混合密码系统（Hybrid Cryptosystem）

- **对称加密**的缺点
  - 不能很好地解决密钥配送问题（密钥会被窃听）

- **非对称加密**的缺点
  - 加密解密速度比较慢

- 混合密码系统：是将**对称加密**和**非对称加密**的优势相结合的方法
  - 解决了**非对称加密**速度慢的问题
  - 并通过**非对称加密**解决了**对称加密**的密钥配送问题

- 网络上的密码通信所用的SSL/TLS都运用了混合密码系统

混合密码 – 加密

- 会话密钥（session key）
  - 为本次通信随机生成的临时密钥
  - 作为**对称加密**的密钥，用于加密消息，提高速度

- 加密步骤（发送消息）

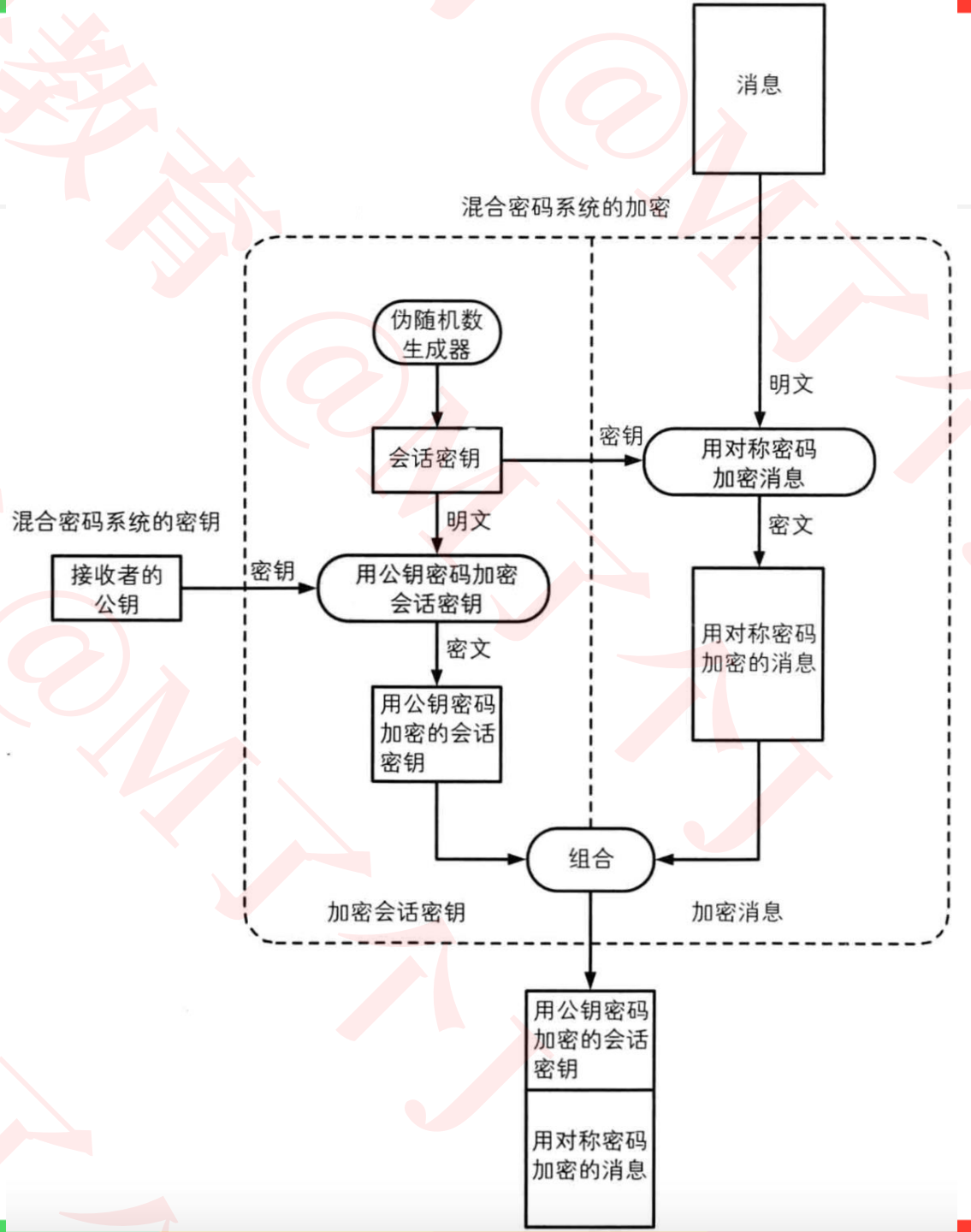
① 首先，消息发送者要拥有消息接收者的公钥

② 生成会话密钥，作为**对称加密**的密钥，加密消息

③ 用消息接收者的公钥，加密会话密钥

④ 将前2步生成的加密结果，一并发给消息接收者

- 发送出去的内容包括
  - 用会话密钥加密的消息（加密方法：**对称加密**）
  - 用公钥加密的会话密钥（加密方法：**非对称加密**）

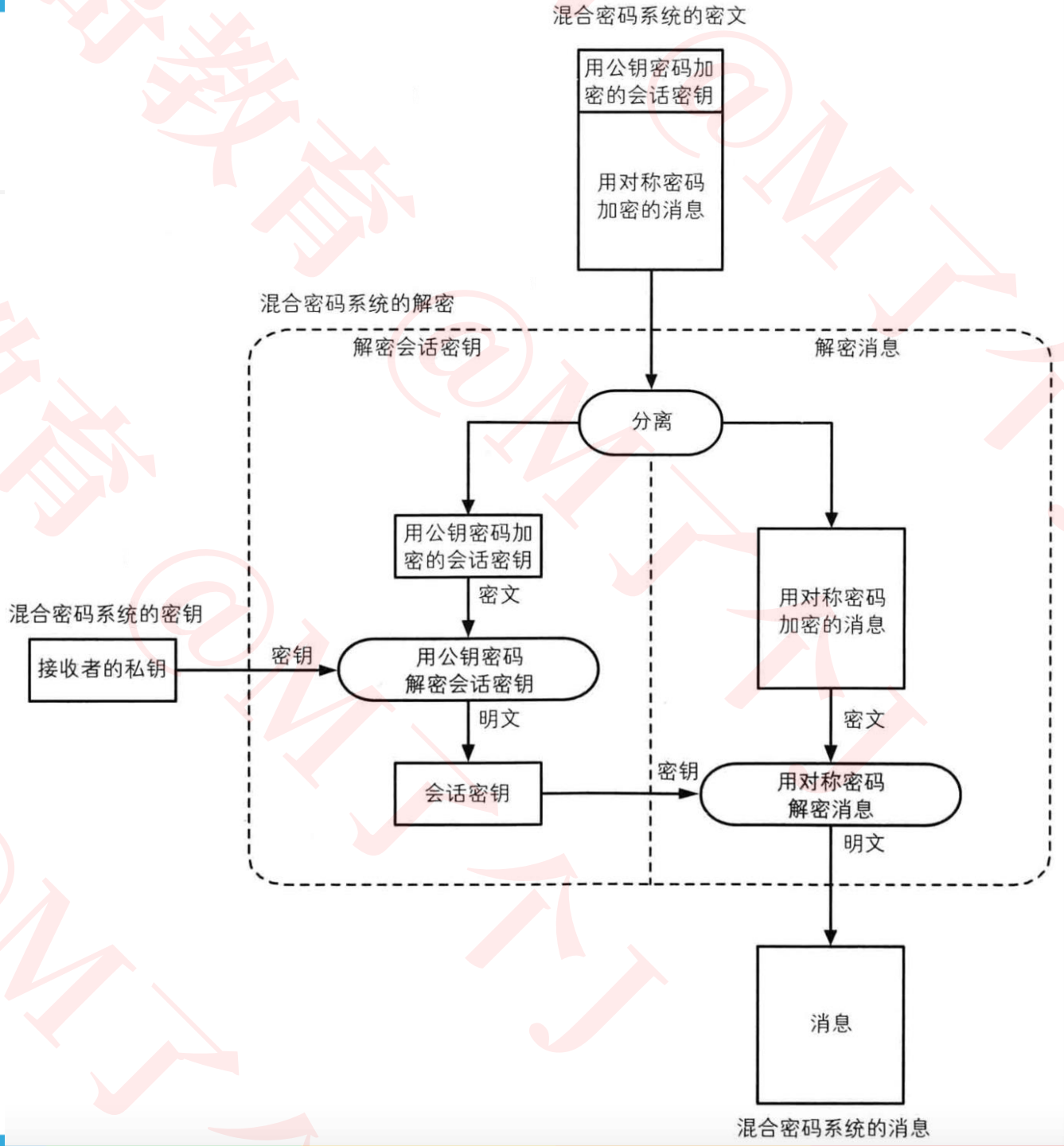


混合密码 – 解密

■ 解密步骤（收到消息）

① 消息接收者用自己的私钥解密出会话密钥

② 再用第①步解密出来的会话密钥，解密消息



混合密码 – 加密解密流程

■ Alice >>>>>> Bob

□发送过程（加密过程）

① Bob先生成一对公钥、私钥

② Bob把公钥共享给Alice

③ Alice随机生成一个会话密钥（临时密钥）

④ Alice用会话密钥加密需要发送的消息（使用的是**对称加密**）

⑤ Alice用Bob的公钥加密会话密钥（使用的是**非对称加密**）

⑥ Alice把第④、⑤步的加密结果，一并发送给Bob

□接收过程（解密过程）

① Bob利用自己的私钥解密会话密钥（使用的是**非对称加密**算法进行**解密**）

② Bob利用会话密钥解密发送过来的消息（使用的是**对称加密**算法进行解密）