安全编程

沈佳辰
jcshen@sei.ecnu.edu.cn

- 办公室:理科大楼B1203
- Email: jcshen@sei.ecnu.edu.cn
- 电话：62233147

助教信息

- 姓名：陈馨
- Email: 51184501097@stu.ecnu.edu.cn
- 答疑时间：周二 10:00-11:00
  地点：理科大楼B1212

主要内容

- 概述
- 大素数生成
- 流密码
- 对称加密
- 非对称(公钥)加密
- 消息摘要
- MAC（消息认证码）
- 数字签名

- 考核方式

平时成绩60%，期末考试40%

0.1 概述

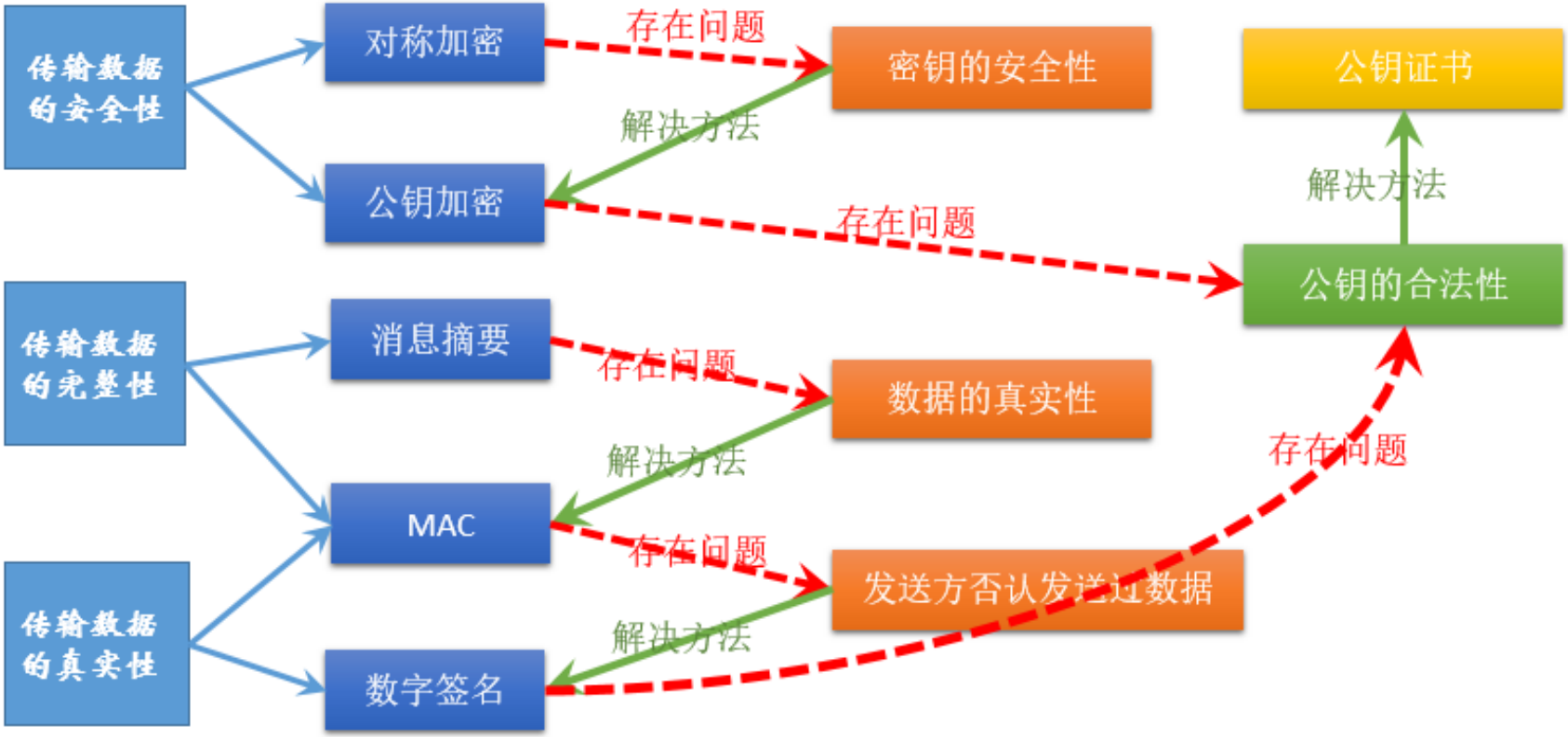
当发送方A向接收方B发送数据时，需要考虑的问题有：

0.1 概述

当发送方A向接收方B发送数据时，需要考虑的问题有：

1. 数据的安全性。
2. 数据的完整性，即数据不被篡改。
3. 数据的真实性，即数据确实来自于发送方，传输过程中没有被替换。
4. 数据的不可否认性，即验证发送方确实发送了数据。

0.1 概述


传输数据的安全性
传输数据的完整性
传输数据的真实性
对称加密
公钥加密
消息摘要
MAC
数字签名
存在问题
解决方法
密钥的安全性
数据的真实性
发送方否认发送过数据
公钥证书
公钥的合法性

0.1.1 基本概念

- 明文（Plaintext）

  待伪装或加密的消息（Message）。在通信系统中它可能是比特流，如文本、位图、数字化的语音流或数字化的视频图像等。一般可以简单的认为明文是有意义的字符或比特集，或通过某种公开的编码标准就能获得的消息。明文常用m或p表示。

- 密文(Ciphertext)

  对明文施加某种伪装或变换后的输出，也可认为是不可直接理解的字符或比特集，密文常用c表示。

0.1.1 基本概念

- 明文（Plaintext）

  待伪装或加密的消息（Message）。在通信系统中它可能是比特流，如文本、位图、数字化的语音流或数字化的视频图像等。一般可以简单的认为明文是有意义的字符或比特集，或通过某种公开的编码标准就能获得的消息。明文常用m或p表示。

- 密文(Ciphertext)

  对明文施加某种伪装或变换后的输出，也可认为是不可直接理解的字符或比特集，密文常用c表示。

- 加密（Encrypt）

  把原始的信息（明文）转换为密文的信息变换过程。

- 解密（Decrypt）

  把已加密的信息（密文）恢复成原始信息明文的过程，也称为脱密。

0.1.1 基本概念

- 密码算法(Cryptography Algorithm)

  也简称密码（Cipher），通常是指加、解密过程所使用的信息变换规则，是用于信息加密和解密的数学函数。对明文进行加密时所采用的规则称作加密算法，而对密文进行解密时所采用的规则称作解密算法。加密算法和解密算法的操作通常都是在一组密钥的控制下进行的。

0.1.1 基本概念

- 密码算法(Cryptography Algorithm)

  也简称密码（Cipher），通常是指加、解密过程所使用的信息变换规则，是用于信息加密和解密的数学函数。对明文进行加密时所采用的规则称作加密算法，而对密文进行解密时所采用的规则称作解密算法。加密算法和解密算法的操作通常都是在一组密钥的控制下进行的。

- 密钥（Secret Key）

  密码算法中的一个可变参数，通常是一组满足一定条件的随机序列。用于加密算法的叫做加密密钥，用于解密算法的叫做解密密钥，加密密钥和解密密钥可能相同，也可能不相同。

0.1.1 基本概念

- 密码算法(Cryptography Algorithm)

  也简称密码（Cipher），通常是指加、解密过程所使用的信息变换规则，是用于信息加密和解密的数学函数。对明文进行加密时所采用的规则称作加密算法，而对密文进行解密时所采用的规则称作解密算法。加密算法和解密算法的操作通常都是在一组密钥的控制下进行的。

- 密钥（Secret Key）

  密码算法中的一个可变参数，通常是一组满足一定条件的随机序列。用于加密算法的叫做加密密钥，用于解密算法的叫做解密密钥，加密密钥和解密密钥可能相同，也可能不相同。

  密钥常用k表示。在密钥k的作用下，加密变换通常记为$E_k(\cdot)$，解密变换记为$E_k(\cdot)$或$E_k^{-1}(\cdot)$。

0.2 对称加密

又称共享加密，加解密使用相同的密钥。

0.2 对称加密

又称共享加密，加解密使用相同的密钥。

常见算法：DES AES

1）A将数据加密后发送给B。

2）密文即使在传送过程中被截获，因为不知道密钥也无法解密。

3）B接收到密文之后，需要使用加密相同的密钥来解密。

4）需要A将密钥传给B，但保证密钥传输过程中的安全又成了问题。

0.2 对称加密

优点：计算速度快。

0.2 对称加密

优点：计算速度快。

缺点：为了传送数据的安全，将数据加密后进行传输，但是对称加密需要发送方将密钥安全地传给接收方以便接收方解密，因此密钥如何安全传送又成了一个问题。

问题：如何保证密钥的安全性？

0.3 非对称加密

也称公钥加密，这套密钥算法包含配套的密钥对，分为加密密钥和解密密钥。加密密钥是公开的，又称为公钥；解密密钥是私有的，又称为私钥。数据发送者使用公钥加密数据，数据接收者使用私钥进行数据解密。

0.3 非对称加密

也称公钥加密，这套密钥算法包含配套的密钥对，分为加密密钥和解密密钥。加密密钥是公开的，又称为公钥；解密密钥是私有的，又称为私钥。数据发送者使用公钥加密数据，数据接收者使用私钥进行数据解密。

常见算法：RSA　椭圆曲线算法

1）B生成密钥对，将公钥传给A，私钥自己保留。公钥即使被其他人获得也没有关系。

2）A用B传过来的公钥将要发送的明文数据加密，然后将密文发送给A。其他人即使获得密文也无法解密，因为没有配对的用来解密的私钥。

3）B接收到A传送过来的密文，用自己保留的私钥对密文解密，得到明文。

0.3 对称加密

优点：解决了密钥的安全性问题。

缺点：一是计算速度慢；

二是无法保证公钥的合法性，因为接收到的公钥不能保证是B发送的，比如，攻击者截获B的消息，将公钥替换。

0.4 消息摘要

消息摘要函数时一种用于判断数据完整性的算法，也称为散列函数或哈希函数，函数的返回值就散列值，散列值又称为消息摘要或者指纹。这种算法是不可逆的，即无法通过消息摘要反向推导出消息，因此又称为单向散列函数。

0.4 消息摘要

消息摘要函数时一种用于判断数据完整性的算法，也称为散列函数或哈希函数，函数的返回值就散列值，散列值又称为消息摘要或者指纹。这种算法是不可逆的，即无法通过消息摘要反向推导出消息，因此又称为单向散列函数。

常见算法：MD5 SHA

当我们使用某一软件时，下载完成后需要确认是否是官方提供的完整版，是否被人篡改过。通常软件提供方会提供软件的散列值，用户下载软件之后，在本地使用相同的散列算法计算散列值，并与官方提供的散列值向对比。如果相同，说明软件完整，未被修改过。

0.4 消息摘要

优点：可以保证数据的完整性。

0.4 消息摘要

优点：可以保证数据的完整性。

缺点：无法保证数据的真实性，即不能确定数据和散列值是来自发送方的，因为攻击者完全可以将数据和散列值一起替换。

问题：如何验证发送的数据确实来自于发送方？

0.5 MAC

消息认证码（Message Authentication Code，简称MAC）是一种可以确认消息完整性并进行认证的技术。消息认证码可以简单理解为一种与密钥相关的单向散列函数。

0.5 MAC

消息认证码（Message Authentication Code，简称MAC）是一种可以确认消息完整性并进行认证的技术。消息认证码可以简单理解为一种与密钥相关的单向散列函数。

1）A把消息发送给B前，先把共享密钥发送给B。

2）A把要发送的消息使用共享密钥计算出MAC值，然后将消息和MAC发送给B。

3）B接收到消息和MAC值后，使用共享密钥计算出MAC值，与接收到的MAC值对比。

4）如果MAC值相同，说明接收到的消息是完整的，而且是A发送的。

0.5 MAC

优点：可以保证数据的完整性和真实性。

0.5 MAC

优点：可以保证数据的完整性和真实性。

缺点：接收方虽然可以确定消息的完整性和真实性，解决篡改和伪造消息的问题，但不能防止A否认发送过消息。例：加入A给B发送了消息，B接收到之后，A否认自己发送过消息给B，并抵赖说，“虽然我和B都能计算处正确的MAC值，但是可能是B的密钥被攻击者盗取了，攻击者给B发的消息。”

问题：如何让发送方无法否认发送过数据？

0.6 数字签名

数字签名（Digital Signature）可以解决发送方否认发送过消息的问题。数字签名的重点在于发送方和接收方使用不同的密钥来进行验证，并且保证发送方密钥的唯一性，将公钥算法反过来使用可以达到此目的：A发送消息前，使用私钥对消息进行签名，B接收到消息后，使用配对的公钥对签名进行验证；如果验证通过，说明消息就是A发送的，因为只有A采用配对的私钥；第三方机构也是依据此来进行裁决，保证公正性。

0.6 数字签名

1）A把消息用哈希函数处理生成消息摘要，并将摘要用私钥进行加密生成签名，把签名和消息一起发送给B。

2）数据经过网络传送给B，当然，为了安全，可以用上述的加密方法对数据进行加密。

3）B接收到数据后，提取出消息和签名进行验签。采用相同的哈希函数生成消息摘要，将其与接收的签名用配对的公钥解密的结果对比，如果相同，说明签名验证成功。消息是A发送的，如果验证失败，说明消息不是A发送的。

0.6 数字签名

1）A把消息用哈希函数处理生成消息摘要，并将摘要用私钥进行加密生成签名，把签名和消息一起发送给B。

2）数据经过网络传送给B，当然，为了安全，可以用上述的加密方法对数据进行加密。

3）B接收到数据后，提取出消息和签名进行验签。采用相同的哈希函数生成消息摘要，将其与接收的签名用配对的公钥解密的结果对比，如果相同，说明签名验证成功。消息是A发送的，如果验证失败，说明消息不是A发送的。

问题：仍然没有解决确保公钥合法性的问题。

0.7 公钥证书

我们看到，上面的公钥加密，数字签名的问题都在于如何保证公钥的合法性。

解决办法是将公钥交给一个第三方权威机构——认证机构（Certification Authority）CA来管理。接收方将自己的公钥注册到CA，由CA提供数字签名生成公钥证书（Public-Key Certificate）PKC，简称证书。证书中有CA的签名，接收方可以通过签名验证来验证公钥的合法性。

0.7 公钥证书

1）接收方B生成密钥对，私钥自己保存，将公钥注册到CA。

2）CA通过一系列严格的检查确认公钥是B本人的。

3）CA生成自己的密钥对，并用私钥对B的公钥进行数字签名，生成数字证书。证书中包含B的公钥和CA的签名。这里进行签名并不是要保证B的公钥的安全性，而是要确定公钥确实属于B。

4）发送方A从CA获取B的证书。

5）A使用CA的公钥对从CA获取的证书进行签名验证，如果成功就可以确保证书中的公钥确实来自B。

6）A使用证书中B的公钥对消息进行加密，然后发送给B。

7）B接收到密文后，用自己的配对的私钥进行解密，获得消息明文。