现代密码学

第一讲 密码学的基本概念

信息与软件工程学院

第一讲 密码学的基本概念

- 信息安全与安全威胁
- 什么是密码学
- 密码算法的分类
- 密码学的作用和地位

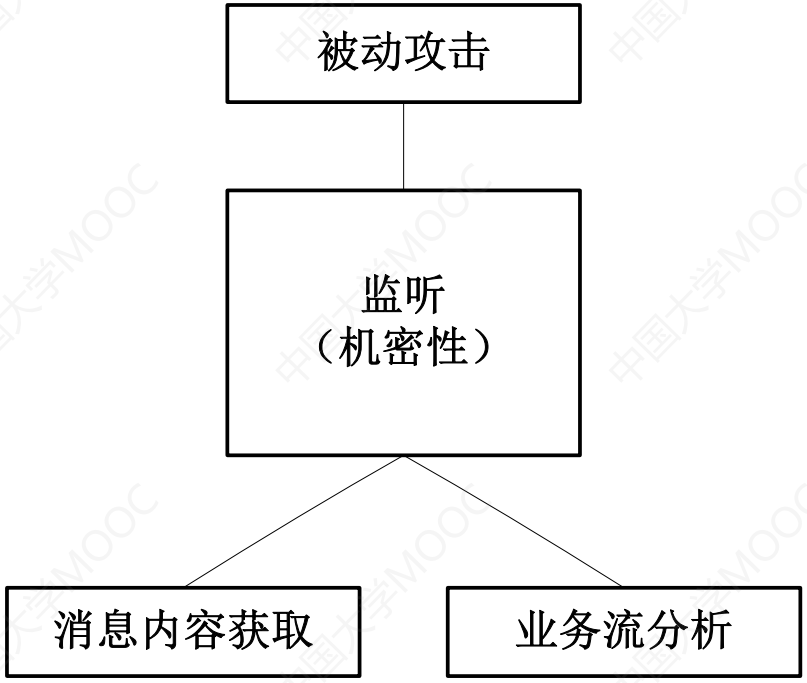
信息时代网络无处不在

威胁信息安全的主要方式

（1）信息泄露
（2）破坏信息的完整性
（3）拒绝服务
（4）非法使用
（5）窃听
（6）业务流分析
（7）假冒
（8）旁路控制
（9）授权侵犯
（10）特洛伊木马
（11）陷阱门
（12）抵赖
（13）重放
（14）计算机病毒
（15）人员不慎
（16）媒体废弃
（17）物理侵入
（18）窃取
（19）业务欺骗

攻击手段分类

1. 被动攻击



2. 主动攻击

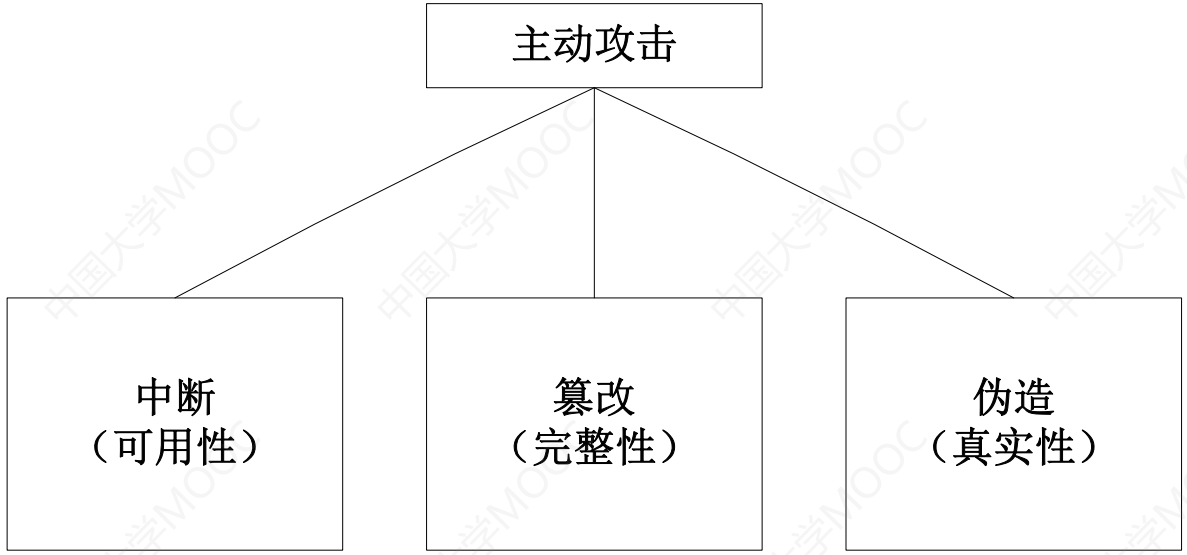
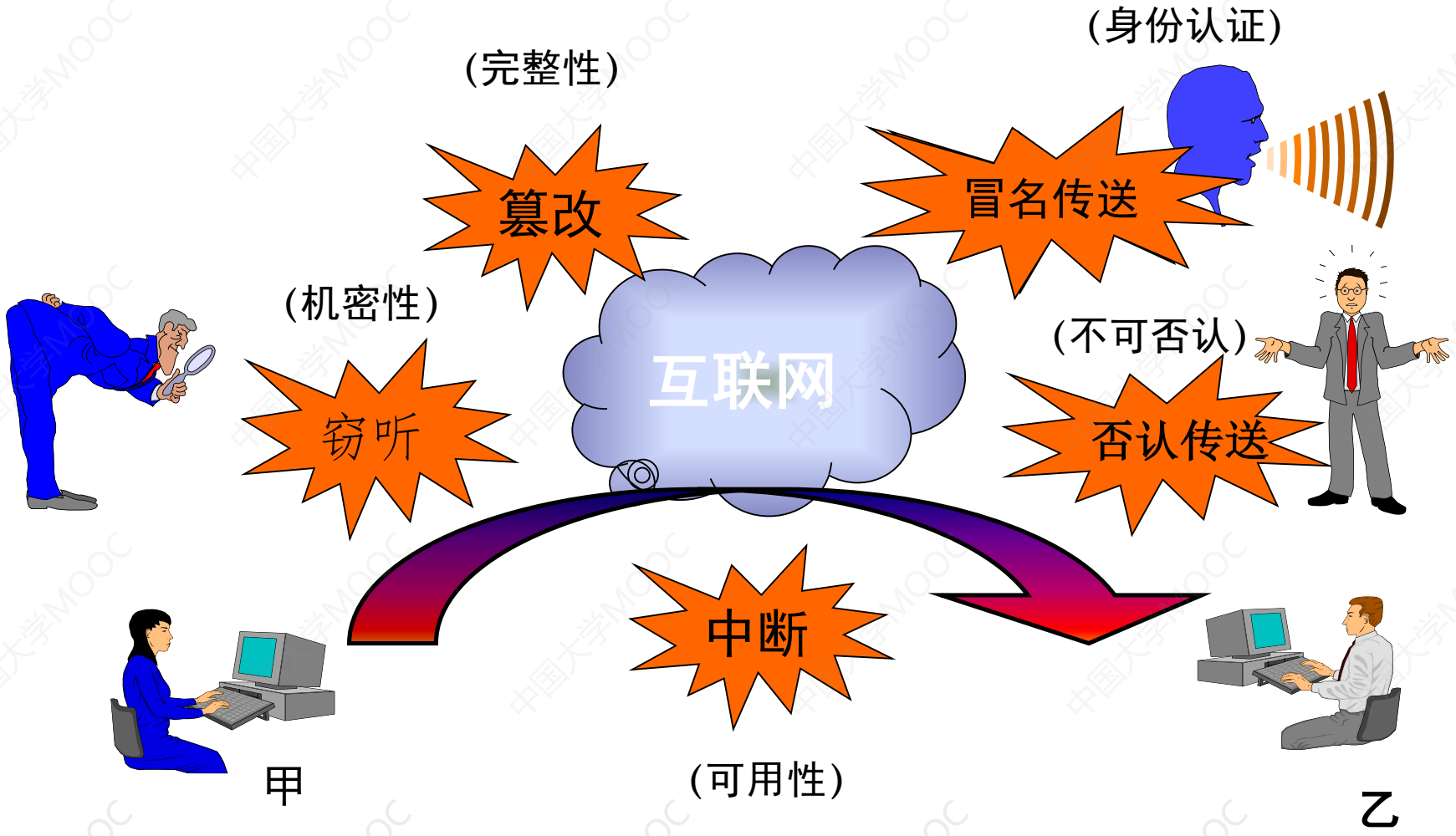


图1.1 攻击分方式及特点

信息为什么不安全



第一讲 密码学的基本概念

- 信息安全与安全威胁
- 什么是密码学
- 密码算法的分类
- 密码学的作用和地位

什么是密码？

解锁的数字?

登录的口令?

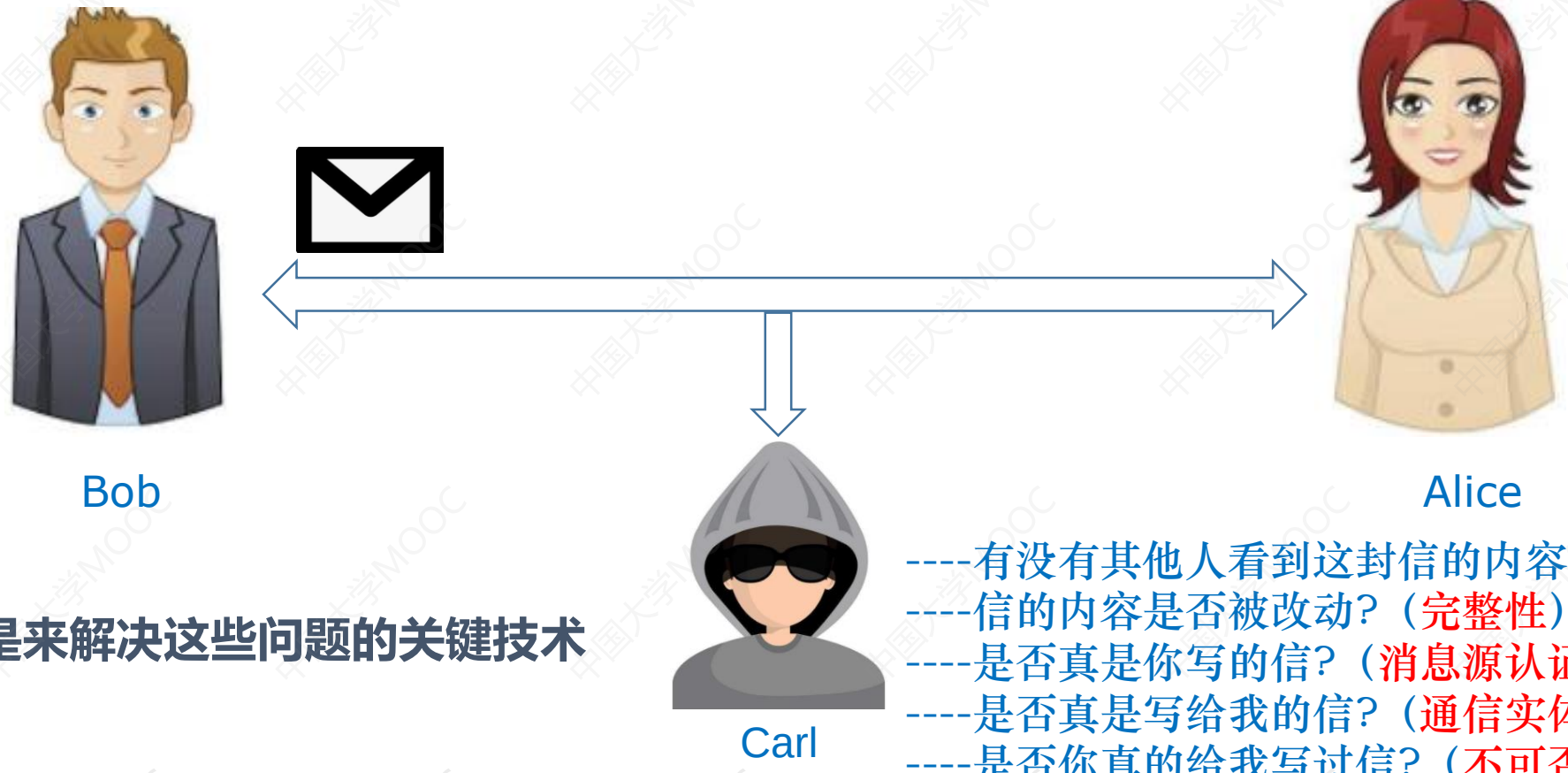
隐藏的奥秘?

这都不是今天我要给同学们讲的密码

什么是密码？

- 什么是密码？
  - 密码是指采用特定变换的方法对信息等进行加密保护、安全认证的技术、产品和服务。——《中华人民共和国密码法》
- 什么是密码学？
  - 密码学是研究编制密码和破译密码的技术科学。
    - 研究密码变化的客观规律，应用于编制密码以保护通信秘密的，称为密码编码学。
    - 应用于破译密码以获取通信情报的，称为密码分析学或破译学。

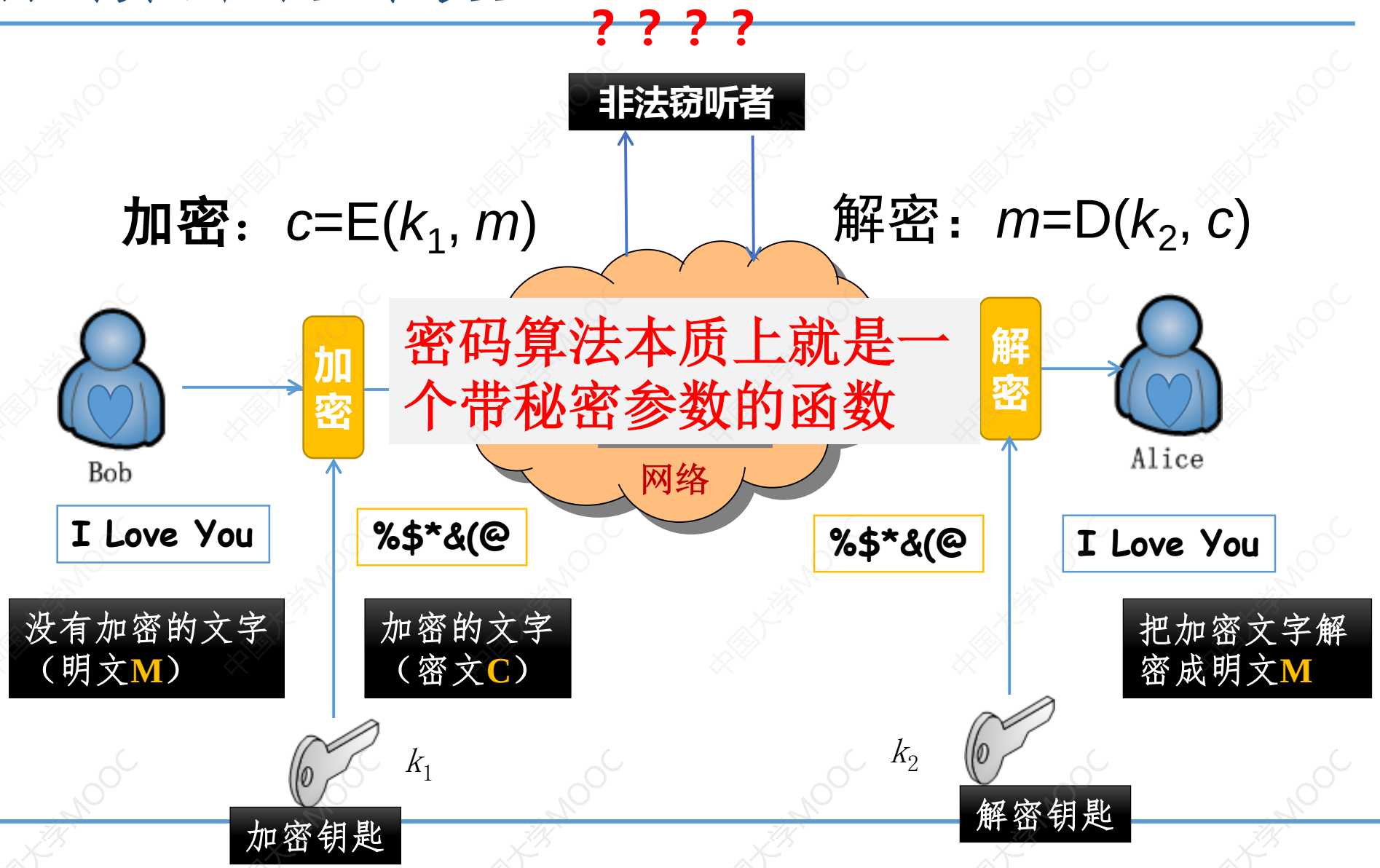
什么是密码学？



密码学就是来解决这些问题的关键技术

----有没有其他人看到这封信的内容？（机密性）
----信的内容是否被改动？（完整性）
----是否真是你写的信？（消息源认证）
----是否真是写给我的信？（通信实体认证）
----是否你真的给我写过信？（不可否认性）

密码算法的基本模型


？？？？
非法窃听者
加密：$c=E(k_1, m)$
解密：$m=D(k_2, c)$
密码算法本质上就是一个带秘密参数的函数
Bob
加密
网络
解密
Alice
I Love You
%$*&(@
%$*&(@
I Love You
没有加密的文字（明文M）
加密的文字（密文C）
把加密文字解密成明文M
k_1
k_2
加密钥匙
解密钥匙

密码算法

基本概念

- 明文M ——要处理的数据——**Message (Plaintext)**
- 密文C ——处理后的数据——**Ciphertext**
- 密钥k_1, k_2 ——秘密参数——**Key**
- 加密函数：$C = E(k_1, M)$或$C = E_{k_1}(M)$——**Encryption**
- 解密函数：$M = D(k_2, C)$或$M = D_{k_2}(C)$——**Decryption**

密码算法（续）

- 密码算法需求：
  - 需求1：可逆——算法的使用者可以将密文恢复成明文
  - 需求2：不可逆——敌手无法将密文恢复成明文
  - 秘密参数——密钥
- 密码算法实际上是一个带有秘密参数的函数。
  - 知道秘密参数，求逆非常容易
  - 不知道秘密参数，求逆是不可行的

密码算法（续）

一个好的密码体制至少应满足的两个条件：

（1）在已知明文m和加密密钥k_1时，计算$c = E_{k_1}(m)$容易，

在已知密文c和解密密钥k_2时，计算$m = D_{k_2}(c)$容易；

（2）在不知解密密钥k_2时，不可能由密文c恢复出明文m。

第一讲 密码学的基本概念

- 信息安全与安全威胁
- 什么是密码学
- 密码算法的分类
- 密码学的作用和地位

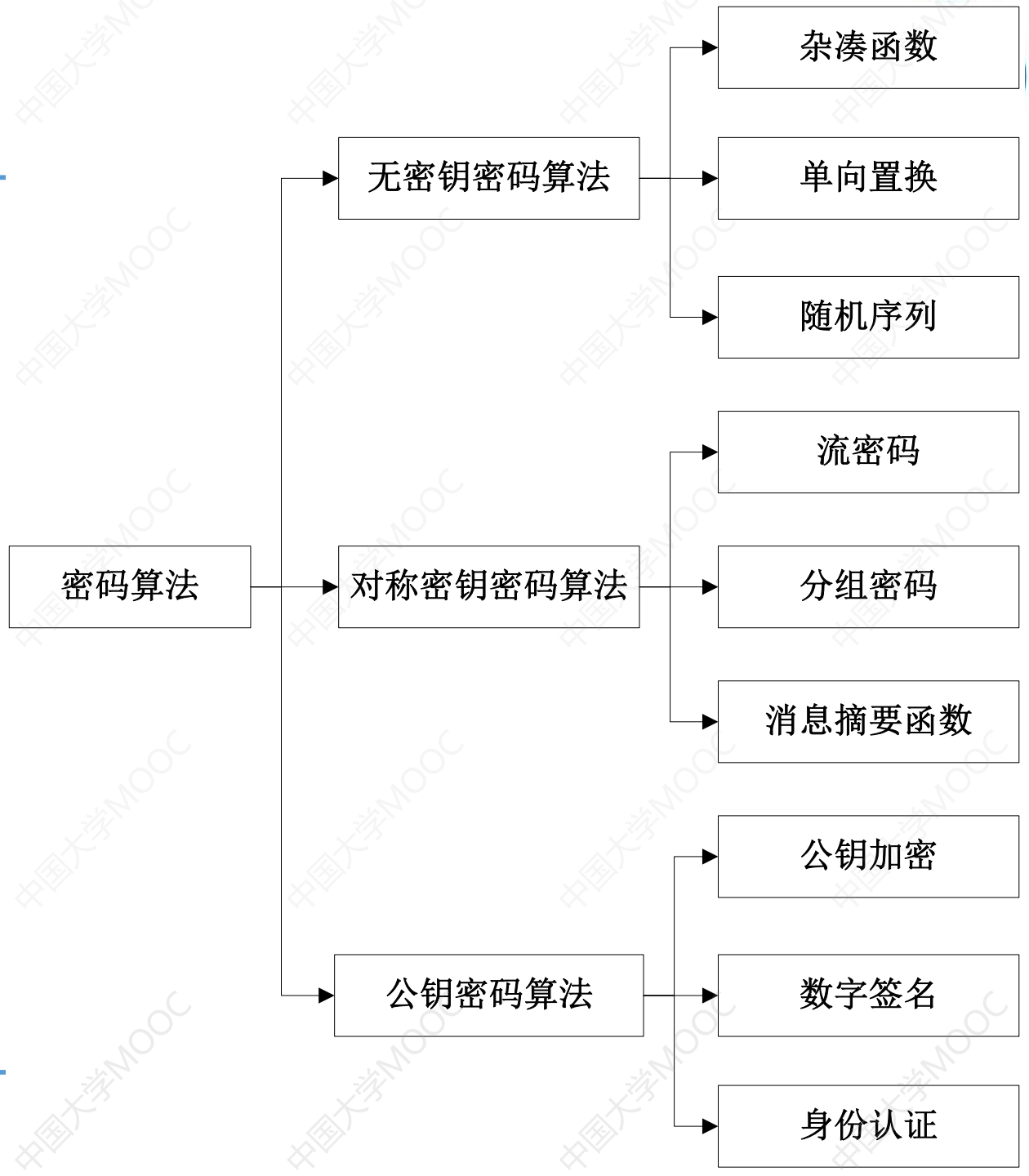
密码算法分类

机密性：对称密钥加密（流密码、分组密码）、公钥加密

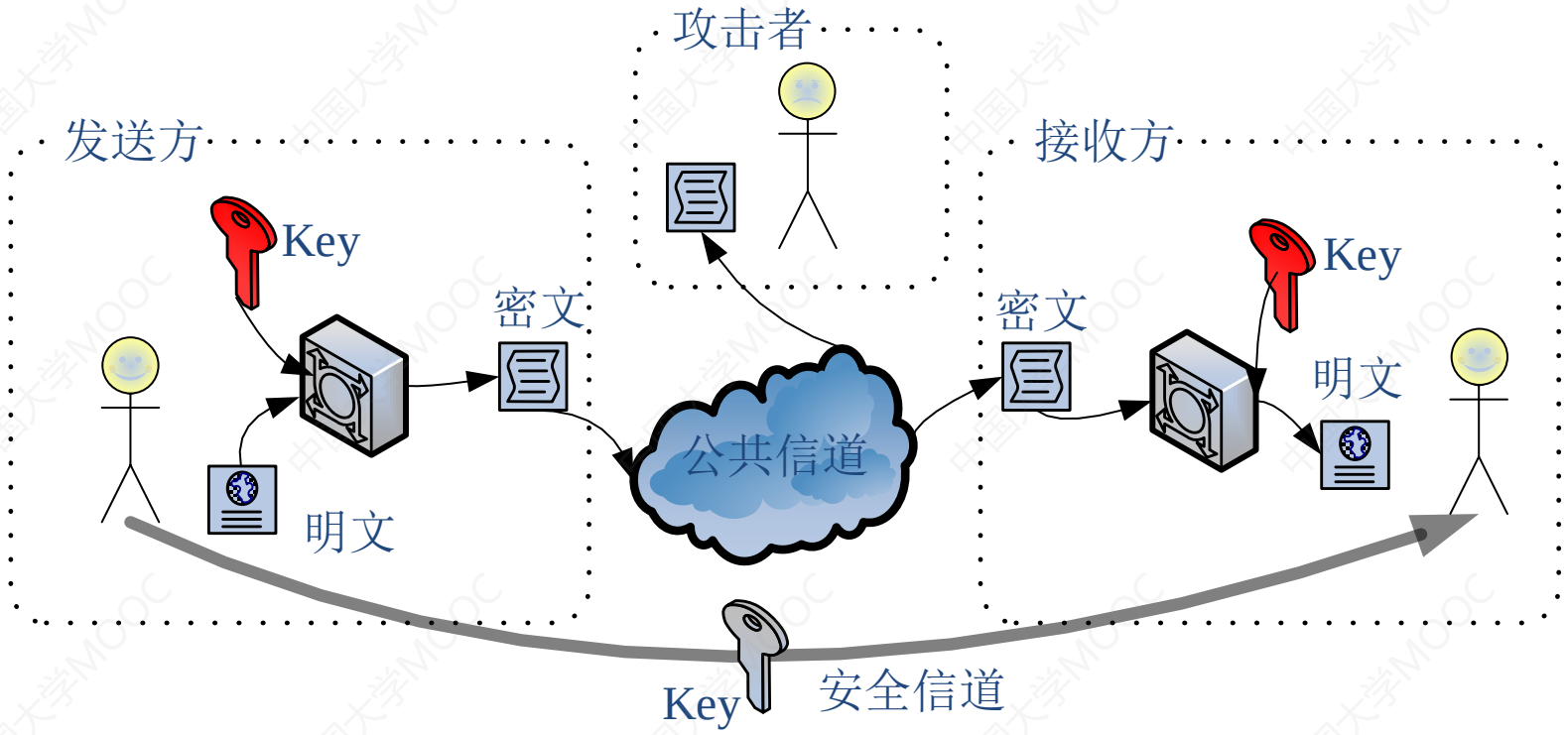
完整性：杂凑函数、消息摘要函数

认　证：数字签名、身份认证协议

不可否认性：数字签名

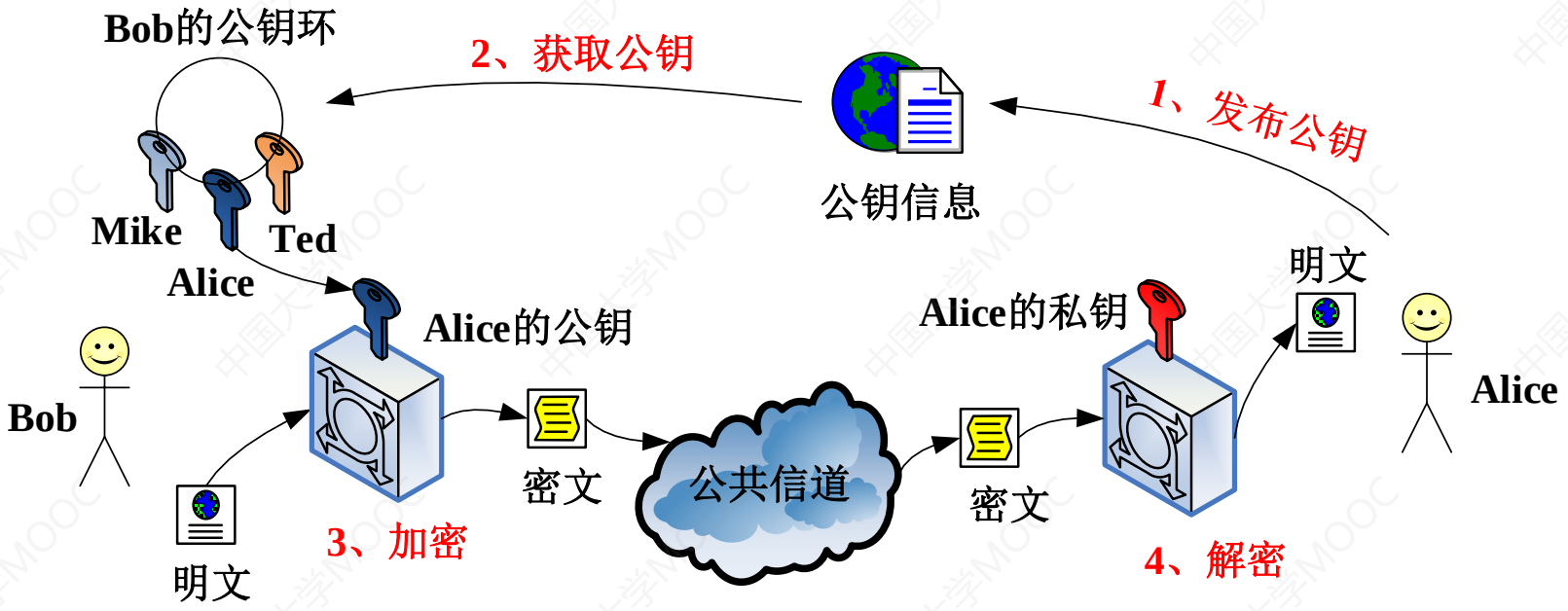


对称密钥加密算法



- 特点：
  - 加解密密钥相同
  - 加解密速度快
- 应用：
  - 大量数据加密
  - 消息认证码
- 常见算法：
  - ZUC，DES，AES，SM4……

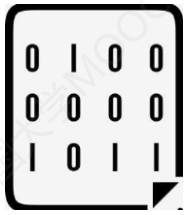
公开密钥密码体制



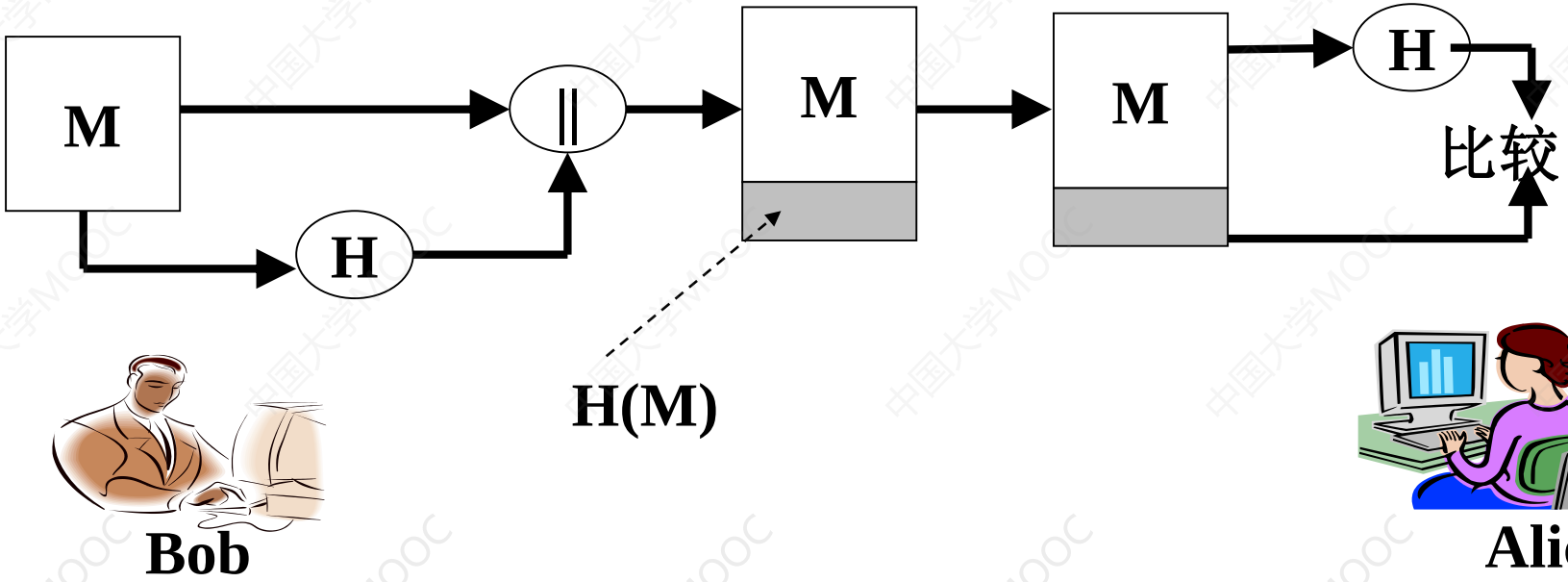
- 特点：
  - 加解密密钥不同
  - 加解密速度慢
- 应用：
  - 短消息加密
  - 数字签名
  - 身份认证
- 常见算法：
  - RSA，ECC，SM2，ElGamal....

杂凑函数（Hash算法）

任意长度数据



定长摘要值



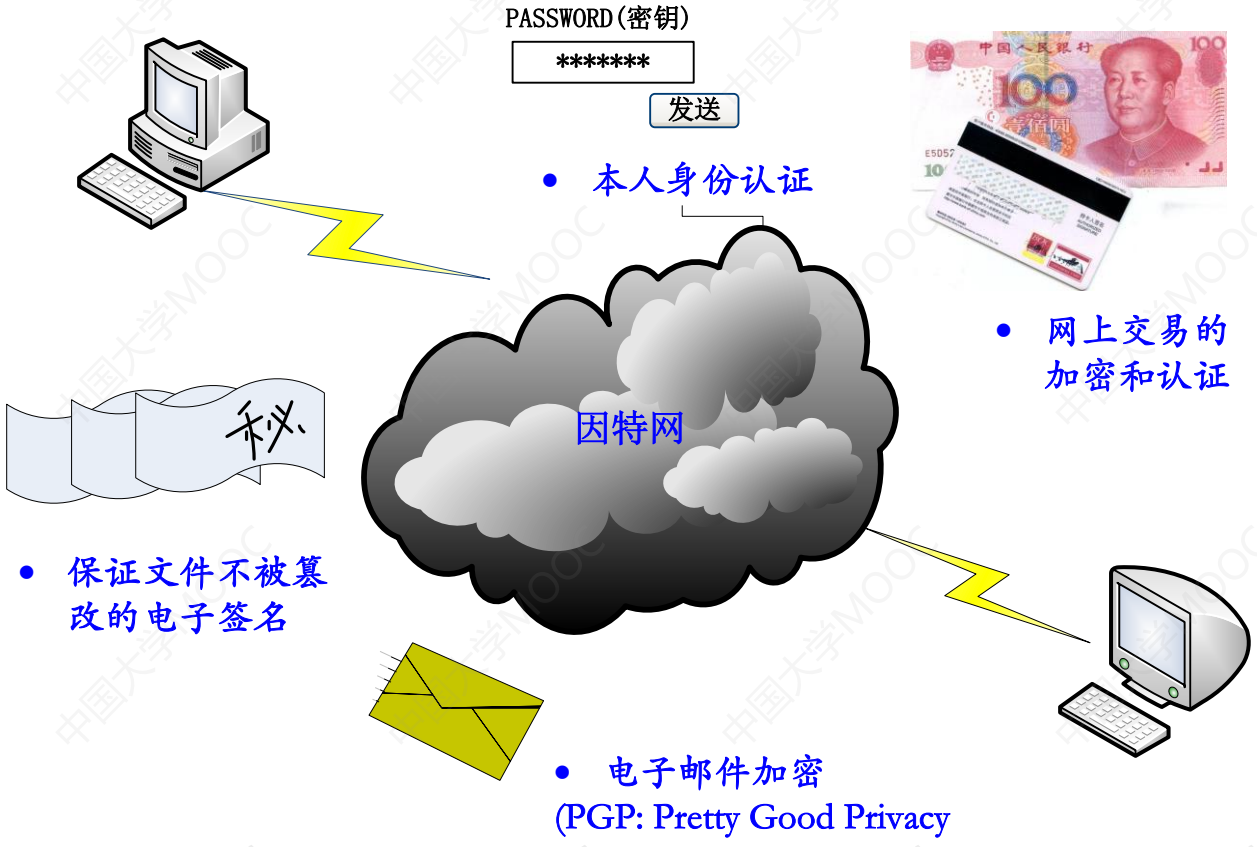
- 特点：
  - 任意长输入映射为定长输出；
  - 输入变化，输出发生不可预测的变化；
  - 输出无法推导出输入。
- 应用：
  - 完整性校验；
- 常见算法：
  - SHA系列，MD5，SM3……

第一讲 密码学的基本概念

- 信息安全的基本属性
- 什么是密码学
- 密码算法的分类
- 密码学的作用和地位

为什么需要密码学？

- **现代密码在社会中的广泛应用**



“密码技术”是保障信息安全的基本技术

密码学的重要性

目前，密码学被应用到国家安全、电子商务、隐私保护……，几乎所有信息安全的领域都用密码学的身影。

棱镜门事件

华住5亿用户信息泄露

“没有网络安全就没有国家安全”——习近平《在中央网络安全和信息化领导小组第一次会议上的讲话》（2014年）

密码是国家重要战略资源，是保障网络与信息安全的核心技术和基础支撑。

密码工作是党和国家的一项特殊重要工作，直接关系国家政治安全、经济安全、国防安全和信息安全。

《中华人民共和国密码法》


深入学习贯彻密码法　奋力开创新时代密码工作新局面
中华人民共和国
密码法
法律出版社
中华人民共和国主席令
第三十五号
《中华人民共和国密码法》已由中华人民共和国第十三届全国人民代表大会常务委员会第十四次会议于2019年10月26日通过，现予公布，自2020年1月1日起施行。
中华人民共和国主席　习近平
2019年10月26日
Baidu 百科


《中华人民共和国密码法》的主要内容
日前，全国人大常委会审议通过《中华人民共和国密码法》，自2020年1月1日起施行
密码法是总体国家安全观框架下，国家安全法律体系的重要组成部分，也是一部技术性、专业性较强的专门法律
密码法共五章四十四条，重点规范了以下内容：
第一章 总则部分
规定了本法的立法目的、密码工作的基本原则、领导和管理体制，以及密码发展促进和保障措施
第二章 核心密码、普通密码部分
规定了核心密码、普通密码使用要求、安全管理制度以及国家加强核心密码、普通密码工作的一系列特殊保障制度和措施
第三章 商用密码部分
规定了商用密码标准化制度、检测认证制度、市场准入管理制度、使用要求、进出口管理制度、电子政务电子认证服务管理制度以及商用密码事中事后监管制度
第四章 法律责任部分
规定了违反本法相关规定应当承担的相应的法律后果
第五章 附则部分
规定了国家密码管理部门的规章制定权，解放军和武警部队密码立法事宜以及本法的施行日期
新华社记者 孟丽静 编制

新增专业（2021.2.10）

2020年度普通高等学校本科专业备案和审批结果

二、新增审批本科专业名单

序号	主管部门、学校名称	专业名称	专业代码	学位授予门类	修业年限	备注
教育部						
9	南开大学	密码科学与技术	080918TK	工学	四年	新专业
13	山东大学	密码科学与技术	080918TK	工学	四年	新专业
15	华中科技大学	密码科学与技术	080919TK	工学	四年	新专业
19	西安电子科技大学	密码科学与技术	080918TK	工学	四年	新专业
中央办公厅						
21	北京电子科技学院	密码科学与技术	080918TK	工学	四年	新专业
工业和信息化部						
26	北京理工大学	密码科学与技术	080918TK	工学	四年	新专业
海南省						
152	海南大学	密码科学与技术	080918TK	工学	四年	新专业

新增职业（2021.1.5）

- 4-07-05-06 密码技术应用员
- 定义：运用密码技术，从事信息系统安全密码保障的架构设计、系统集成、检测评估、运维管理、密码咨询等相关密码服务的人员。
- 主要工作任务：
- 1.分析信息系统安全威胁和业务应用场景的密码应用需求；
- 2.设计密码保障应用规划和实施方案；
- 3.从事信息系统的密码资源融合部署实施工作；
- 4.依据标准和规范，开展信息系统密码应用安全性评估工作；
- 5.从事密钥资产安全管理与使用工作；
- 6.应急处置密码应用安全突发事件；
- 7.从事信息系统密码应用态势监控与运维工作；
- 8.提供密码应用技术咨询、密码职业技能培训、密码科普等相关服务。

感 谢 聆 听!

xynie@uestc.edu.cn