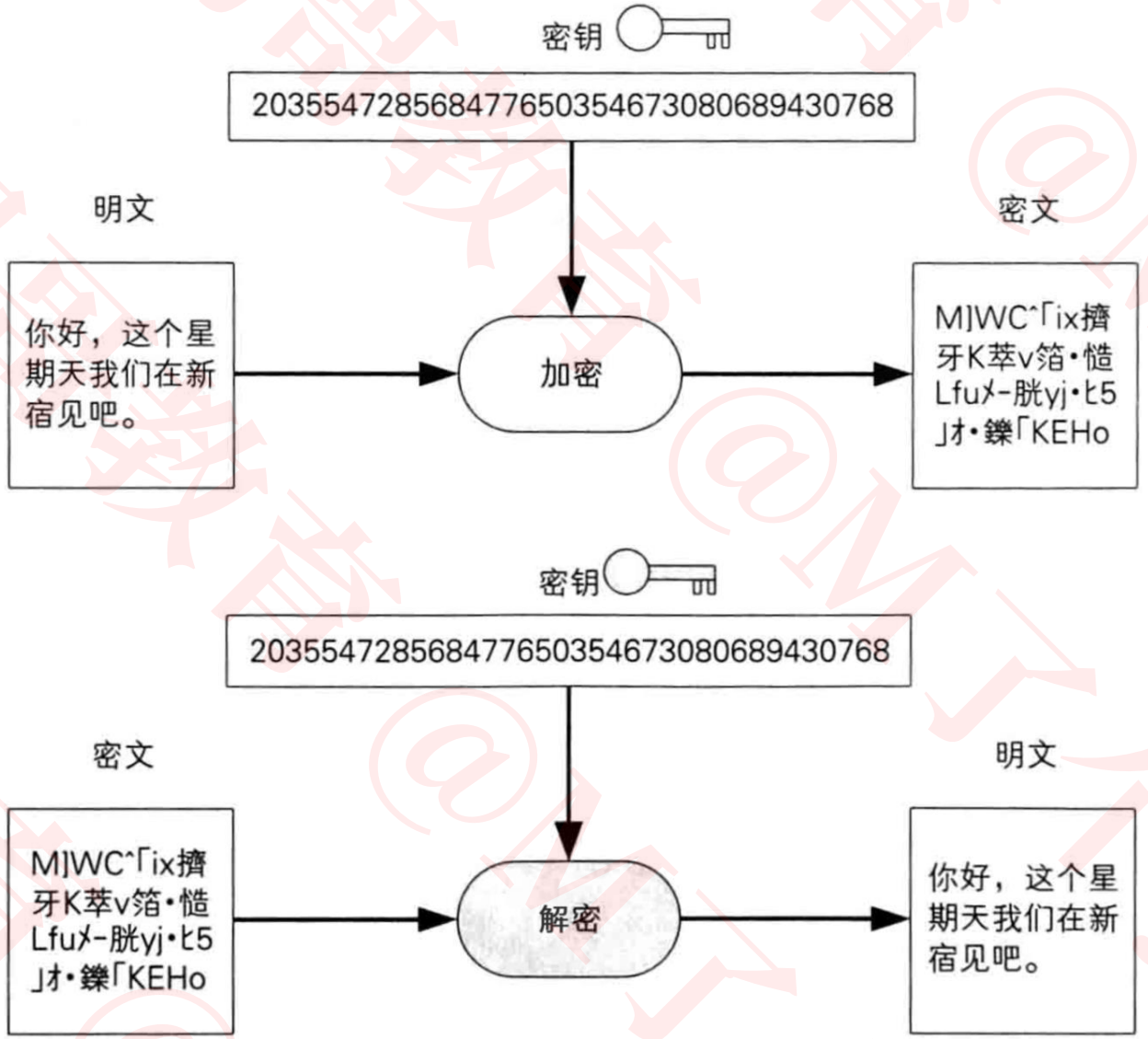
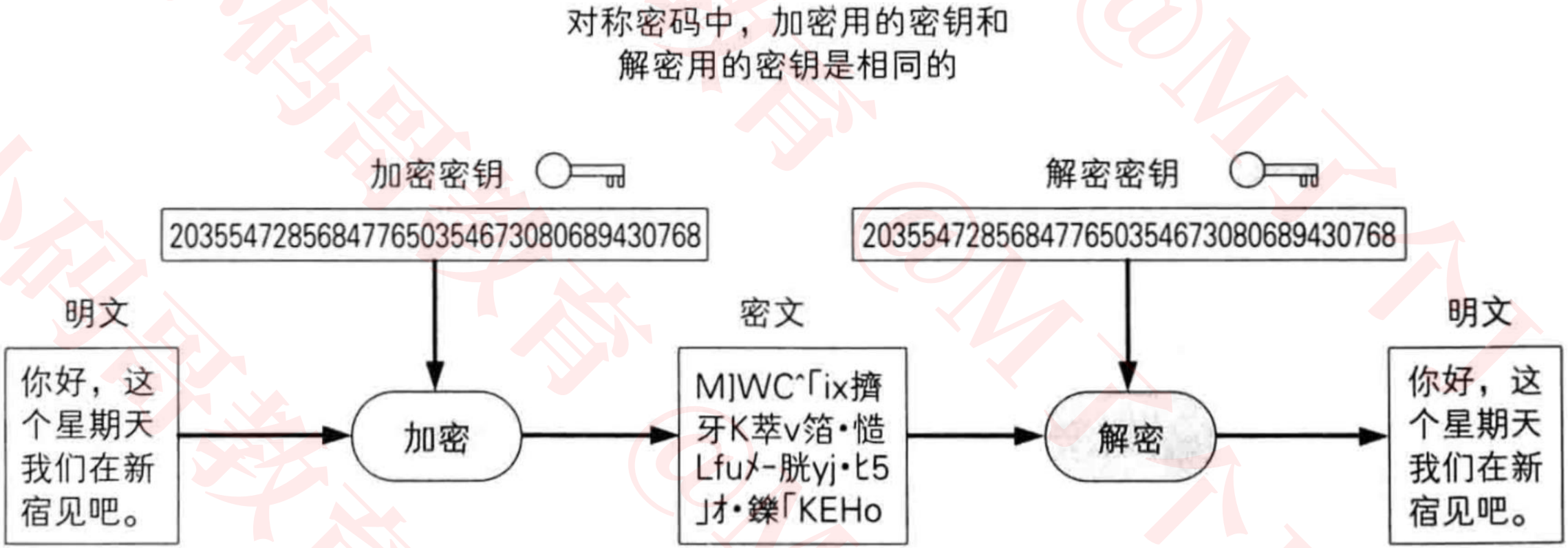
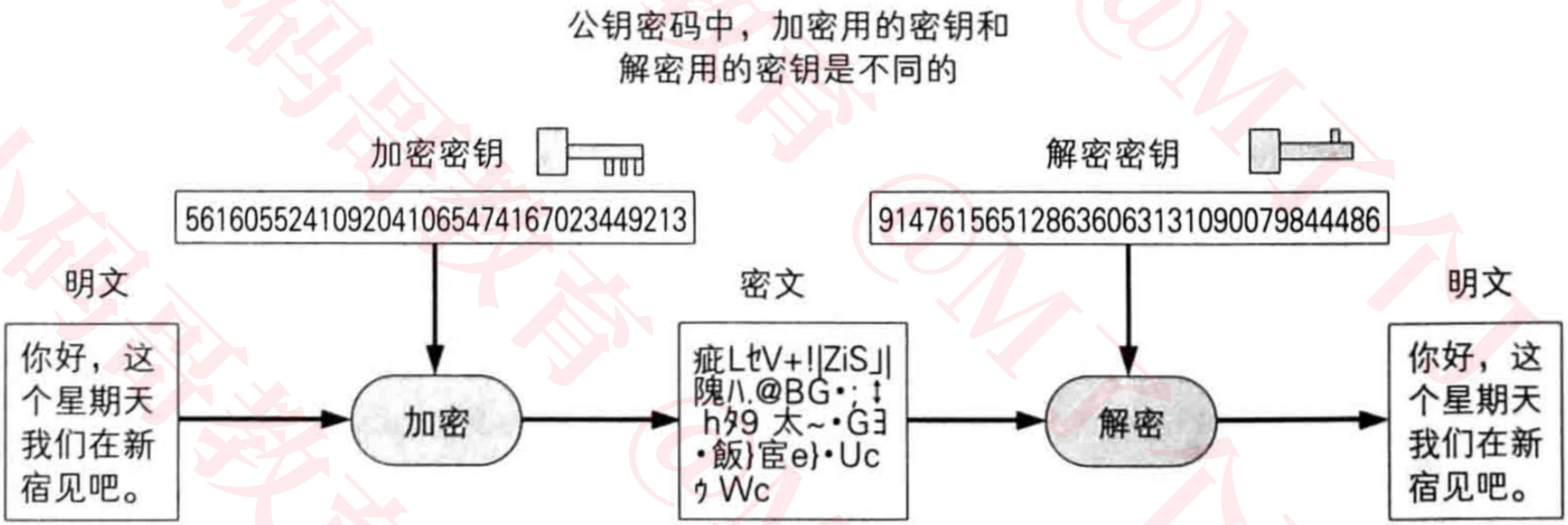
如何加密解密?


密钥
20355472856847765035467308068943076 8
明文
你好，这个星期天我们在新宿见吧。
加密
密文
M]WC^「ix擠牙K萃v箔•慣Lfu乂-胱yj•匕5」才•鑾「KEHo
密钥
20355472856847765035467308068943076 8
密文
M]WC^「ix擠牙K萃v箔•慣Lfu乂-胱yj•匕5」才•鑾「KEHo
解密
明文
你好，这个星期天我们在新宿见吧。

对称加密（对称密码）


对称密码中，加密用的密钥和
解密用的密钥是相同的
加密密钥
20355472856847765035467308068943076 8
解密密钥
20355472856847765035467308068943076 8
明文
你好，这个星期天我们在新宿见吧。
加密
密文
M]WC^「ix擠牙K萃v箔·慥Lfuメ-胱yj·ヒ5」才·鑠「KEHo
解密
明文
你好，这个星期天我们在新宿见吧。

非对称加密（公钥密码）

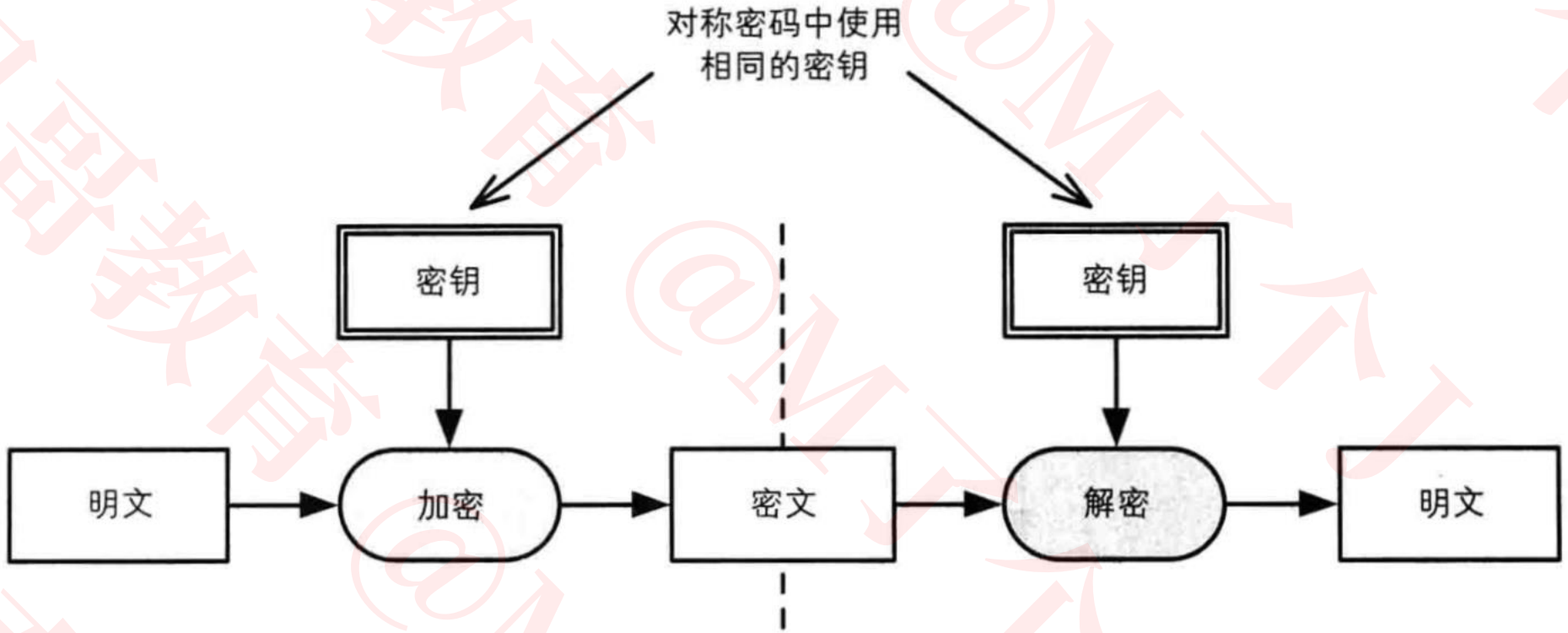


公钥密码中，加密用的密钥和
解密用的密钥是不同的
加密密钥
5616055241092041065474167023449213
解密密钥
9147615651286360631310900798444486
明文
你好，这
个星期天
我们在新
宿见吧。
加密
密文
解密
明文
你好，这
个星期天
我们在新
宿见吧。

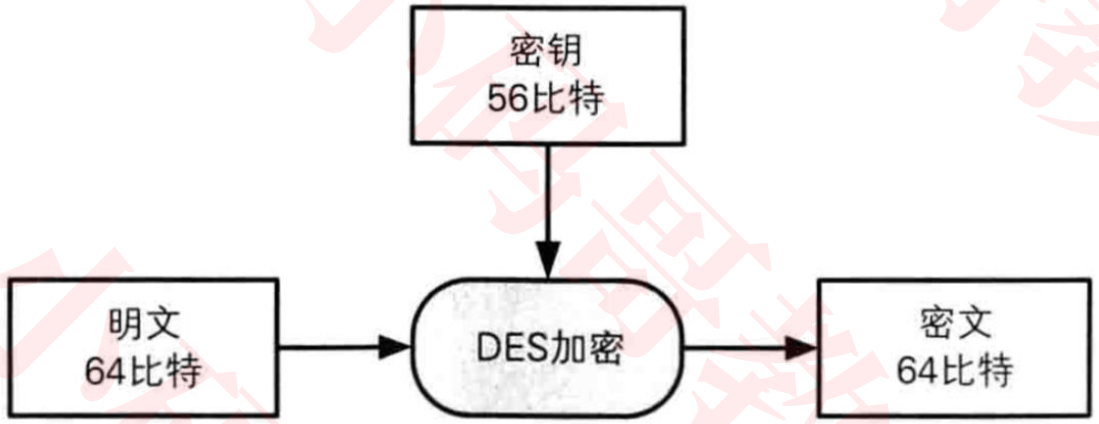
对称加密（Symmetric Cryptography）

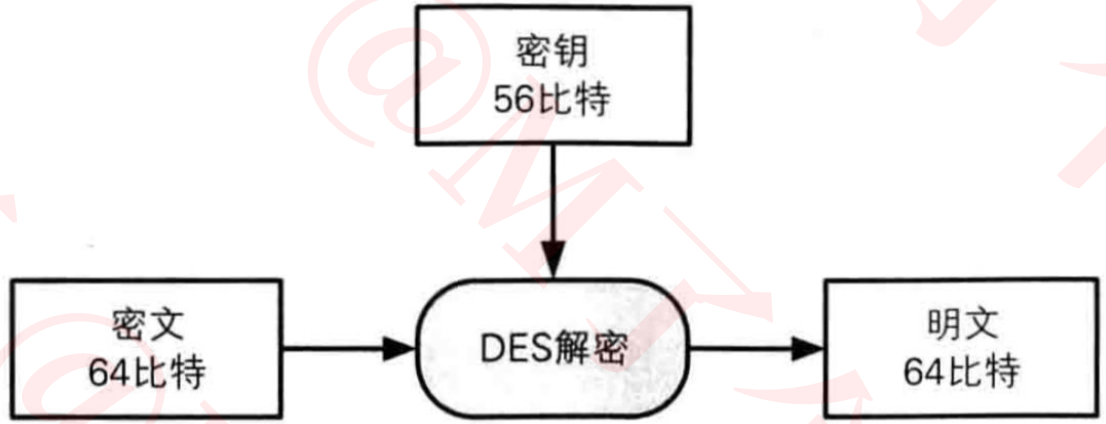
- 在**对称加密**中，加密、解密时使用的是同一个密钥

- 常见的**对称加密**算法有
  - DES
  - 3DES
  - AES



DES (Data Encryption Standard)





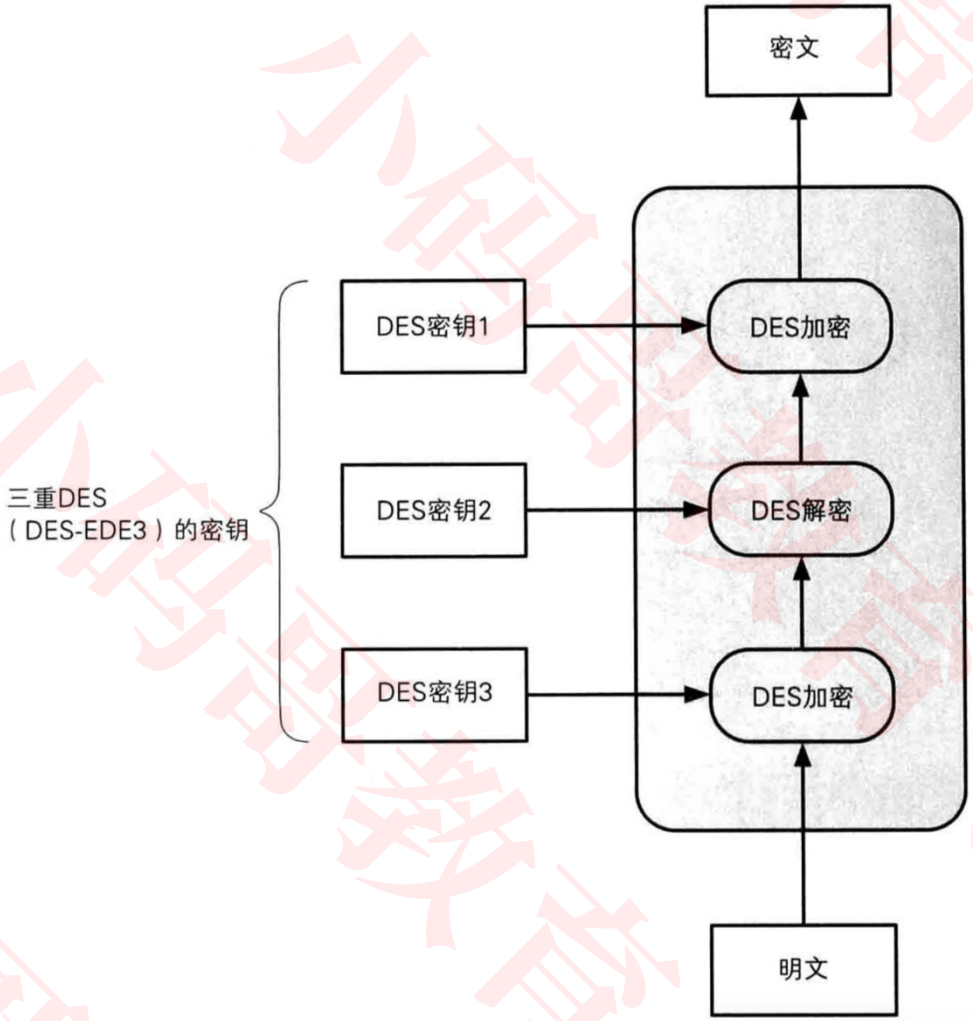
- DES是一种将64bit明文加密成64bit密文的**对称加密**算法，密钥长度是56bit
- 规格上来说，密钥长度是64bit，但每隔7bit会设置一个用于错误检查的bit，因此密钥长度实质上是56bit
- 由于DES每次只能加密64bit的数据，遇到比较大的数据，需要对DES加密进行迭代（反复）
- 目前已经可以在短时间内被破解，所以不建议使用

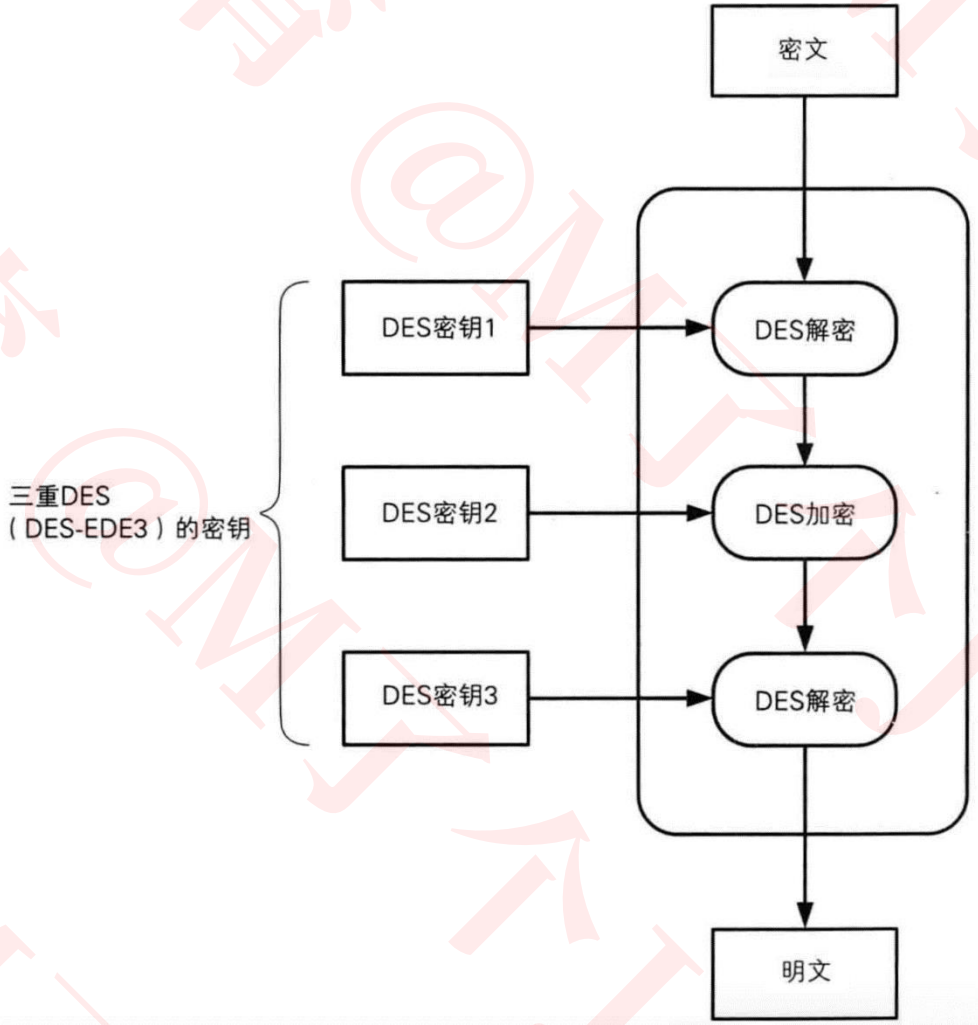
3DES (Triple Data Encryption Algorithm)

- 3DES，将DES重复3次所得到的一种密码算法，也叫做3重DES
  - 三重DES并不是进行三次DES加密（加密 → 加密 → 加密）
  - 而是加密（Encryption） → 解密（Decryption） → 加密（Encryption）的过程

- 目前还被一些银行等机构使用，但处理速度不高，安全性逐渐暴露出问题

3DES

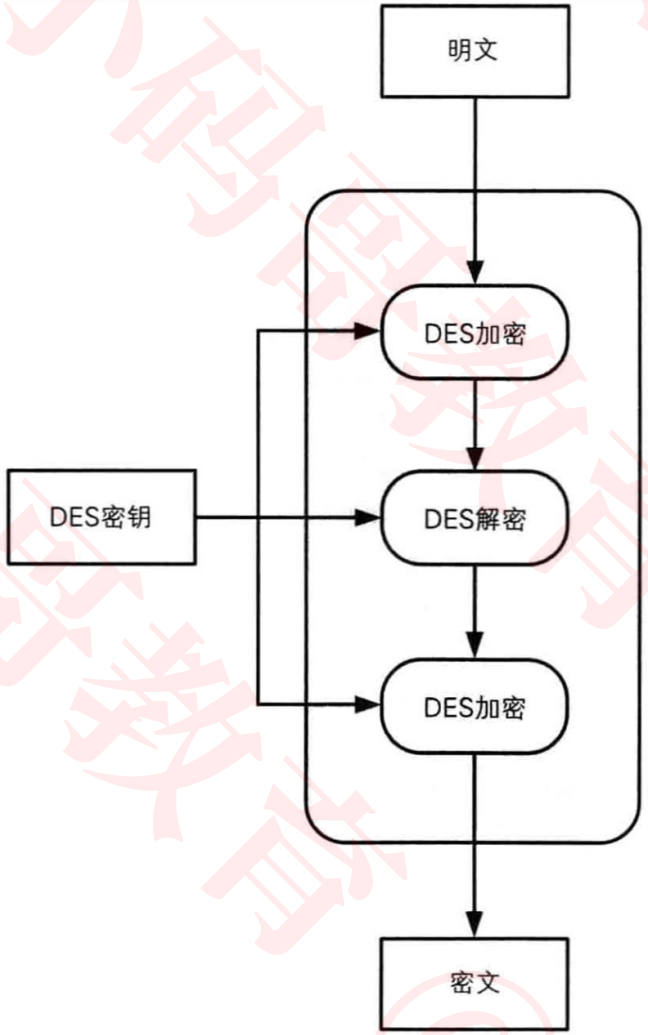


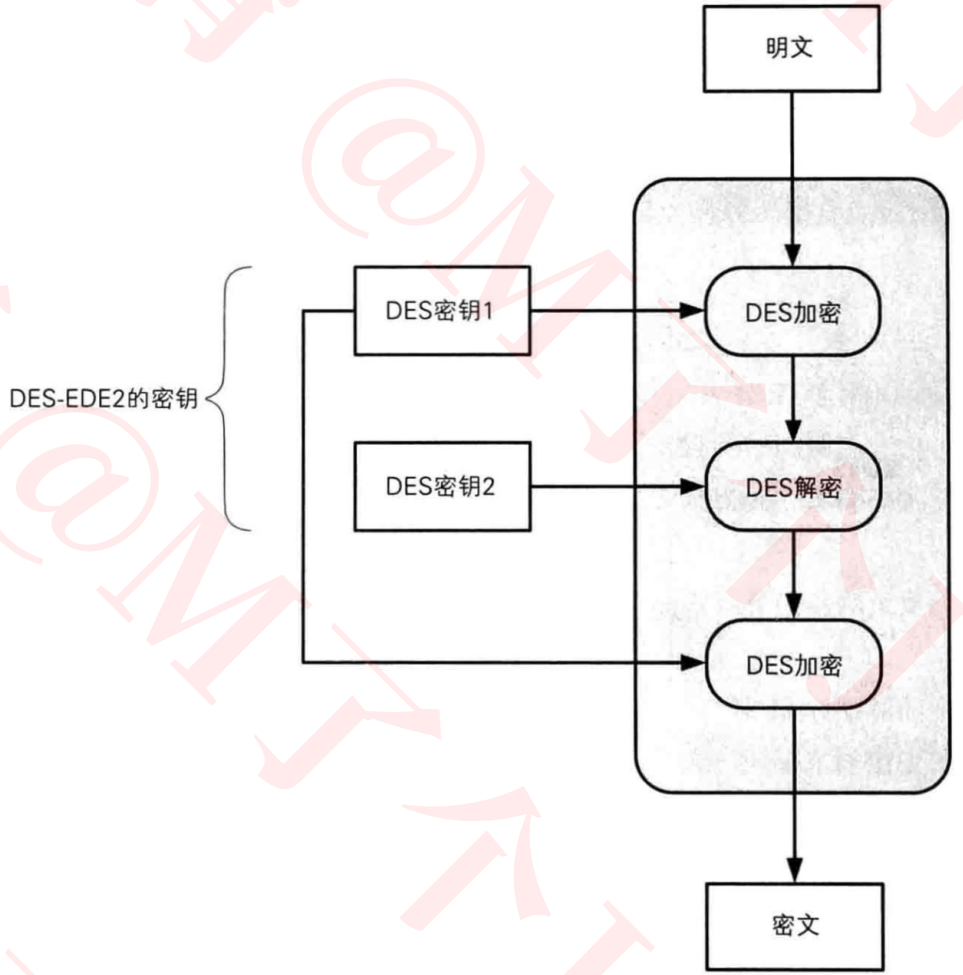


- 3个密钥都是不同的，也称为DES-EDE3

3DES

- 如果所有密钥都使用同一个，则结果与普通的DES是等价的





- 如果密钥1、密钥3相同，密钥2不同，称为DES-EDE2

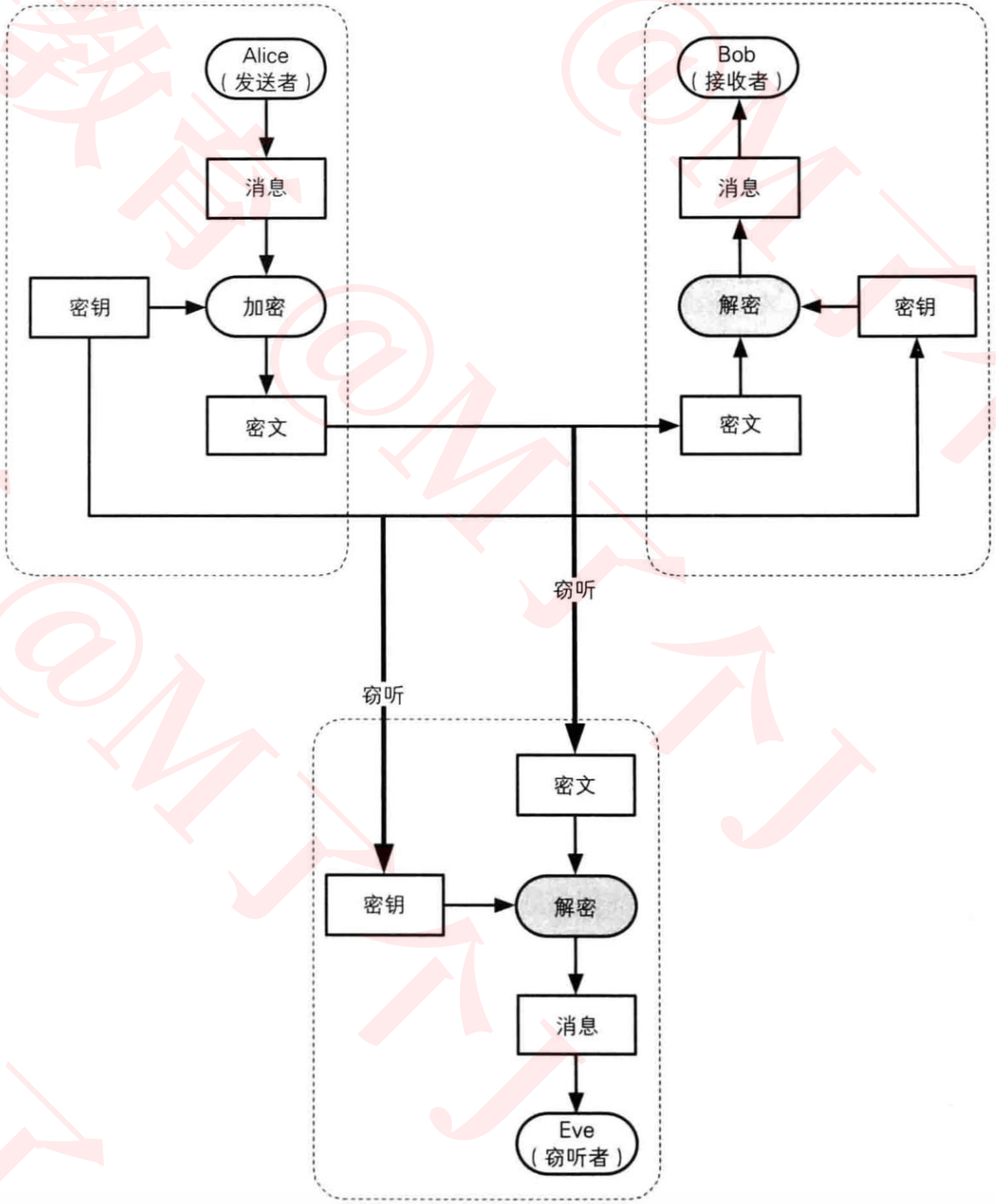
AES (Advanced Encryption Standard)

- 取代DES成为新标准的一种**对称加密**算法，又称Rijndael加密法
- AES的密钥长度有128、192、256bit三种
- 目前AES，已经逐步取代DES、3DES，成为首选的**对称加密**算法
- 一般来说，我们也不应该去使用任何自制的密码算法，而是应该使用AES
  - 它经过了全世界密码学家所进行的高品质验证工作

密钥配送问题

- 在使用**对称加密**时，一定会遇到密钥配送问题

- 如果Alice将使用**对称加密**过的消息发给了Bob
  - 只有将密钥发送给Bob，Bob才能完成解密
  - 在发送密钥过程中
    - ✓ 可能会被Eve窃取密钥
    - ✓ 最后Eve也能完成解密



如何解决密钥配送问题

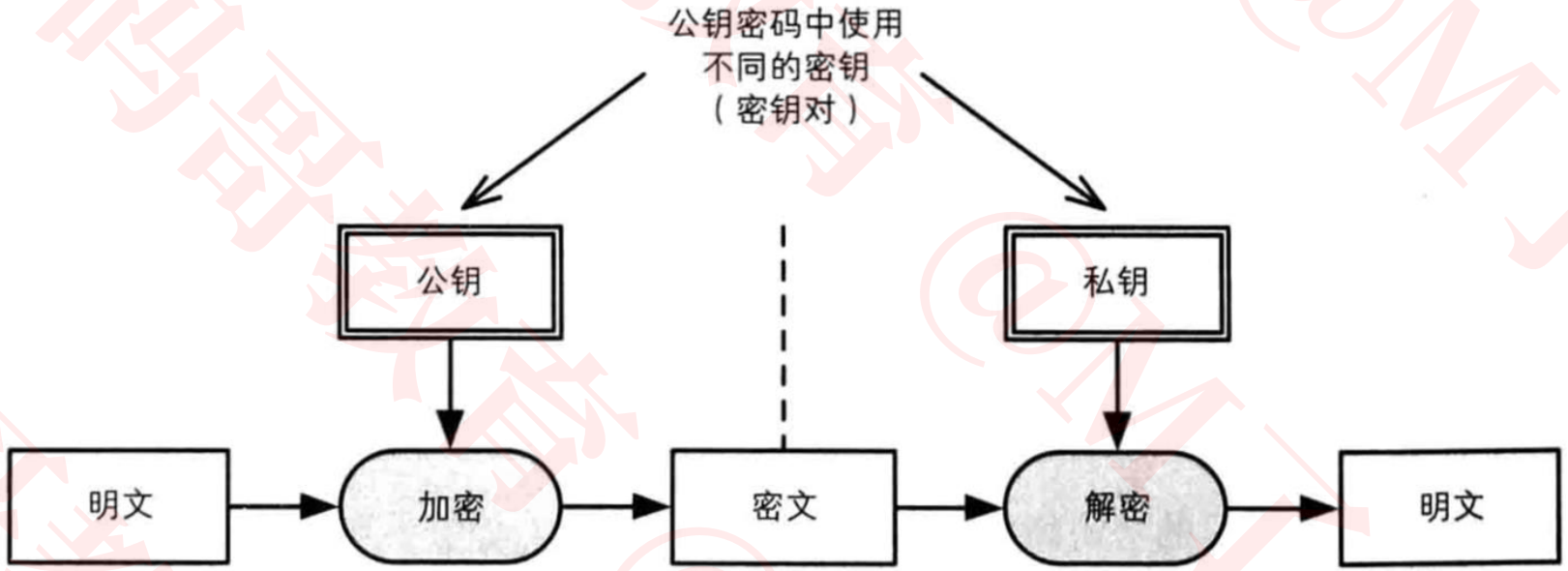
- 有以下几种解决密钥配送的方法
  - 事先共享密钥（比如私下共享）
  - 密钥分配中心（Key Distribution Center，简称KDC）
  - Diffie-Hellman密钥交换
  - 非对称加密

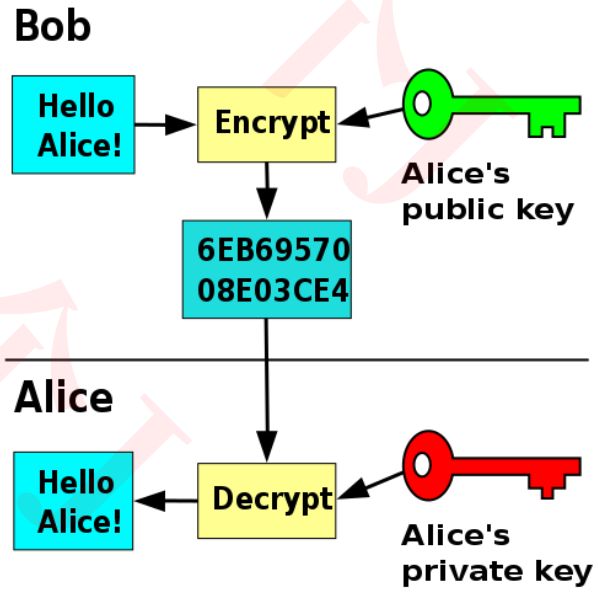
非对称加密（Asymmetric Cryptography）

- 在**非对称加密**中，密钥分为加密密钥、解密密钥2种，它们并不是同一个密钥

- 加密密钥：一般是公开的，因此该密钥称为**公钥**（public key）
  - 因此，**非对称加密**也被称为公钥密码（Public-key Cryptography）

- 解密密钥：由消息接收者自己保管的，不能公开，因此也称为**私钥**（private key）



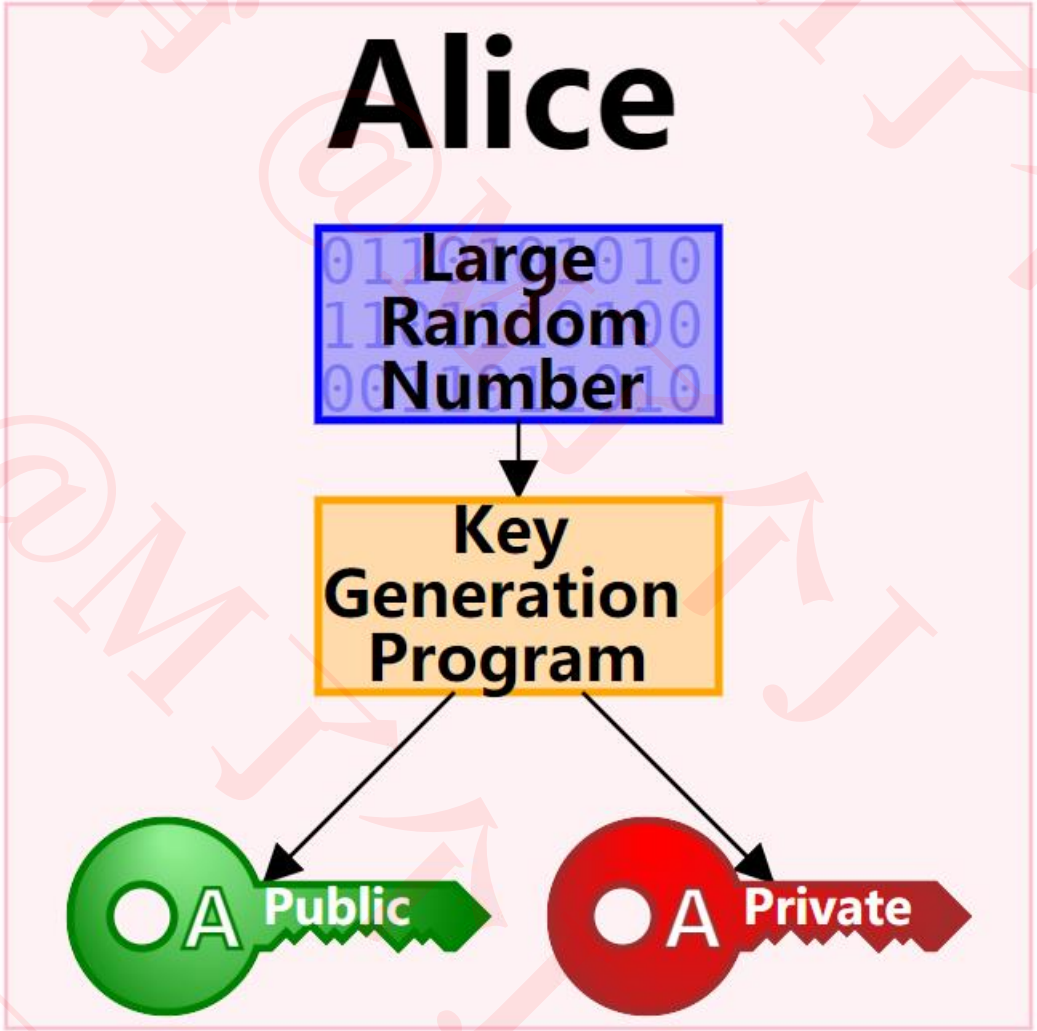


公钥、私钥

- 公钥和私钥是一一对应的，不能单独生成
- 一对公钥和私钥统称为密钥对（key pair）

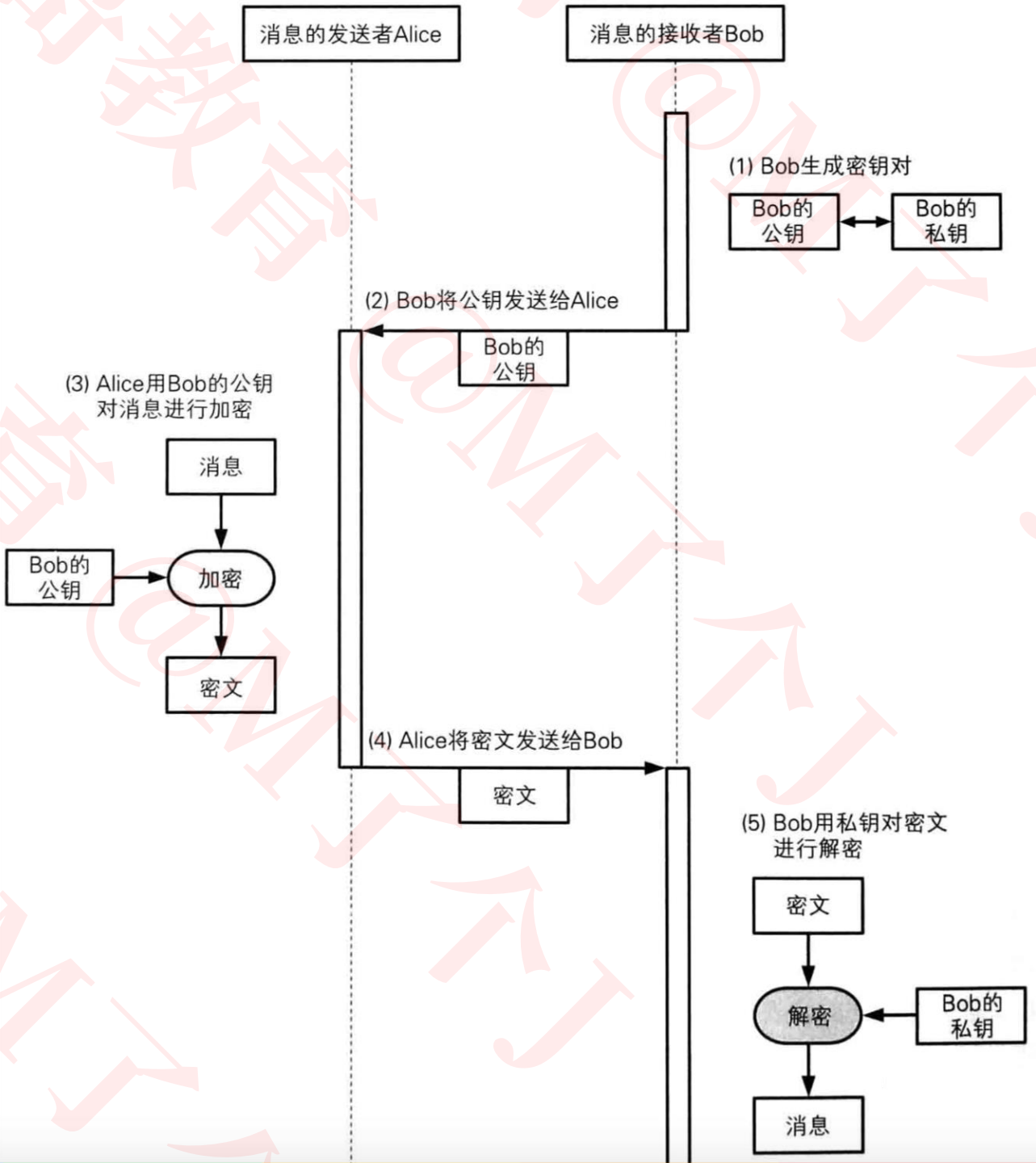
- 由公钥加密的密文，必须使用与该公钥对应的私钥才能解密

- 由私钥加密的密文，必须使用与该私钥对应的公钥才能解密



解决密钥配送问题

- 由消息的接收者，生成一对公钥、私钥
- 将公钥发给消息的发送者
- 消息的发送者使用公钥加密消息
- **非对称加密**的加密解密速度比**对称加密**要慢



小码哥教育 SEEMYGO

RSA

- 目前使用最广泛的**非对称加密**算法是RSA
- RSA的名字，由它的3位开发者，即Ron Rivest、Adi Shamir、Leonard Adleman的姓氏首字母组成