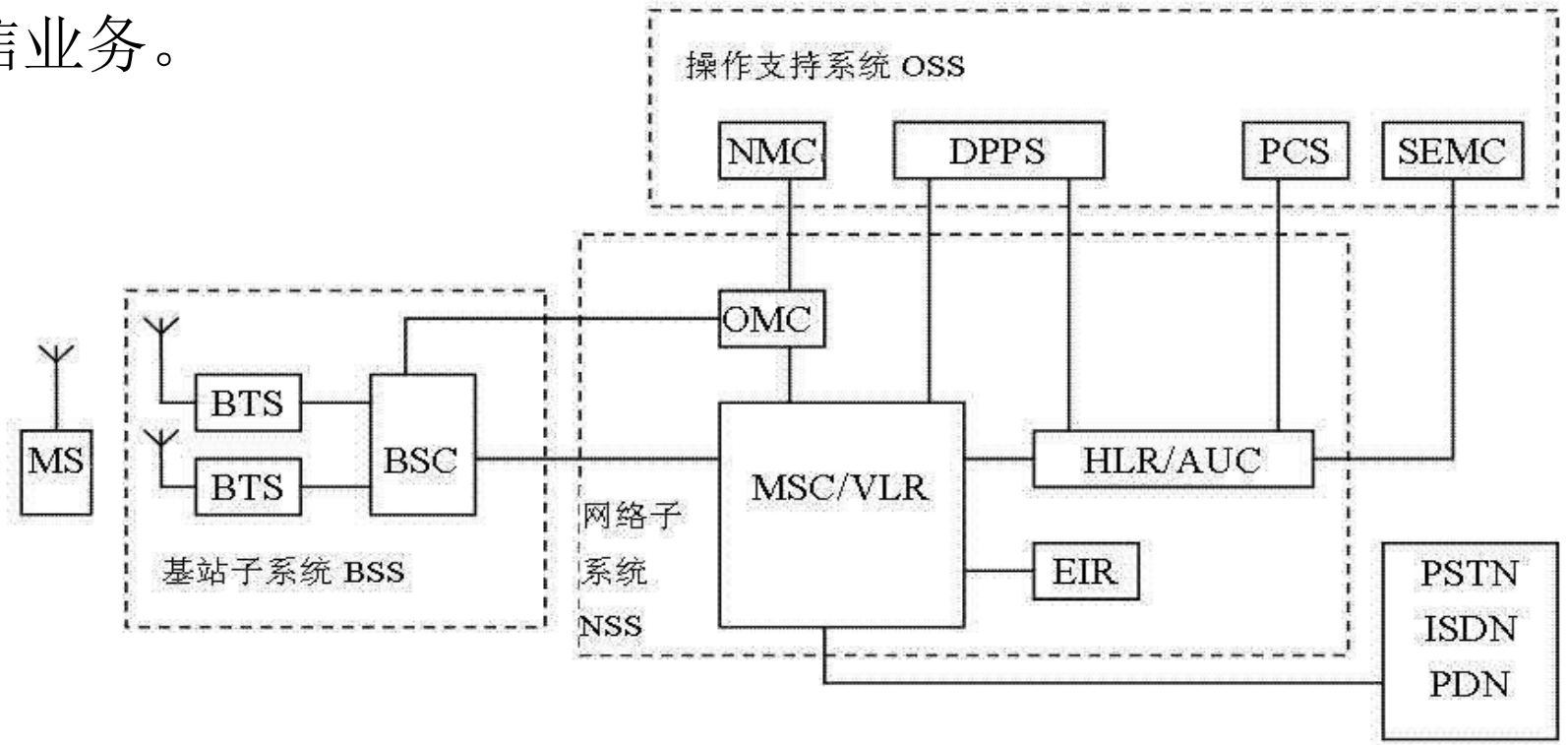
- 全球移动通信系统（global system for mobile communications）由欧洲电信标准组织ETSI制订的一个数字移动通信标准。它的空中接口采用时分多址技术。自90年代中期投入商用以来，被全球超过100个国家采用。GSM标准的无处不在使得在移动电话运营商之间签署“漫游协定”后用户的国际漫游变得很平常。

- 由于GSM系统在安全设计上的不完善，使得随着技术的发展，GSM系统的安全缺陷逐渐暴露出来，针对GSM系统的安全攻击越来越多

GSM网络概述

GSM网络的结构

GSM系统有两个主要的组成部分：固定网络基础结构（即固话网络）和移动基站。移动用户通过网络提供的服务享受无线通信业务。

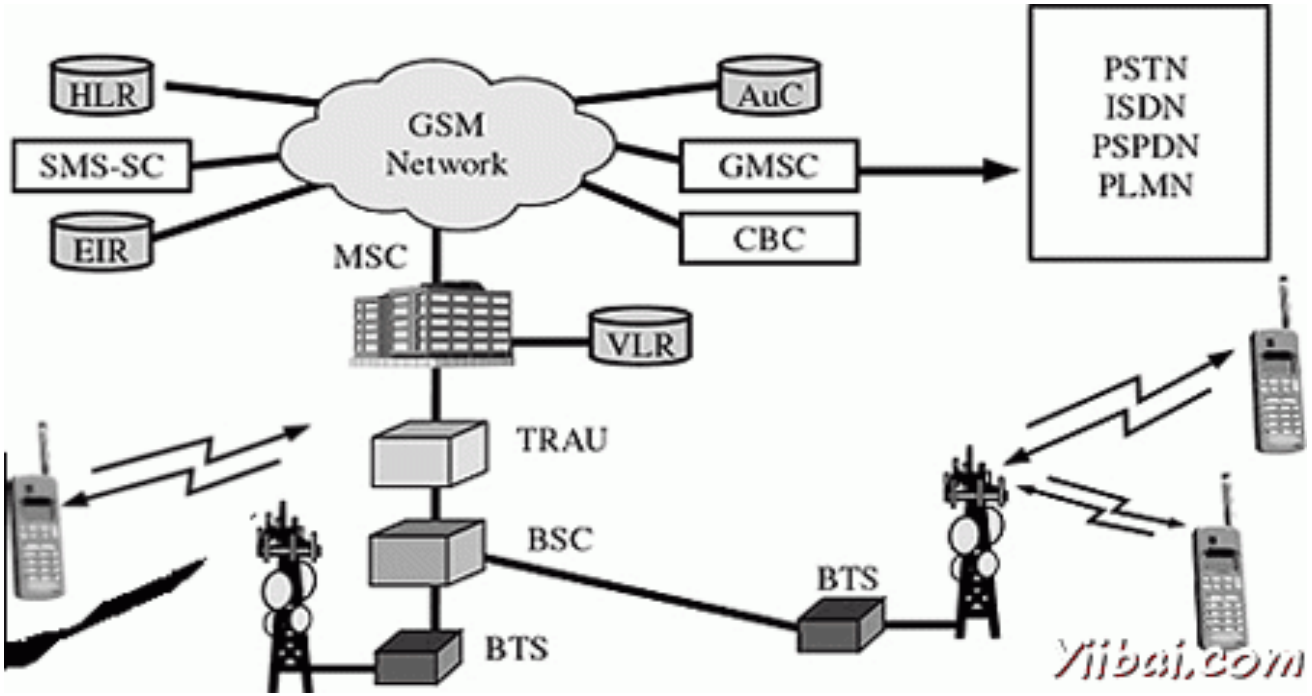


MS：移动台；BTS:收发信基站；BSC:基站控制器；MSC:移动业务交换中心；HLR：归属位置寄存器；AUC：用户鉴权中心；VLR：访问位置寄存器；

GSM网络概述

GSM网络的结构

GSM系统有两个主要的组成部分：固定网络基础结构（即固话网络）和移动基站。移动用户通过网络提供的服务享受无线通信业务。



MS：移动台；BTS:收发信基站；BSC:基站控制器；MSC:移动业务交换中心；
HLR：归属位置寄存器；AUC：用户鉴权中心；VLR：访问位置寄存器；

GSM网络的安全体系结构

◆ GSM系统中主要有两个安全目标：

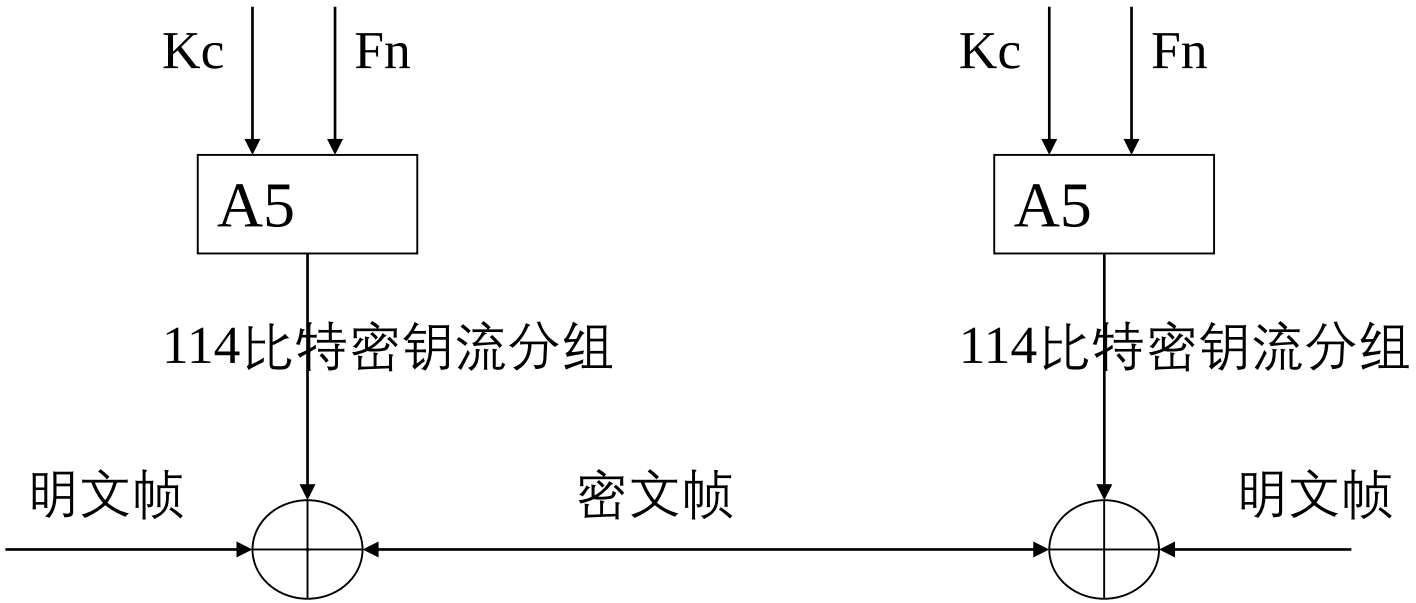
1)保护网络以防止未授权接入，同时保护用户不受假冒；

2)保护用户的隐私权。

- 通过个人化的SIM卡和PIN码实现对SIM卡的访问控制。
- 通过网络对用户的身份认证和会话密钥来防止非授权接入。
- 无线链路的加密，如移动台和基站间通信的加密。
- 在无线链路上隐藏用户的身份，如使用临时识别号（TMSI）来代替用户身份识别号（IMSI：International Mobile Subscriber Identity）

GSM系统的加密

A5算法是一个序列密码算法，通过产生密钥流与明文异或来产生密文。在通信的另一端，通过采取同样的方式与密文异或，得到明文。



GSM系统的会话密钥生成

在MS端，Kc的计算在SIM卡中进行；在固定网络端，Kc的计算在AuC中进行。Kc将一直被存放在SIM卡和AuC中直到下一次认证产生的新认证结果代替原来的会话密钥。

GSM网络的身份认证

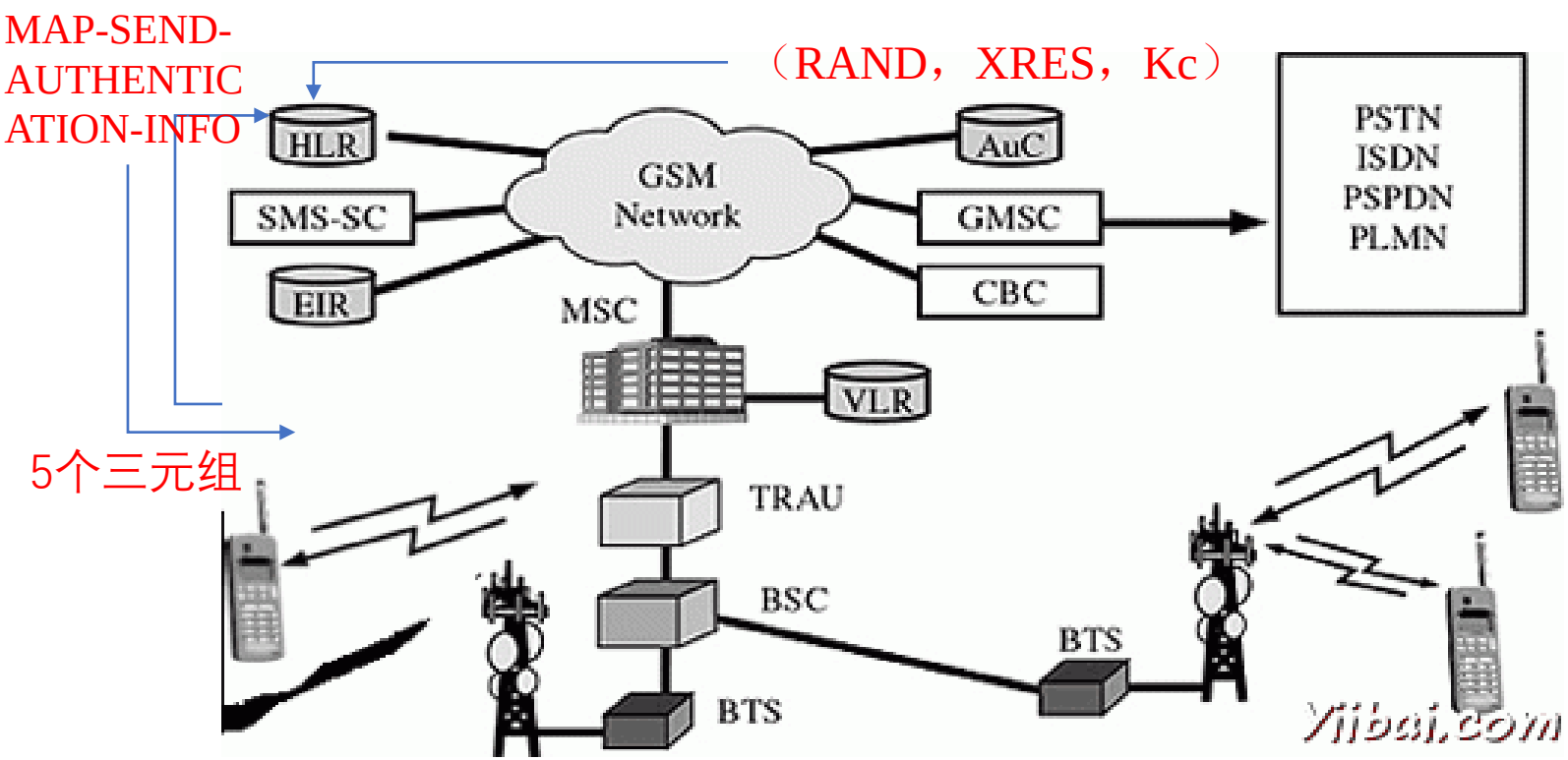
GSM的用户鉴权可以被以下几种情况激活：

1)VLR/HLR中用户相关的信息被更改。

2)用户请求网络服务。

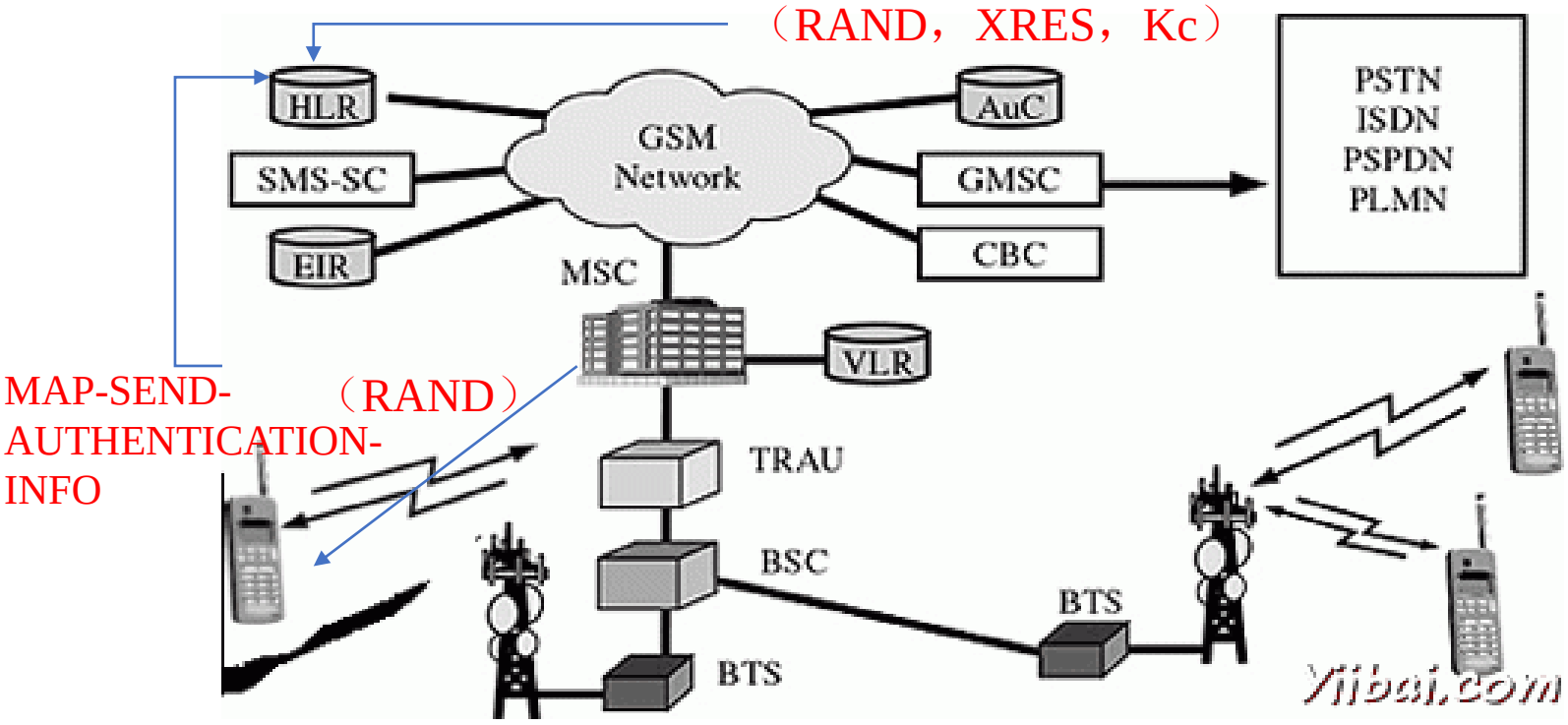
3)在MSC/VLR重启动后的第一次访问网络时。

GSM系统中的用户鉴权



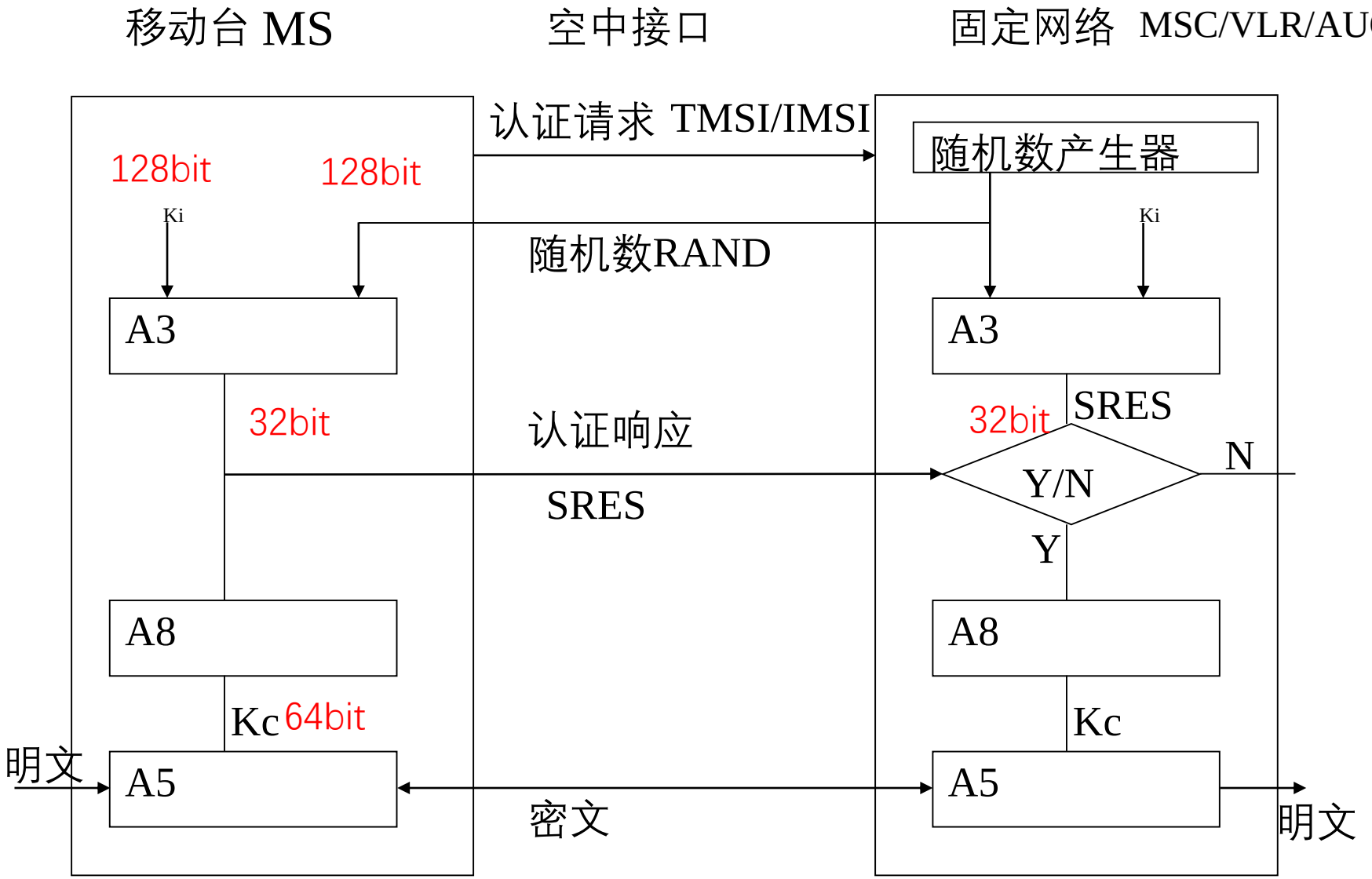
- ✓ 在GSM系统中，AuC(Authentication Center，用户鉴权中心)为每个用户准备了“鉴权三元组”（RAND，XRES，Kc），存储在HLR中。
- ✓ 当MSC/VLR需要鉴权三元组的时候，就向HLR提出要求并发出一个消息“MAP-SEND-AUTHENTICATION-INFO”给HLR（该消息包括用户的IMSI），HLR的回答一般包括五个鉴权三元组。

GSM系统中的用户鉴权



- ✓ 任何一个鉴权三元组在使用以后将被破坏，不会重复使用。
- ✓ 当移动台第一次到达一个新的MSC(Mobile-Service Switching Center,移动业务交换中心）时，MSC会向移动台发出一个随机号码RAND，发起一个鉴权认证过程（MS移动到一个新的MSC时，发起的是TMSI而不是IMSI）

GSM系统的安全体系结构



GSM系统的安全体系结构

① AuC产生一个随机数RAND，通过（AuC中的）A3、A8算法产生认证（鉴权）向量组（RAND，XRES，Kc）。

② VLR/MSC收到鉴权三元组以后存储起来。当移动台注册到该VLR时，VLR/MSC选择一个认证向量，并将其中的随机数RAND发送给移动台。

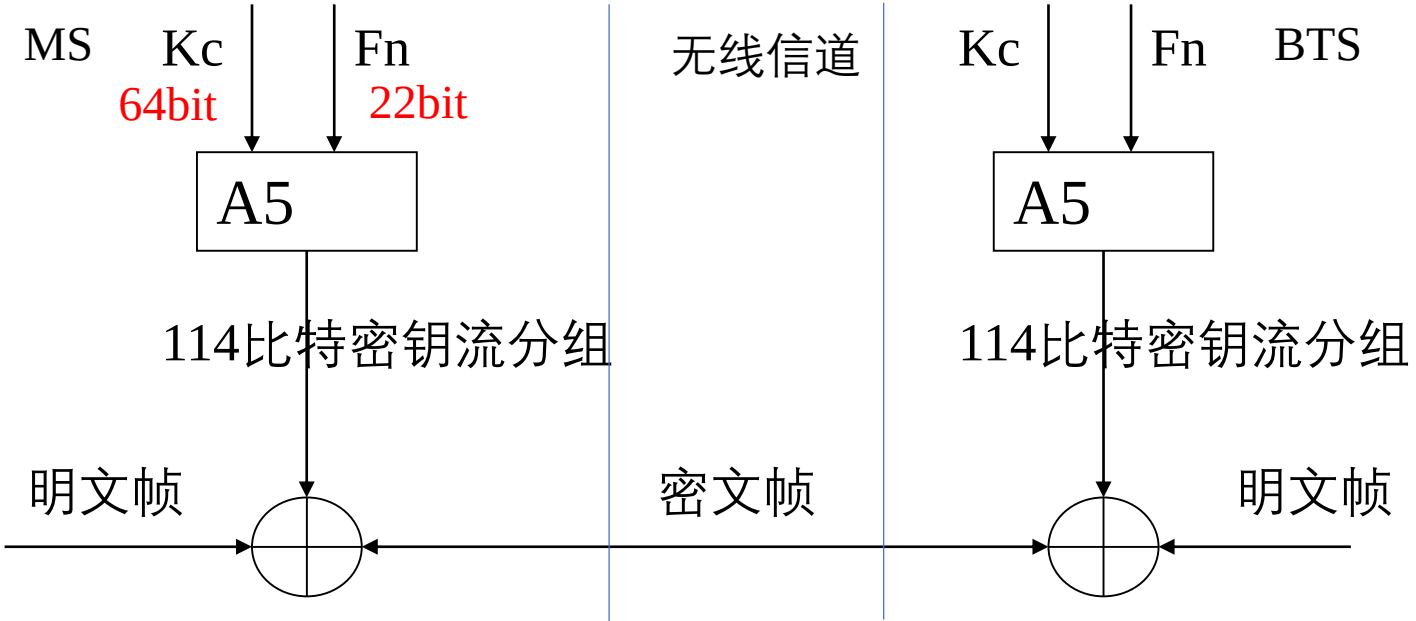
③ 移动台收到RAND以后，利用存储在SIM卡中的A3、A8算法，计算出SRES和Kc。移动台将SRES发送给VLR/MSC,如果SRES等于VLR/MSC发送给用户的RAND所在的鉴权三元组中的XRES，移动台就完成了向VLR/MSC验证自己身份的过程。

④ 由以上分析可看出，在GSM系统中，Kc从来不通过空中接口传送，存储在MS和AuC内的Kc都是由Ki和一个随机数通过A8算法运算得出的。密钥Ki以加密形式存储在SIM卡和AuC中。

GSM系统的安全体系结构

⑤ 鉴权过程完成以后，MSC将鉴权三元组中的Kc传递给基站BTS。这样使得从移动到基站之间的无线信道可以用加密的方式传递信息，从而防止了窃听。

⑥ GSM系统中无线链路信息加解密过程如下图所示。64比特的加密密钥Kc，再和当前帧号Fn(22比特)作为A5算法的输入，计算密钥流。对消息进行逐位加密异或，将密文从移动台传递到基站。基站接收到加密的信息，用相同的密钥流诸位异或来解密。



GSM系统的安全体系结构

① AuC（鉴权认证中心）存放每个用户的国际移动用户身份IMSI，用于用户开机登陆网络或者在临时移动用户身份TMSI不能使用时验证或搜索用户；存放用户的密钥Ki(在用户使用IMSI接续的时候，Ki被授予给用户)；为完成鉴权过程，AuC要负责生成随机值RAND；AuC中还存放了鉴权算法A3以及数据加密密钥生成算法A8。

② VLR/MSC为每个IMSI存放若干鉴权三元组。为了避免IMSI被截取，需要最大限度的减少在无线信道上传送。因此在VLR中记录TMSI与IMSI的对应关系，仅在无线信道上发送移动用户的TMSI.

③ BTS中存储编码算法A5和密钥Kc，用于解密接收到的密文形式的用户数据和信令数据（包括解密）。

④ 移动台将鉴权算法A3和数据加密密钥生成算法A8、用户密钥Ki以及用户身份IMSI(TMSI)存储在SIM卡中。SIM卡是一种防篡改的设备，增强了算法和密钥的安全性。编码算法A5和由A8计算出的加密密钥Kc存储在手机中。

⑤ 由此可以看出A3、A8、A5、Ki、Kc是不在网络中传递的，从而增强了网络的安全性。

GSM存在的安全问题

① GSM系统中的认证是单向的，只有网络对用户的认证，而没有用户对网络的认证。因此存在安全漏洞，非法的设备（如基站）可以伪装成的合法的网络成员，从而欺骗用户，窃取用户的信息。

② GSM系统中的加密不是端到端的，只是在无线信道部分即MS和BTS之间进行加密。在固定网中没有加密，采用明文传输，这给攻击者提供了机会

③ 在移动台第一次注册和漫游时，IMSI可能以明文方式发送到VLR/MSC，如果攻击者窃听到IMSI，则会出现手机“克隆”。

④ 在移动通信中，移动台和网络间的大多数信令信息是非常敏感的，需要得到完整性保护。而在GSM网络中，没有考虑数据完整性保护的问题，如果数据在传输的过程中被篡改也难以发现。

⑤ 随着计算机硬件技术带来的计算速度的不断提供，解密技术也不断发展。GSM中使用的加密密钥长度是64比特，在现在解密技术下，已经可以在较短时间内被破解。

GSM存在的安全问题

⑥ 在GSM系统中，加密算法是不公开的，这些密码算法的安全性不能得到客观的评价，在实际中，也收到了很多攻击。

⑦ 在GSM系统中，加密算法是固定不变的，没有更多的密钥算法可供选择，缺乏算法协商和加密密钥协商的过程。

		GSM	3G
网络认证用户身份		有	有
用户认证网络身份		无	有
数据加密传输	算法	A5	f8
	密钥	Kc:64bit	CK:128bit
	算法灵活性	固定的加密算法	用户可与网络协商加密算法
数据完整性保护		无	有
用户身份识别（IMSI的传送）		IMSI以明文方式在无线链路上传送	增强的用户身份认证（EUIC）
安全服务对用户的可见性		无	增加安全操作对用户的可见性

作业

1. 安全协议的四大属性。
2. 用图示意四大属性的实现案例。