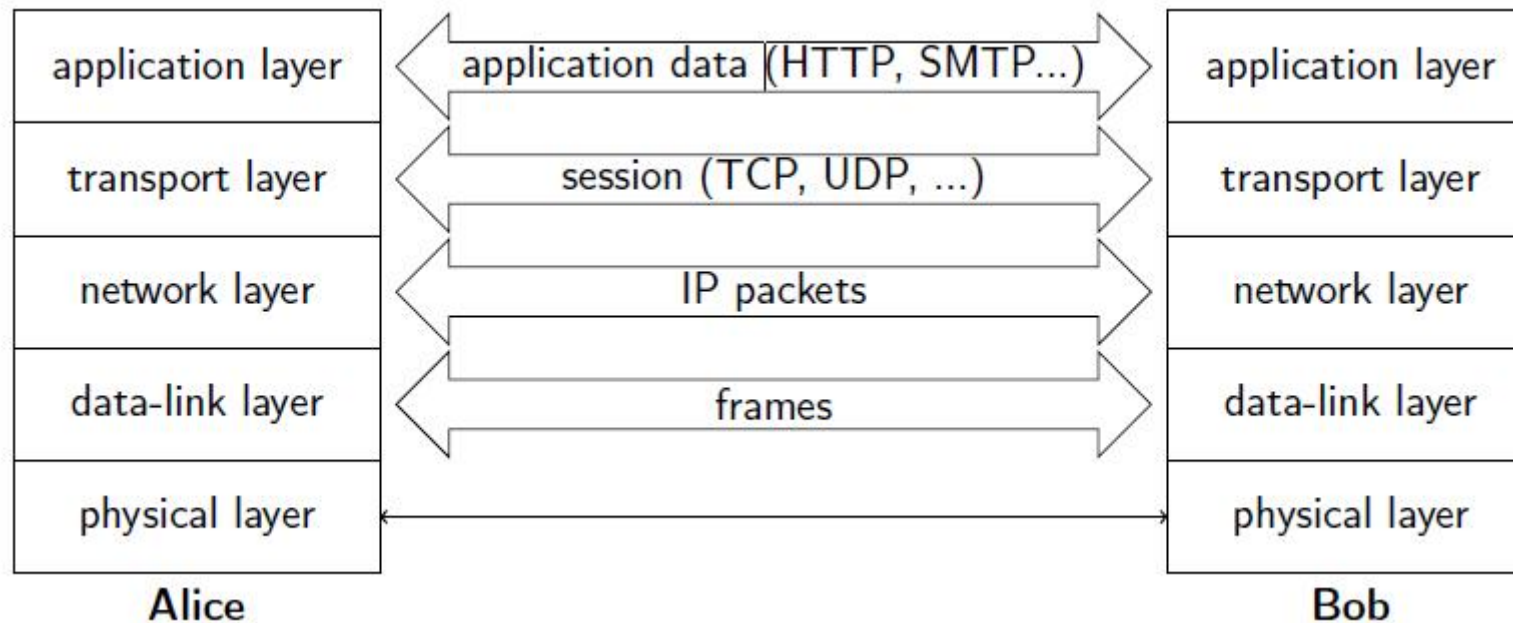


第2章 PGP



- application layer security (SSH, S-MIME, PGP,)
- transport layer security (TLS/SSL,)
- network layer security (IPsec,)
- data-link layer security (WEP, WPA, WPA2,)

内容提要

- PGP概述
- PGP加密与解密
- PGP生成和验证数字签名
- PGP加密+数字签名——解密+签名验证
- PGP信任网 (web of trust)
- PGP实例: GPG4Win

PGP概述

□ Philip Zimmermann设计

- ◆ 目前在瑞士运营公司Silent Cycle, 提供移动/桌面加密通信软件及服务, 目的是保护用户隐私。

□ OpenPGP→RFC4880



PGP概述：安全属性

- 保密性

 - ◆ 对称加密

- 完整性

 - ◆ 对消息摘要进行数字签名

- 身份认证

 - ◆ 数字签名

Building blocks of PGP

- 加解密
- 数字签名
- 压缩
- 电子邮件兼容性

PGP: 压缩

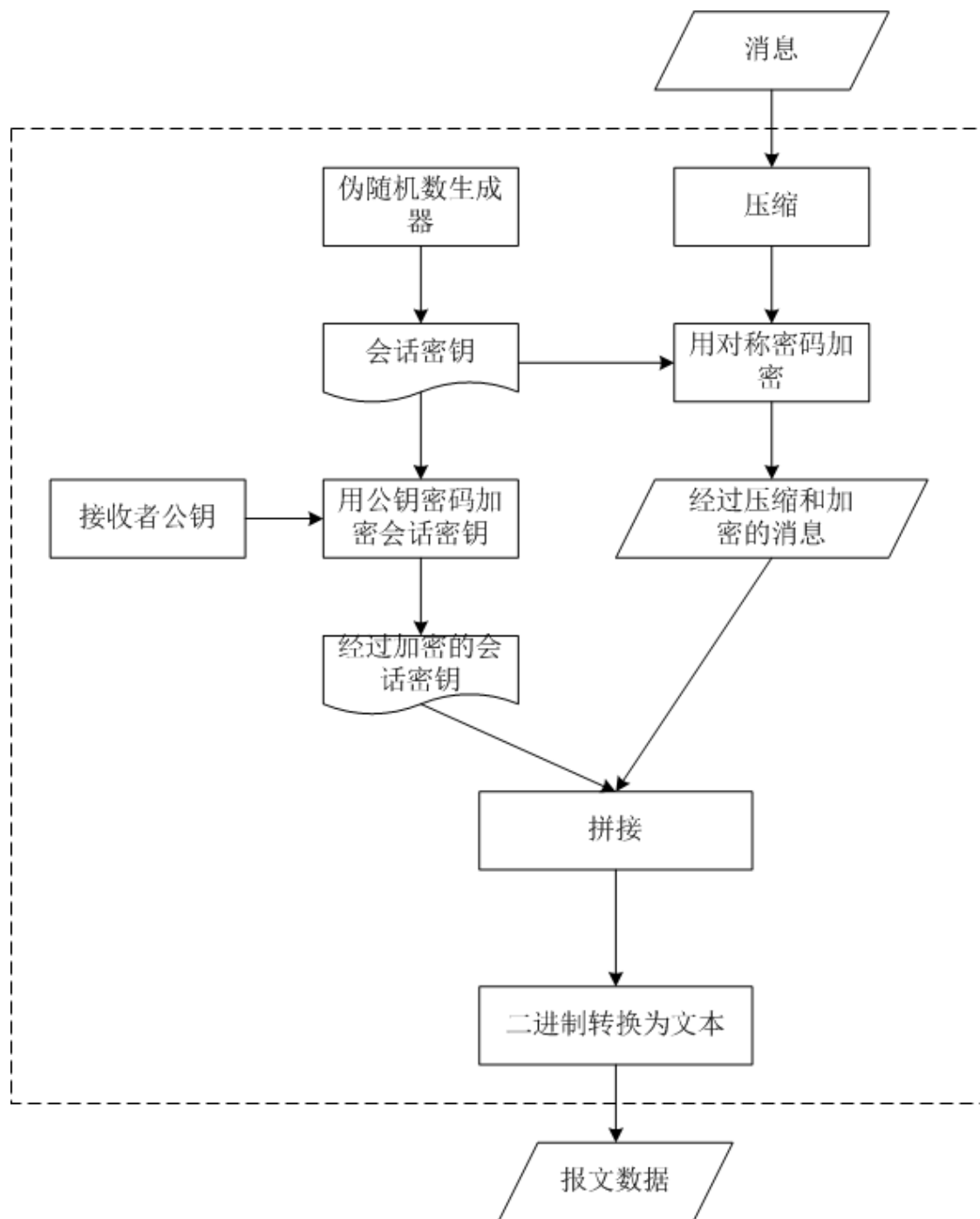
- PGP支持数据的压缩和解压，目的是提高数据存储和传输的效率，支持ZIP、ZLIB、BZIP2等格式

PGP: 电子邮件兼容性

- 电子邮件系统通常支持ASCII文本格式，而加解密通常是对二进制进行操作，因此需要进行兼容性处理，二进制与Radix-64互相转换
- Radix-64编码
 - ◆ 基于base64，增加了检测数据错误的校验和。
 - ◆ Base64编码是一种可以将任何二进制数据都用A~Z、a~z、0~9、+、/共64个字符外加=（用于末尾填充）来表示的编码方法

PGP加密和解密

PGP 的加密流程



PGP: 加密

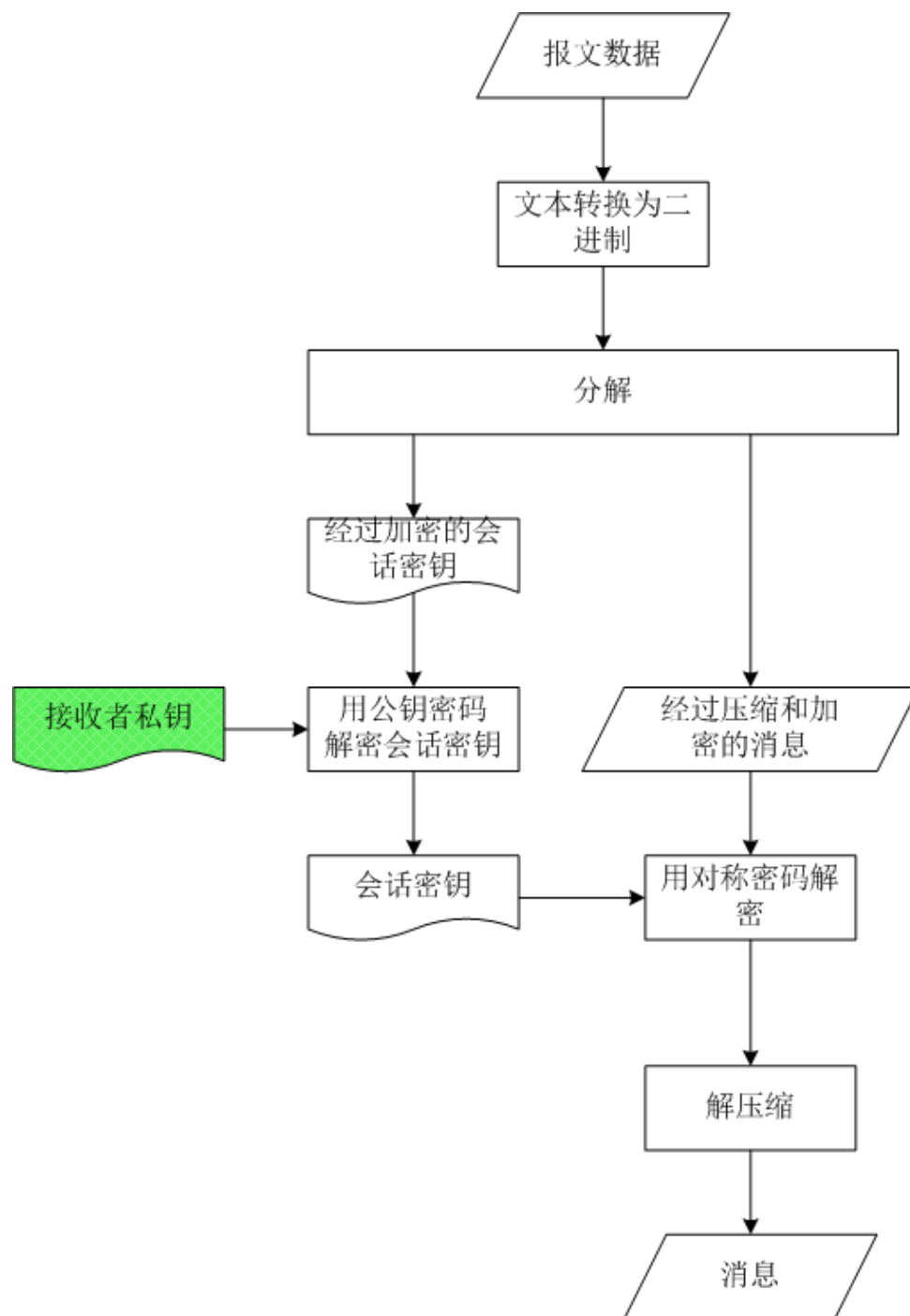
□ 生成和加密会话密钥

- ◆ (1) 用伪随机数生成器生成**会话密钥**
- ◆ (2) 采用公钥加密算法，用接收者的公钥加密会话密钥

□ 压缩和加密消息

- ◆ (3) 压缩消息
- ◆ (4) 使用对称密码对压缩后的消息进行加密，密钥为步骤 (1) 中的**会话密钥**
- ◆ (5) 将加密的会话密钥 (步骤 (2) 中) 与加密的消息 (步骤 (4) 中) 拼接起来
- ◆ (6) 将步骤 (5) 中结果转换为文本数据，得到报文数据。

PGP解密流程



PGP: 解密

□ 解密私钥

- ◆ (1) 接收者输入解密的口令
- ◆ (2) 求口令的散列值, 生成用于解密私钥的密钥
- ◆ (3) 对钥匙串中经过加密的私钥进行解密

□ 解密会话密钥

- ◆ (4) 将报文数据 (文本形式) 转换为二进制数据
- ◆ (5) 将二进制数据分解为两部分: 会话密钥的密文和消息的密文
- ◆ (6) 用步骤 (3) 中生成的接收者的私钥解密会话密钥

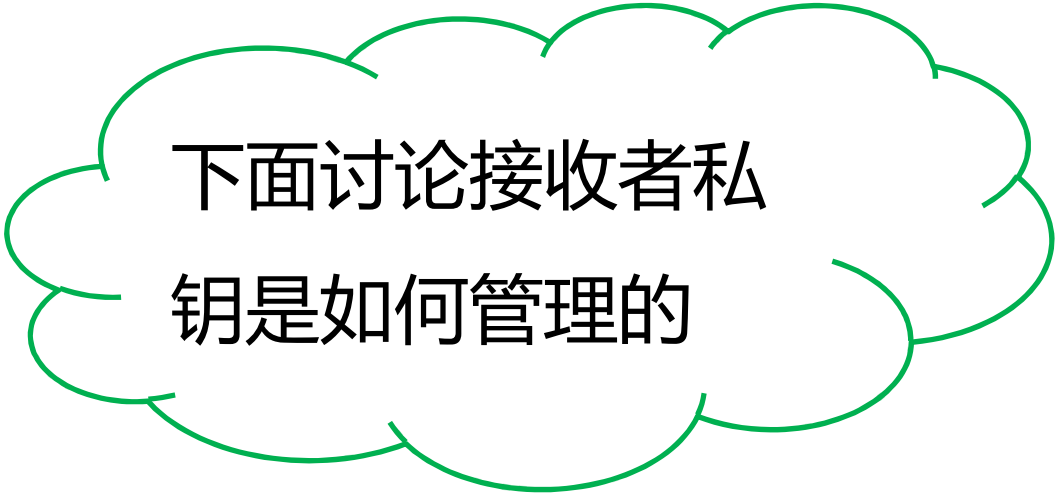
PGP: 解密

□ 解密和解压消息

- ◆ (7) 使用步骤 (6) 中生成会话密钥解密消息密文，得到压缩过的消息
- ◆ (8) 对步骤 (7) 中的输出进行解压缩
- ◆ (9) 得到原始消息

接收者私钥管理

- PGP解密中，我们用到了接收者的私钥，但是私钥是如何管理的并没有提及。

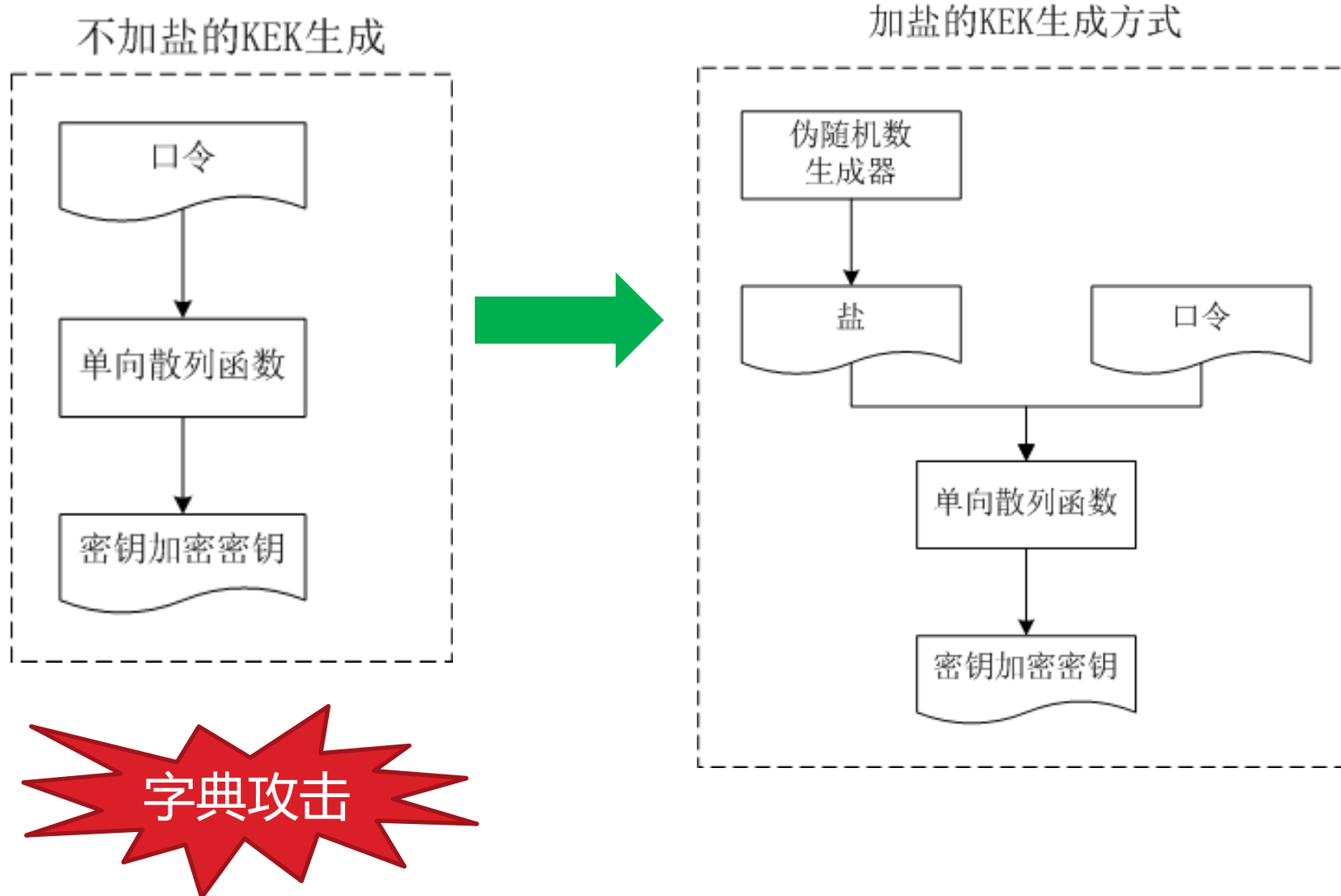


下面讨论接收者私
钥是如何管理的

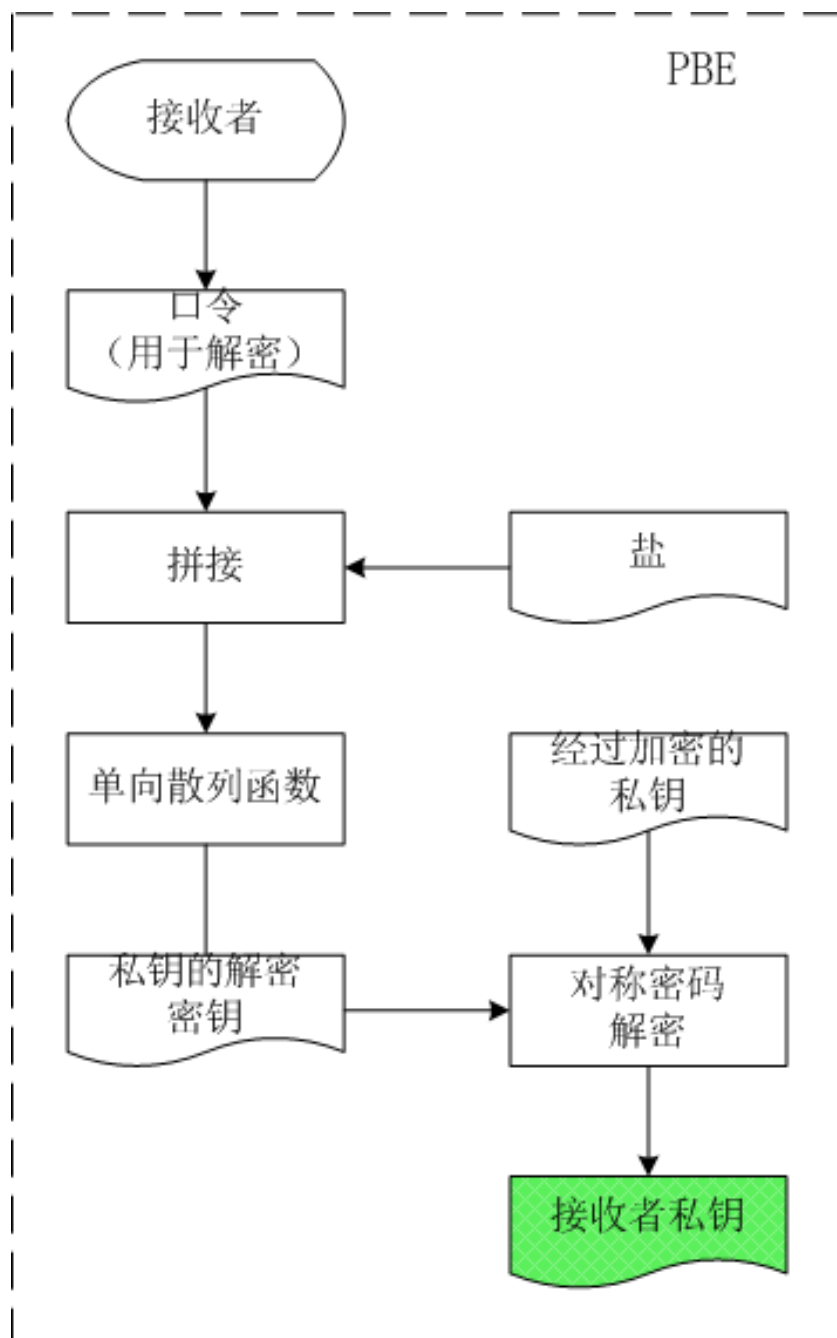
接收者私钥管理

- 私钥——记在脑袋里
 - ◆ 记不住：长串随机数
- 私钥——明文存放计算机上
 - ◆ 不安全
- 加密存放在计算机上
 - ◆ 合理：加密私钥的密钥怎么管理？
- PBE to rescue

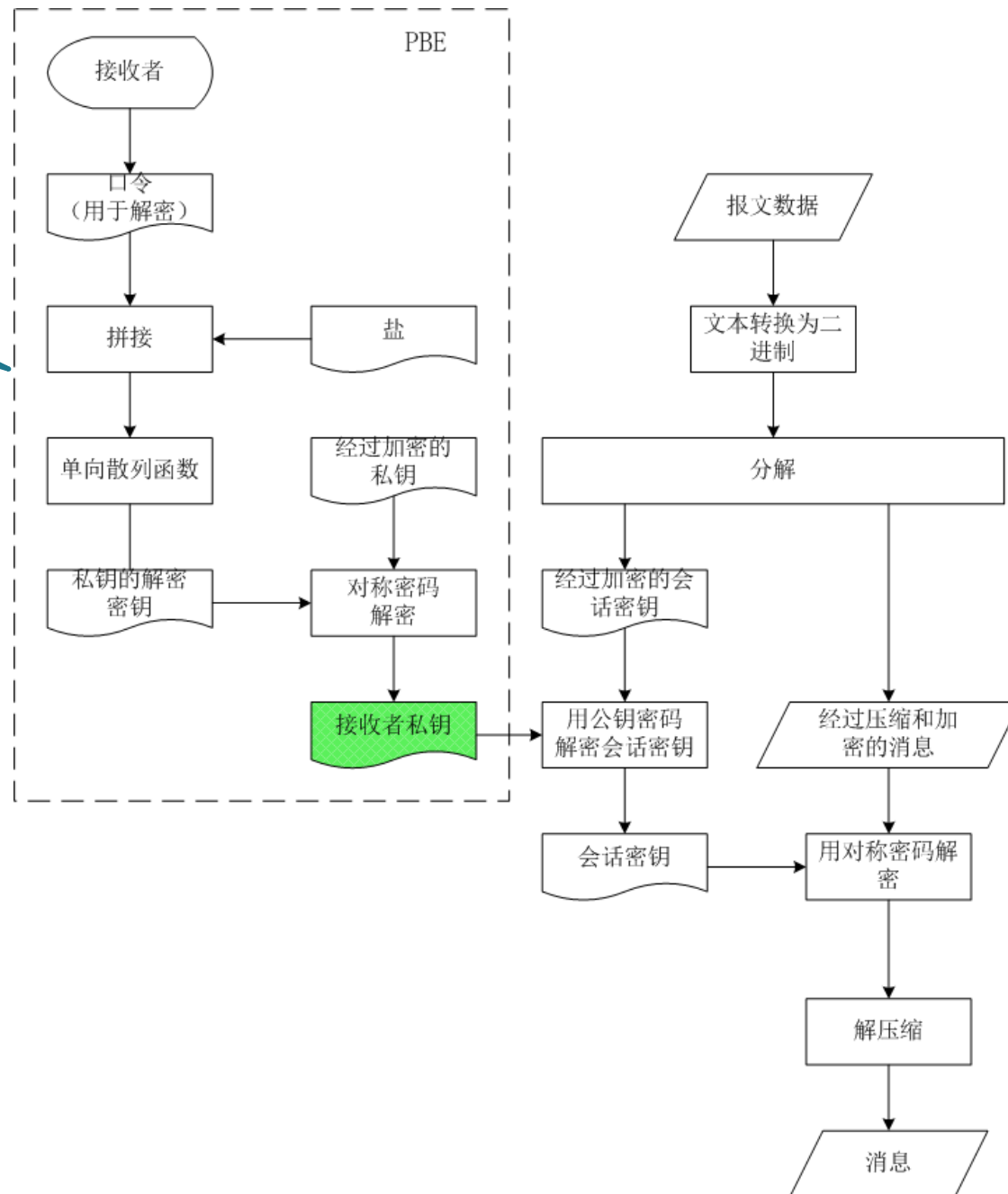
Password Based Encryption



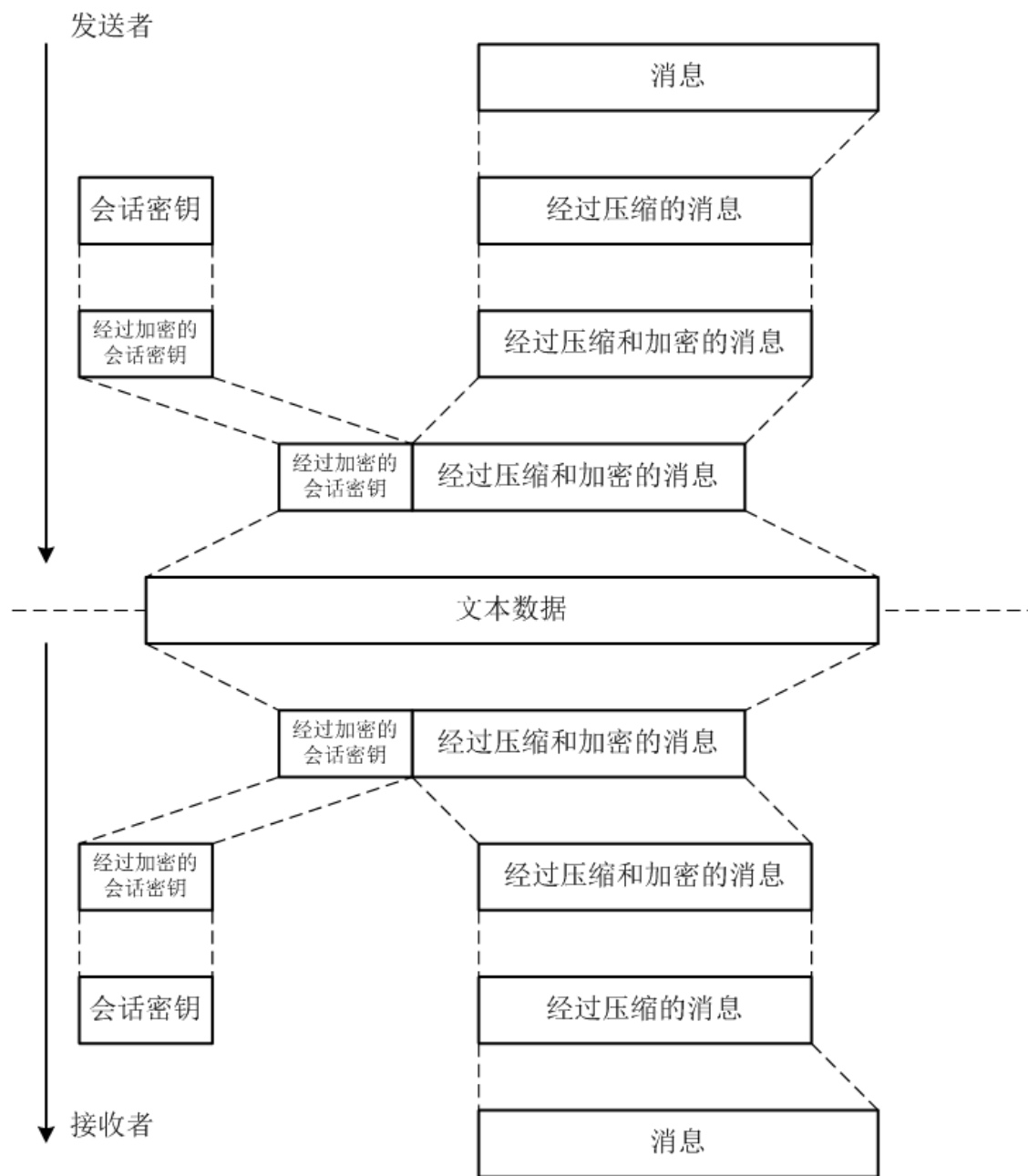
接收者私钥管理: PBE



合并PBE和 解密部分



完整的加解密过程



只采用加解密功能，具有消息的保密性，也确保了接收者是正确的，但是无法保证发送者的身份。因此，在只需要消息的保密性的前提下，只用PGP的加解密功能是可以的。