IP spoofing

- 通常认为IP报文嵌入的是发送方的源IP地址
  - Easy to override using raw sockets
  - SCAPY, libnet: tools for formatting raw packets with arbitrary IP headers
- 任何拥有主机的人都可以发送具有任意源IP地址的数据包
  - response will be sent back to forged source IP
- 结果:
  - 匿名DoS攻击（e.g. Memcached DRDoS）
  - 匿名感染攻击（e.g. slammer worm）

ARP MiTM attack

- ettercap

① 查找并设置攻击目标

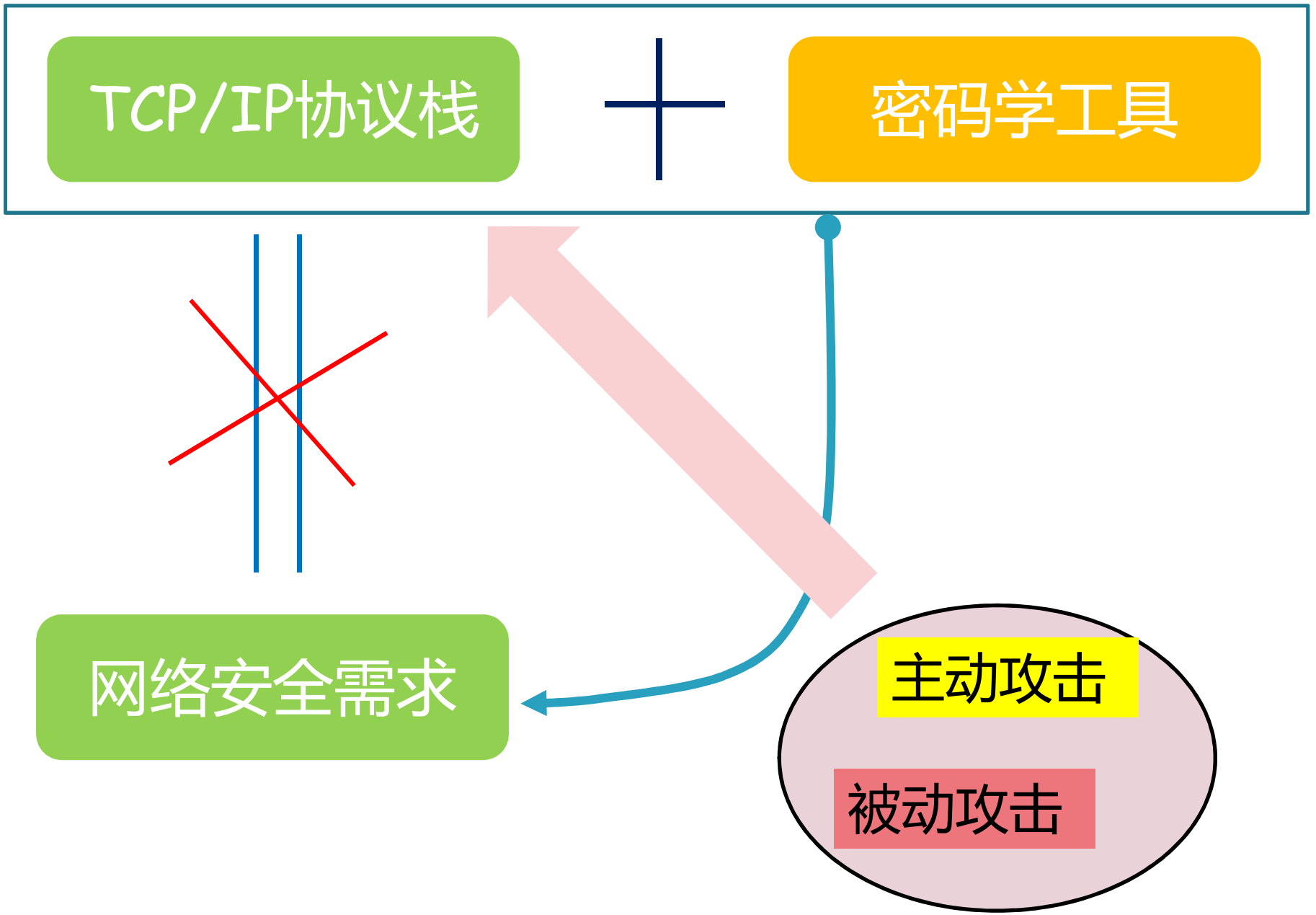
② 启动ARP poisoning 攻击

③ 添加过滤器（事先写好，编译）

- 篡改网页
- 挂马
- 注入js
- 修改下载链接（导向后门程序）
- Dns欺骗（钓鱼攻击）
- ……

主动攻击特点总结

- 可以检测
  - 由于构成系统的物理通信设施、软件和网络协议等存在各种潜在的弱点，因此主动攻击难以绝对防御，但是可以检测。因此，针对主动攻击，重点在于检测并从破坏中恢复过来。


TCP/IP协议栈
密码学工具
网络安全需求
主动攻击
被动攻击

密码学工具箱

密码学工具箱

- 对称加密算法
- 公钥加密算法
- 哈希算法
- 消息认证码
- 随机数
- 密钥协商

openssl

- OpenSSL由三部分组成：
  - libencrypto库
  - libssl库
  - openssl命令行工具
- Programming tutorial
  - https://www.linuxjournal.com/article/4822
  - https://www.linuxjournal.com/article/5487

对称加密算法

- 加密密钥与解密密钥相同
- 加解密效率高
- 典型对称加密算法
  - AES、3DES、RC2、RC4
  - 加密命令：openssl enc -aes-128-cbc -a -in datafile.txt -out cipherdata.txt -pass pass:12345678 -p

适合加密大量数据

公钥加密算法

- 加密密钥和解密密钥不同
- 加解密效率低
- 典型公钥加密算法包括
  - RSA、ElGamal、ECC

不适合加密大量数据，但可用于密钥分发、数字签名等

RSA加解密示例

- 生成私钥
  - openssl genrsa -out privatekey.key 1024
- 生成公钥
  - openssl rsa -in privatekey.key -pubout -out publickey.key
- 加密数据
  - openssl rsautl -encrypt -in test.txt -inkey publickey.key -pubin -out outfile
- 解密数据
  - openssl rsautl -decrypt -in outfile -inkey privatekey.key -out plaintext.txt

哈希（hash）算法

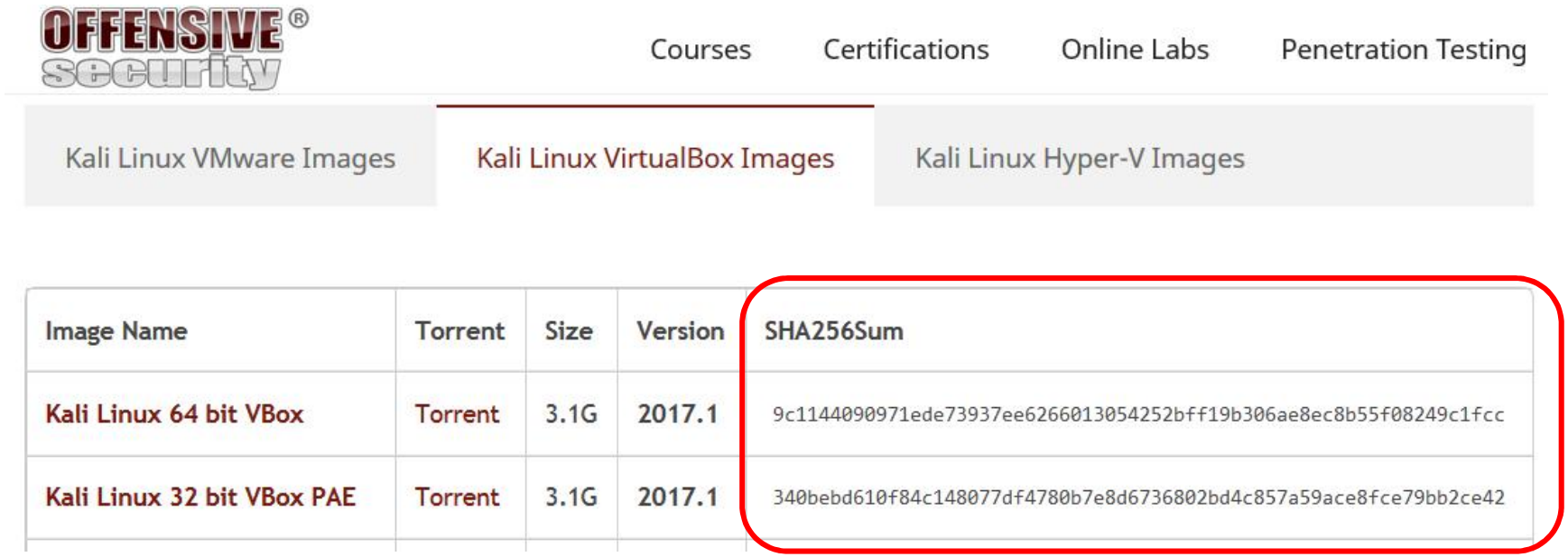
- 接收任意长度的数据，输出定长的散列值
- 密码学哈希函数应具备
  - 映射分布均匀性和差分分布均匀性
  - 单向性
  - 抗冲突性，包括：
    - 抗弱冲突性：给定M，计算上无法找到M'，满足H(M) = H(M')
    - 抗强冲突性：计算上也难以寻找一对任意的M和M'，使其满足H(M) = H(M')

哈希算法

- ~~消息摘要算法5，MD5~~
  - 不安全，不应使用
- ~~SHA-1~~
  - 不安全，不应该用于新的用途
- SHA-2(SHA-256, SHA-384, SHA-512)
- RIPEMD-160（用于bitcoin）
- SHA-3（Keccak）

哈希函数：用途1

- 检测软件是否被篡改
  - openssl dgst -sha256 filename



哈希函数：用途2

- 基于口令的加密
- 数字签名
- 伪随机数生成器
- 消息认证码

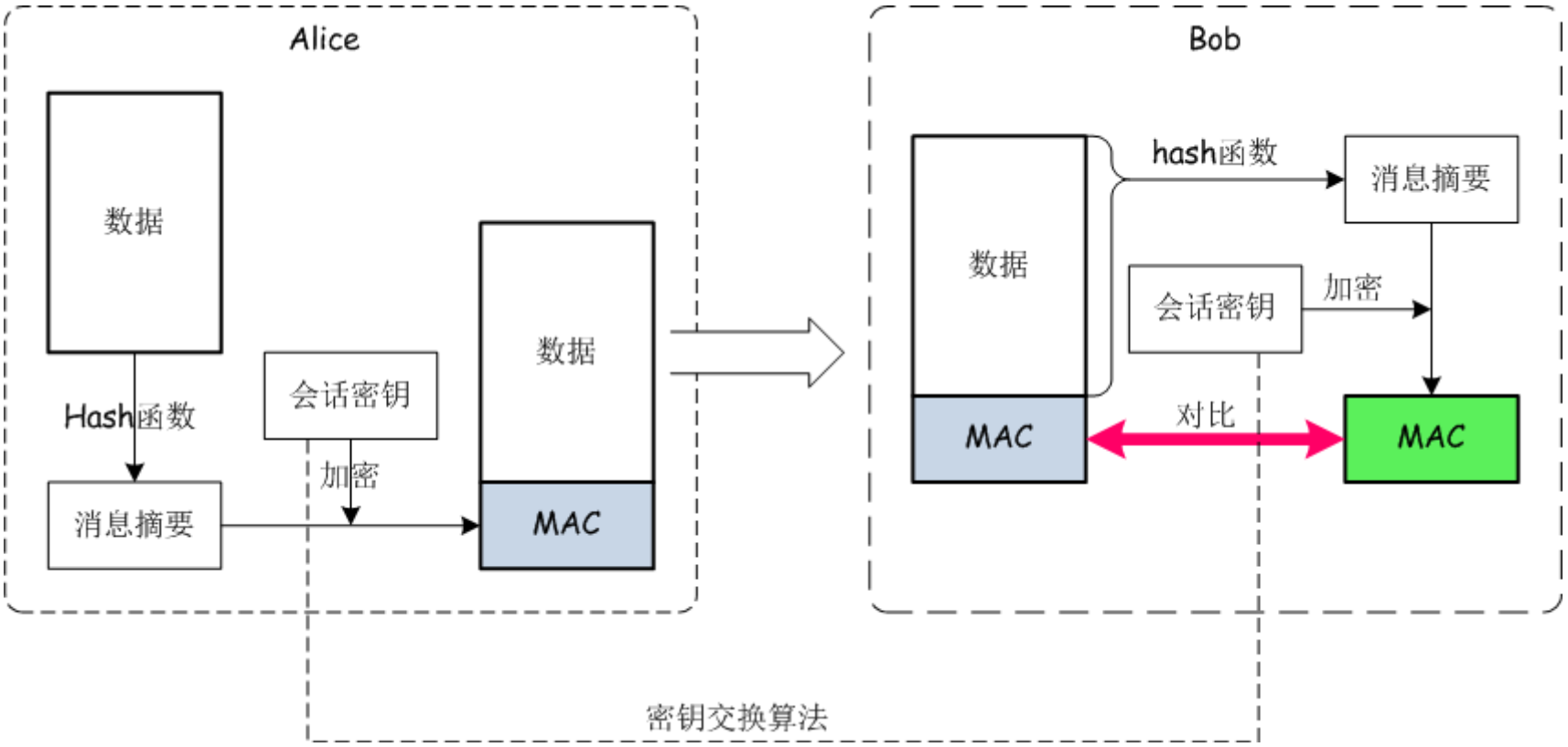
消息认证码(MAC)

Alice发送一条消息给Bob，Bob收到消息后，怎么来确认消息没有被篡改过呢？怎么确认消息就是来自Alice呢？

~~Hash函数？~~

- 消息认证码（Message Authentication Code）
  - 确认消息完整性
  - 消息源发认证

消息认证码1：基于已有加密算法



采用对称加密算法，比如DES等

而密钥交换可以是DH等。

消息认证码2：HMAC

- Hash-based Message Authentication Code

$$HMAC(\mathrm{K},\mathrm{M}) = \mathrm{H}(\mathrm{K} \otimes opad \mid \mathrm{H}(\mathrm{K} \otimes ipad \mid M))$$

- H是hash函数，如：SHA-2
- K是密钥
- opad和ipad分别为0X5C和0X36组成的填充字符串
- M是消息
- |表示拼接，⊗表示XOR运算

消息认证码：总结

- 输入：
  - 任意长度的消息
  - 发送者和接收者之间共享的密钥
- 输出：
  - 固定长度的数据：*MAC*

总之，消息认证码是一种与密钥相关联的单向散列函数

随机数

- 具有下述属性
  - 随机性：不存在统计学偏差，是完全杂乱的数列
  - 不可预测性：不能从过去的数列推测出下一个出现的数
  - 不可重现性：除非将数列本身保存下来，否则不能重现相同的数列

随机数

	随机性	不可预测性	不可重现性	
弱伪随机数	✓	×	×	只具备随机性
强伪随机数	✓	✓	×	具备不可预测性
真随机数	✓	✓	✓	具备不可重现性

可用于密码技术

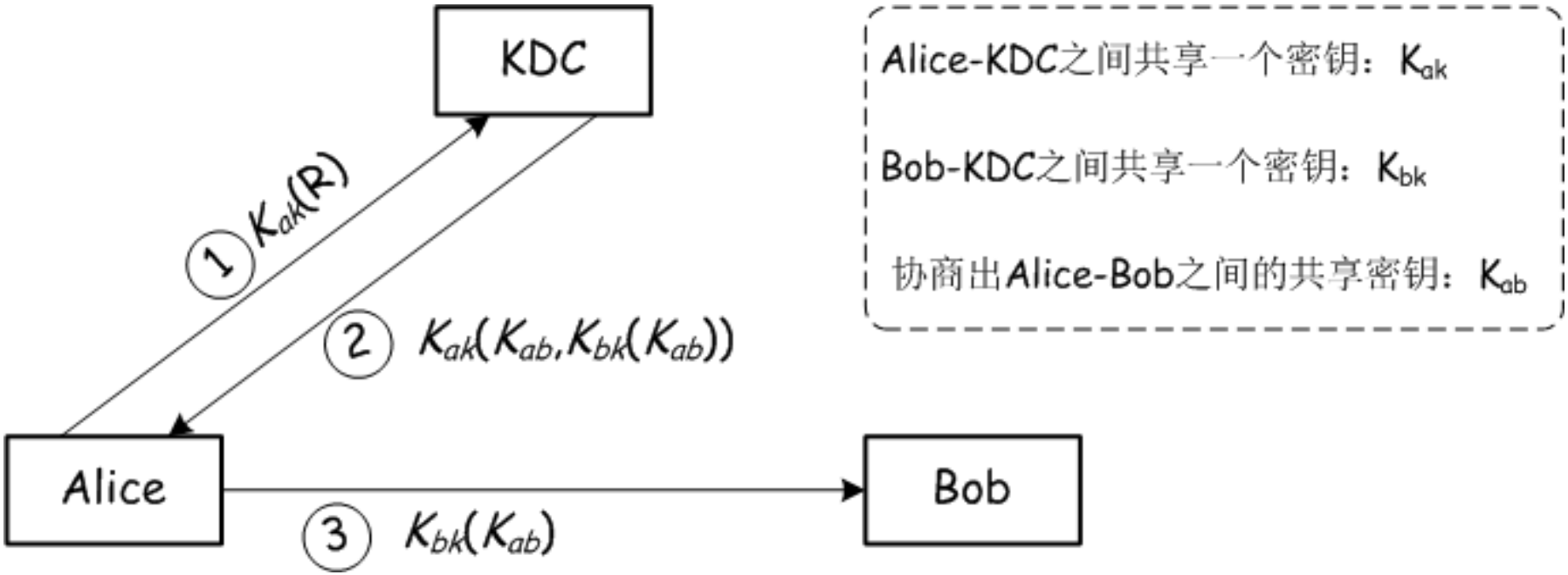
随机数：用途

- 生成密钥
  - 对称密码、消息认证码
- 生成初始化向量
  - 分组密码的CBC、CFB和OFB模式
- 生成密钥对
  - 公钥密码、数字签名
- 生成nonce
  - 用于防御重放攻击及分组密码的CTR模式
- 生成盐
  - 用于基于口令的密码（PBE）等

对称密码的密钥管理

- 基于可信第三方（KDC）
- 基于密钥协商算法
- 基于公钥密码

对称密钥管理：基于可信第三方(KDC)



1：当Alice要和Bob通信时，Alice向KDC发送一条请求消息，该消息使用Alice和KDC的共享密钥K_{ak}加密以便KDC认证Alice的身份。

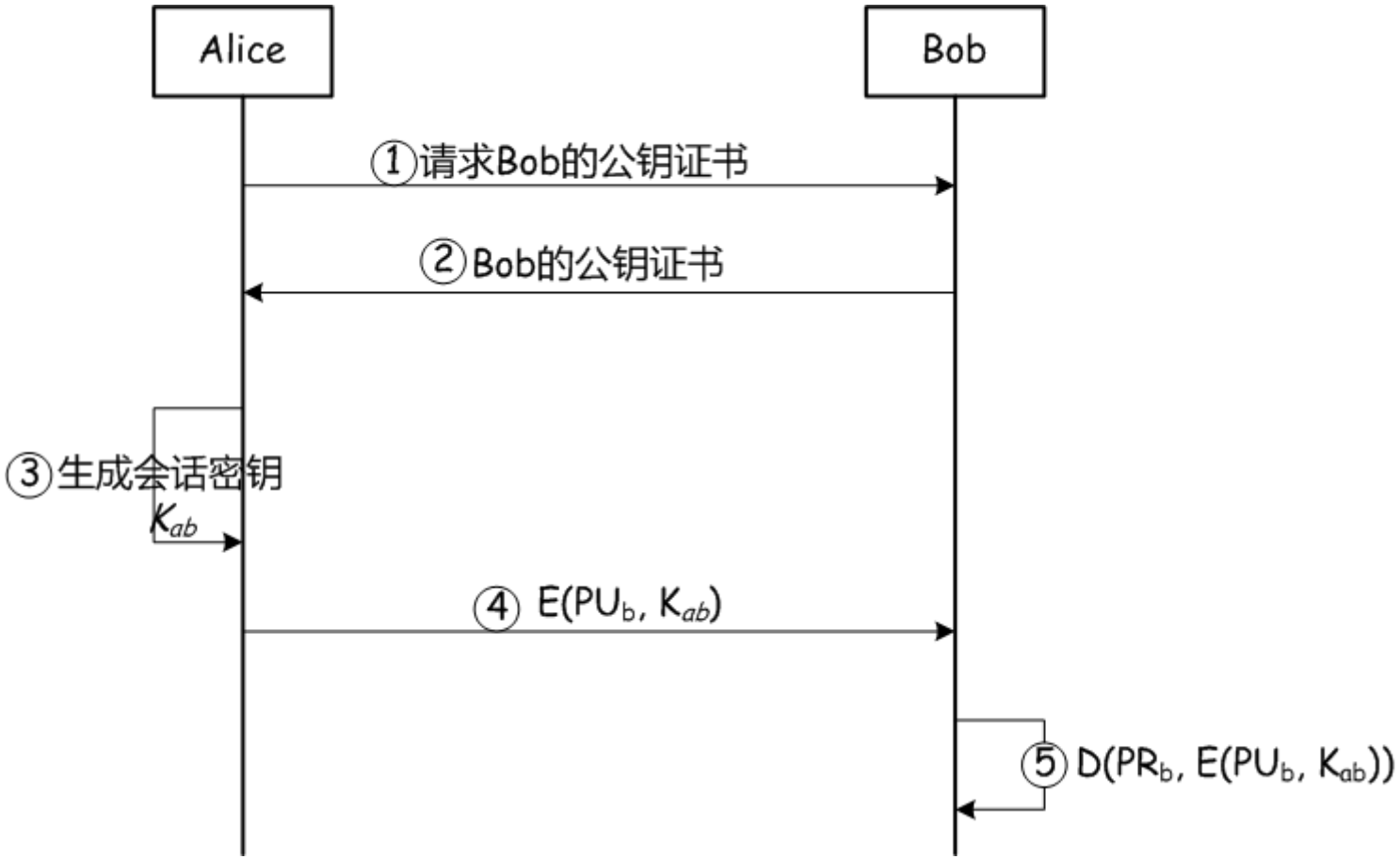
2：KDC收到请求后，生成Alice和Bob的共享密钥K_{ab}，并以一条票据（ticket）的形式返回给Alice.

3：Alice收到票据后，提取其中的K_{ab}，并把$K_{bk}(K_{ab})$发送给Bob

对称密钥管理：基于密钥协商算法

- 密钥协商的思想：通信双方交换生成密钥的素材，并各自利用这些素材在本地生成共享密钥。即使攻击者获取这些素材，也无法生成共享密钥。
- 密钥协商算法：
  - DH(Diffie-Hellman)
  - ECDH

对称密钥管理：基于公钥密码



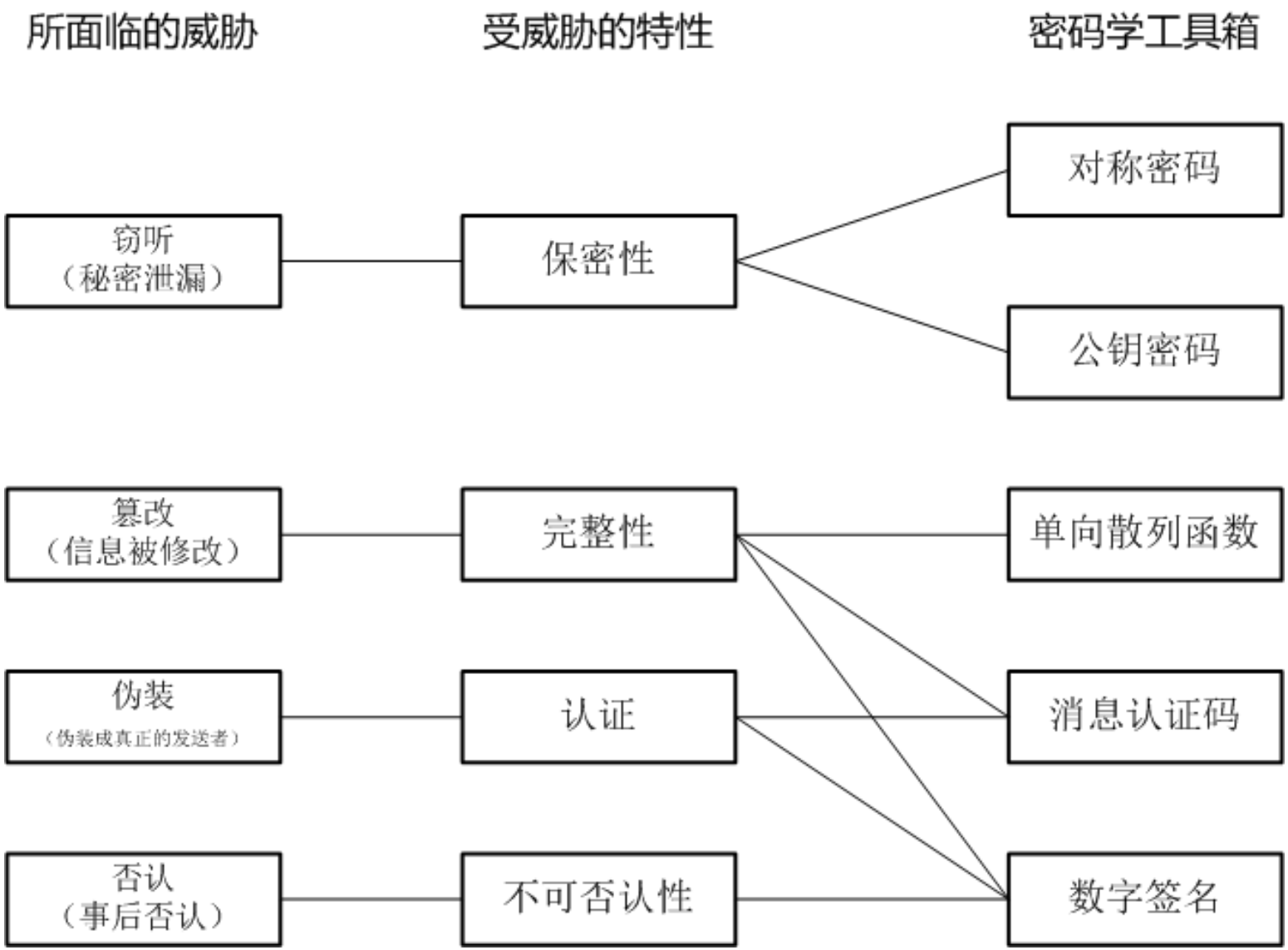
公钥密码密钥管理

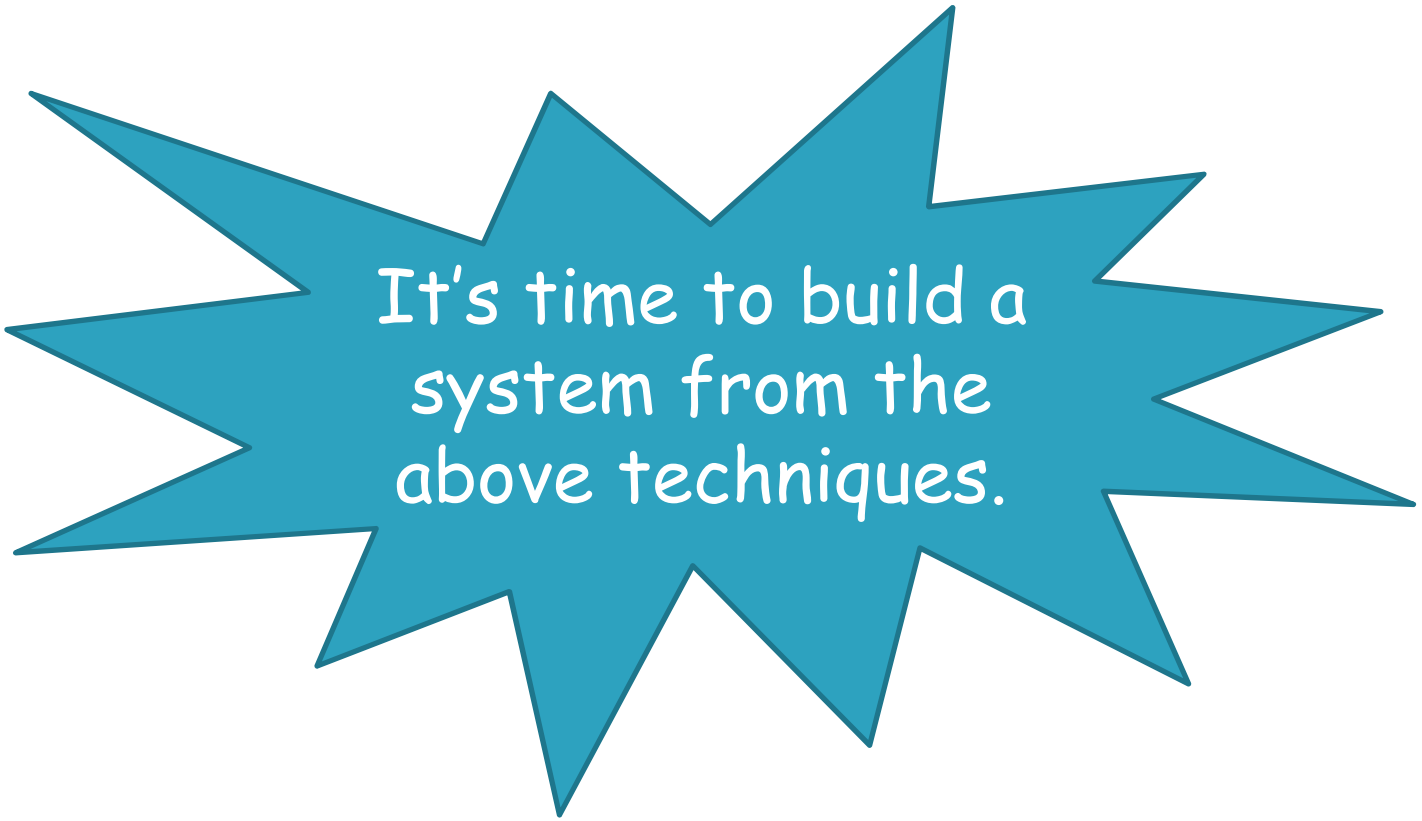
- 通过网络直接发送公钥
  - 中间人攻击
- 数字证书
  - 公钥
  - CA数字签名：保证了真实性和完整性
  - 版本
  - 序列号
  - 签名算法
  - ……

网络安全威胁 vs. 密码技术

- 网络安全需求
- TCP/IP协议栈及弱点
- 网络安全威胁
  - 被动攻击
  - 主动攻击
- 密码学工具

网络安全威胁 vs. 密码技术





简单的安全消息系统

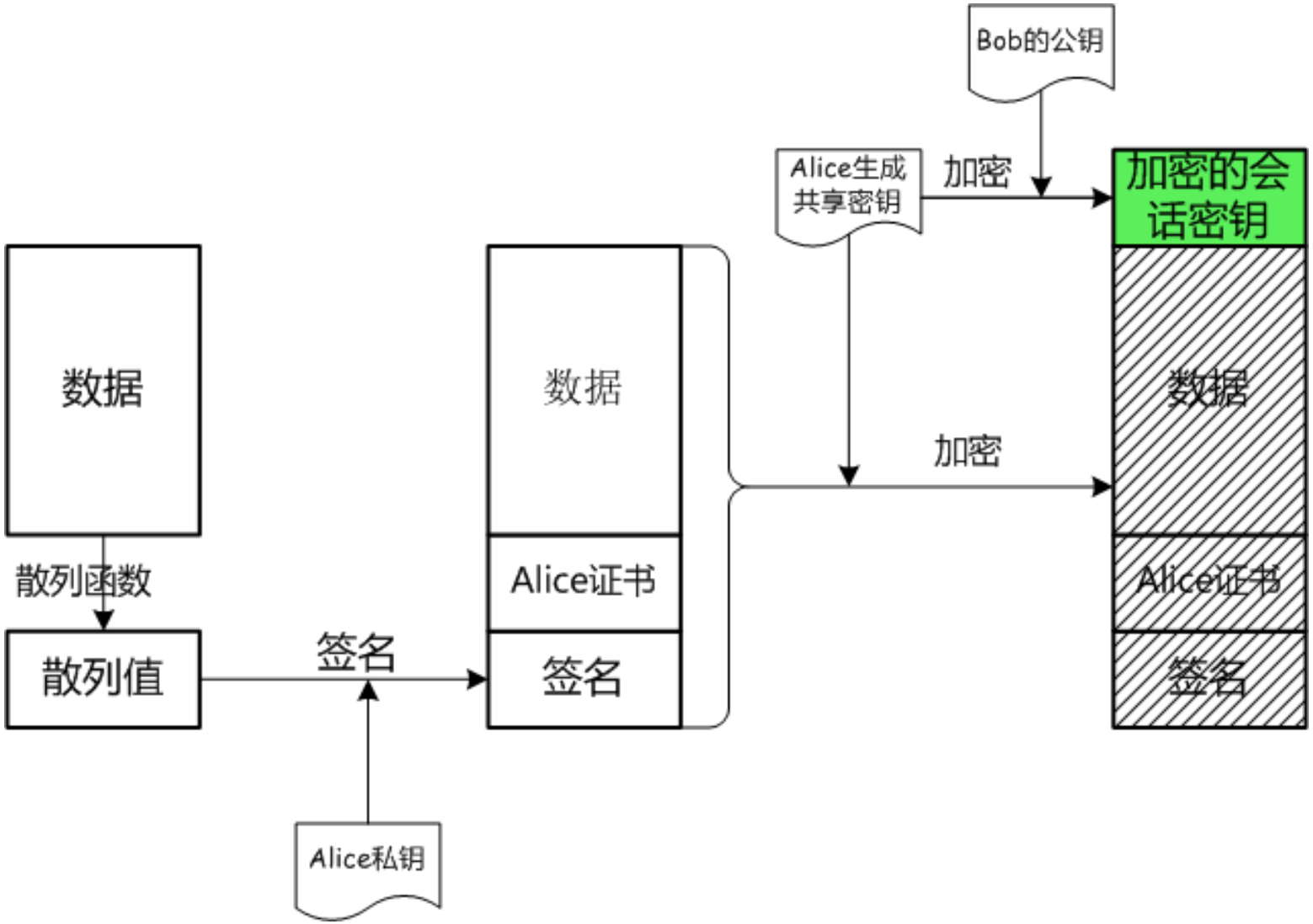
简单的安全消息系统

- Alice拥有一个**较大**的数据文件，Alice想和Bob通过网络安全地共享这个数据文件。
- 如何设计一个安全消息系统，能够用于发送者Alice和接收者Bob之间进行安全的数据通信?

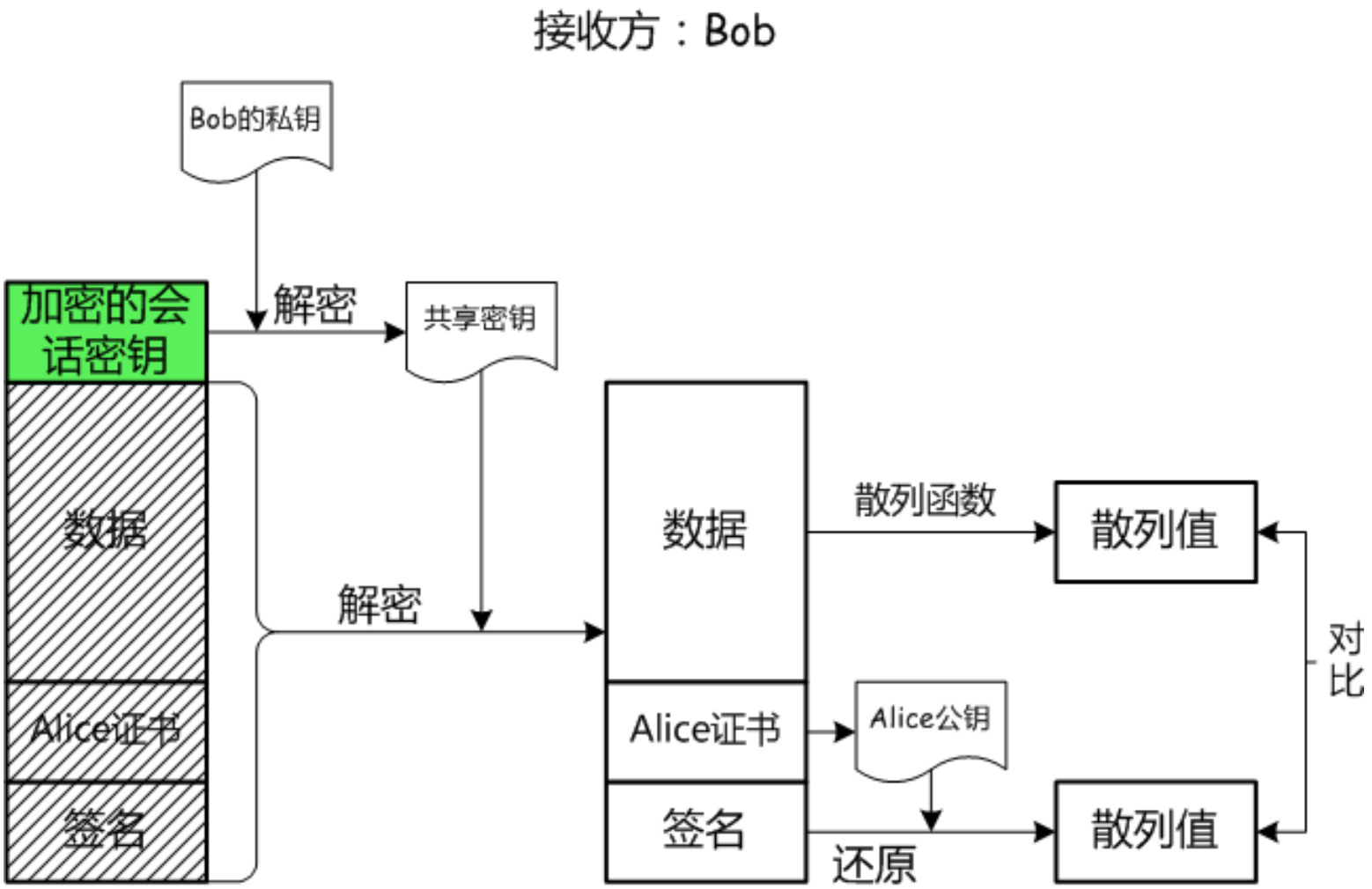
简单的安全消息系统

- ~~采用公钥密码?~~
  - 效率低，不适合加密较大的数据文件
- 公钥密码+对称密码
  - 公钥密码进行密钥分发
  - 对称密码进行数据加密

简单安全消息系统：发送方Alice



简单安全消息系统：接收方Bob



上述设计忽略了哪些问题？

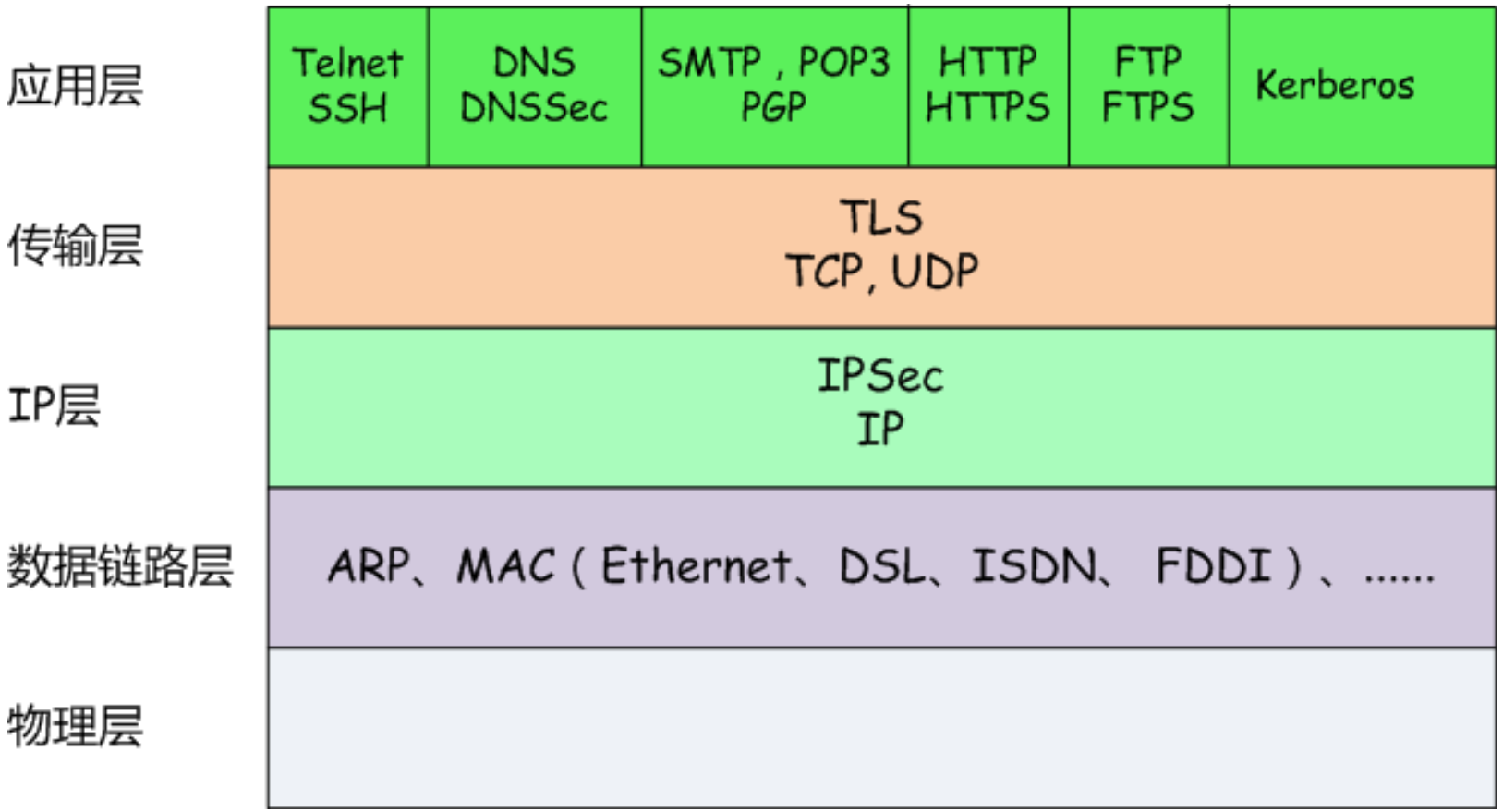
- 忽略了**身份认证**过程
  - Alice发送数据之前，已经认为接收方就是预期的Bob，但是并没有从技术上来保证。
- 忽略了**算法协商**
  - 通信双方使用的加解密算法、散列算法、签名算法必须一致，否则无法正确通信，但是通信双方事前无此协商过程。
- 忽略了**效率**问题
  - 每次传输都需要携带证书和会话密钥，对于大数据合适；但是对于小数据（如1B）则开销较大。

实际网络安全协议的设计思路

- 实际的网络安全协议通常把整个协议交互过程划分为**协商过程**和**数据通信**两个步骤，并针对两个步骤分别规定了相应的语法、语义和时序。
- 协商过程包括：
  - 身份认证
  - 算法协商，包括：加解密算法、散列算法、数字签名算法等
  - 会话密钥协商，通信双方就保护数据保密性的加密密钥达成共识。

网络安全协议概览

网络安全协议概览


应用层
Telnet
SSH
DNS
DNSSec
SMTP , POP3
PGP
HTTP
HTTPS
FTP
FTPS
Kerberos
传输层
TLS
TCP, UDP
IP层
IPSec
IP
数据链路层
ARP、MAC（Ethernet、DSL、ISDN、 FDDI）、.....
物理层

应用层：PGP

- Pretty Good Privacy
- Philip Zimmermann设计开发
- 保护邮件通信的隐私性
- 提供安全服务：
  - 保密性
  - 数字签名

传输层：SSL/TLS

- 由网景公司发起（Secure Socket Layer，SSL），用于解决浏览器和Web服务器之间通信的安全性
- IETF进行标准化（Transportation Layer Secure，TLS）
- 提供安全服务：
  - 身份认证
  - 保密性
  - 完整性

IP层：IPSec

- IPSec是IETF开发的一套认证、加密协议，用于解决IP-based网络所缺少的安全性。
- RFC2401和2411等，对IPSec进行了具体描述
- IPSec是IPv6协议的内置功能，是IPv4的补充功能

IP层：IPSec

- IPSec提供以下安全服务：
  - 完整性：确保接收到的流量没有被篡改过
  - 保密性：确保所传输的流量没有被非授权访问
  - 认证：特别是源认证，当目的主机接收到一个带特定地址的数据包，能够确保该数据包就是拥有这个特定源IP地址的主机生成。
  - 重放保护：确保通信双方交互的每个数据包都是不同的。

IP层：IPSec

- IPSec 主要通过两个协议来提供上述安全服务
  - Authentication Header (AH) protocol
  - Encapsulation Security Payload (ESP) protocol
- AH协议提供源认证和数据完整性，但是不提供保密性
- ESP协议提供认证、数据完整性和保密性

数据链路层：WPA/WPA2

- 无线通信
  - 广播信道
    - 访问控制?
    - 保密性?

- WPA/WPA2
  - 身份认证
  - 保密性

小结

- 网络安全的需求
- TCP/IP协议栈
- 网络安全威胁
- 密码学工具及应用示例
- 安全消息系统示例
- 网络安全协议概览

课后作业

- 通过在实验环境重现arpspoof攻击，理解TCP/IP协议栈存在的安全缺陷及攻防方法
- 回顾密码学原理，利用openssl进行数据加解密实践
- 查阅资料，理解Memcached DRDos攻击的原理