小码哥教育 SEEMYGO

HTTP协议的安全问题

- HTTP协议默认是采取明文传输的，因此会有很大的安全隐患
- 常见的提高安全性的方法是：对通信内容进行加密后，再进行传输

- 常见的加密方式有
- 不可逆
  - ✓ 单向散列函数：MD5、SHA等
- 可逆
  - ✓ 对称加密：DES、3DES、AES等
  - ✓ 非对称加密：RSA等
- 其它
  - ✓ 混合密码系统
  - ✓ 数字签名
  - ✓ 证书

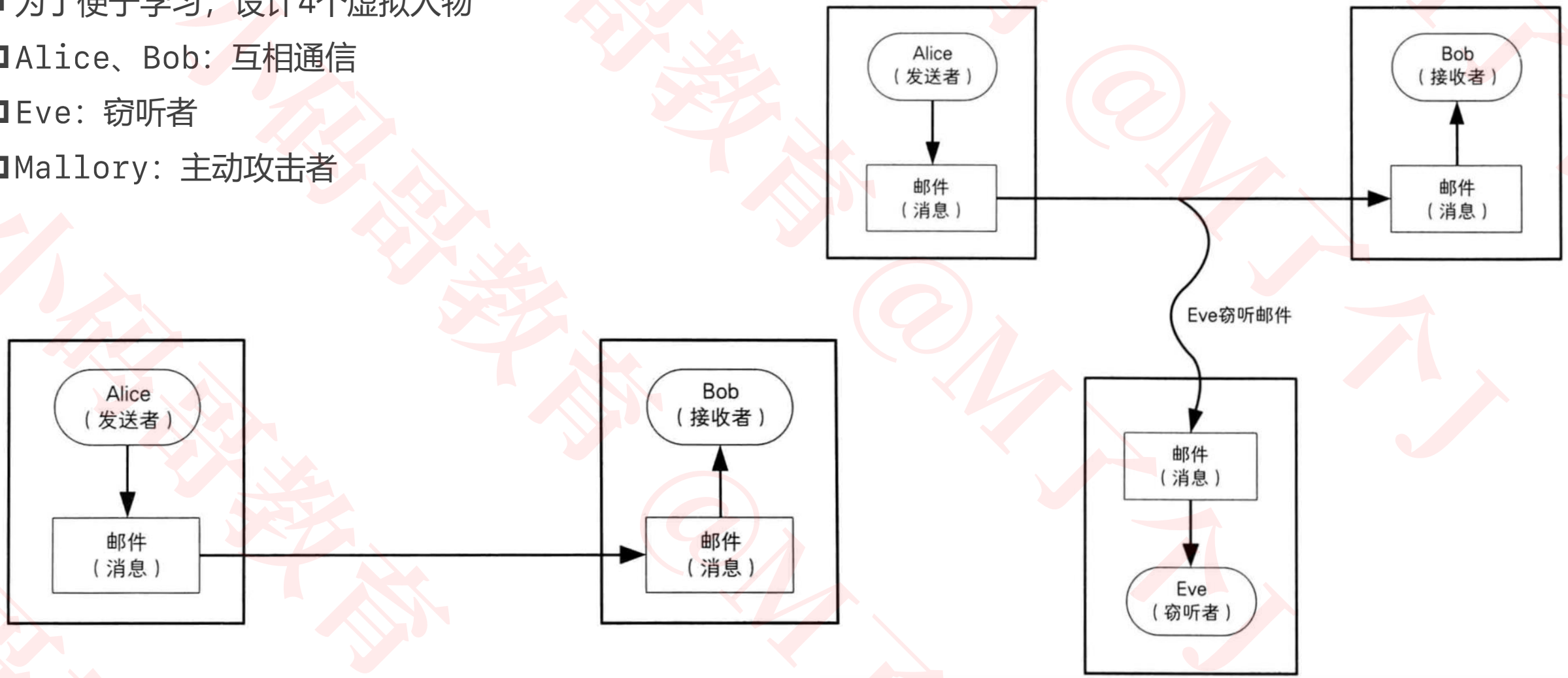
小码哥教育 SEEMYGO

常见英文

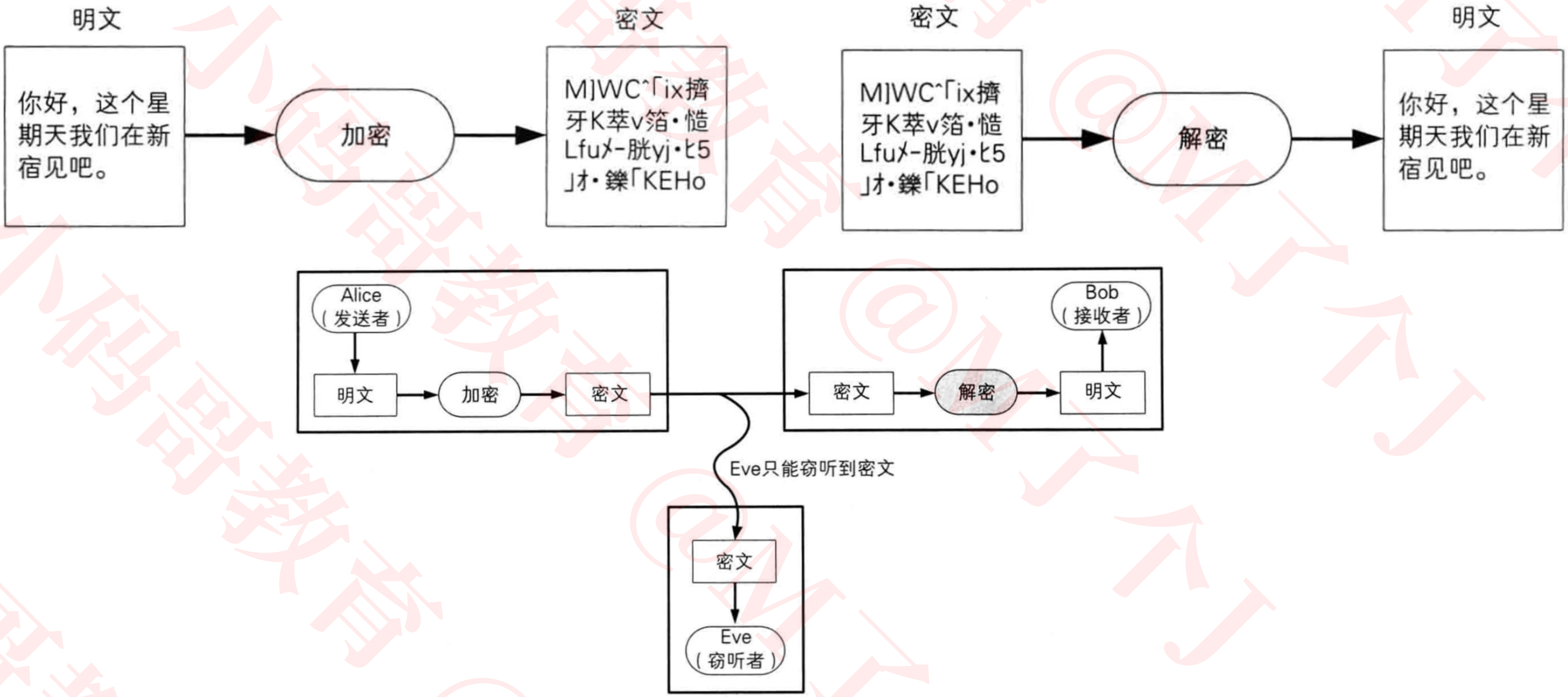
- encrypt：加密
- decrypt：解密
- plaintext：明文
- ciphertext：密文

学前须知

- 为了便于学习，设计4个虚拟人物
  - Alice、Bob：互相通信
  - Eve：窃听者
  - Mallory：主动攻击者



如何防止被窃听?


明文
你好，这个星期天我们在新宿见吧。
加密
密文
MJWC^「ix擠牙K萃v箔・慥Lfuメ-胱yj・
ㄝ5」オ・鑠「KEHo
密文
MJWC^「ix擠牙K萃v箔・慥Lfuメ-胱yj・ㄝ5」オ・鑠「KEHo
解密
明文
你好，这个星期天我们在新宿见吧。
Alice（发送者）
明文
加密
密文
密文
解密
明文
Bob（接收者）
Eve只能窃听到密文
密文
Eve（窃听者）