网络安全技术

实验报告

学院：网安学院

年级：2020

班级：信安班

学号：2011395

姓名：魏伯繁

手机号：18611111192

2023 年 4 月 22 日

目录

1 实验要求

请简要评述以 DES 为代表的对称密钥密码系统的优缺点，以 RSA 为代表的非对称秘钥密码系统的优缺点。

2 对称密钥的优缺点分析

2.1 优点

2.1.1 加密解密速度快

以 DES 为代表的对称密钥密码系统一般都是快速高效的加密解密算法，一般处理速度都较快，具有较好的性能，这得益于对称密钥体制的实现方式，许多加密解密流程都可以通过移位操作或者查表对应位置置换等操作完成，而这些操作所需要的 cpu 指令数都很少，所以速度极快。这样的特性让对称密钥加密体制可以应用于很多对实时性有要较高求的场景，比如网络信息传输或者金融交易市场等等，这些领域都对信息的实时性有较高的要求，适合使用对称加密密码体制。

2.1.2 易于实现和使用

对称加密密码体制的一个重要的特点就是加密流程和解密流程的原理是一致的，像 DES 加密体制，他的加密和解密流程的算法组成部分是完全一致的，只是顺序有区别，所以说对于编程这来说是十分友好的

2.1.3 密钥管理简单

以 DES 密码体制为例的对称加密体制一般都采用 64、128、192、256 比特为单位作为密钥的长度，且在一般情况下密钥是在较长时间段内不更换的，所以通信双方只需要在长时间维护一个占用存储空间很少的密钥，之后便不再需要对密钥的信息进行交互，在一定程度上降低了密钥管理难度，增大了密钥的安全性。

2.1.4 对设备的要求低普适性强

正如前面所说，一般而言，对称加密密码体制的加密解密速度都很快，其内部的操作一般由移位或者查表转换完成，而这些操作方式非常简单，且计算量一般不大，在一些算力一般的设备上也可以顺利高效的运行，一些很简单的嵌入式硬件都可以很好的集成 DES 算法，普适性非常强。

2.2 缺点

2.2.1 易遭受穷举密钥攻击

以 DES 为例，很多对称密钥加密体制的密钥长度都只有不超过 64 位（DES 实际上只有 56 位），随着计算机硬件的高速发展以及各种超算中心的诞生，穷举 DES 的密钥空间已经成为一件可能的事

情，所以 DES 在一些重要领域，尤其是一些实时性没有那么强但十分注重隐私的领域已经不再适用。

2.2.2 密钥分配困难

一般情况下，我们默认通信双方已经共享了对称密码体制的密钥，一般而言我们认为是通过绝对安全的信道进行共享的，但是事实上这样的绝对安全的信道是不存在的，这也就导致通信双方交流一个共同的密钥变得十分困难，而且一般而言，对称密码体制的密钥是需要定期更换的，否则很可能遭受穷举密钥攻击，那么此时如何让通信双方协调一个新的密钥就成为了一个很棘手的问题。

2.2.3 缺乏前向保密性

对称密码体制缺乏基本的前向保密性，也就是说一旦密钥被破解，则之前所有的用该密钥传输的信息都能够被破解，这样可能导致大量的信息泄露，是无法被接受的重大缺陷。

2.2.4 难以抵抗散列攻击和重放攻击

对称密码体制的密钥只在消息的发送和接收时才有效，这就导致当密钥泄漏时攻击者可以通过这个密钥对信息进行篡改从而重新计算散列值欺骗通信方，使其认为被篡改后的信息是合法的，重放攻击则为使用之前的信息重复传输，这在军事领域可能造成非常严重的后果

2.3 改进

针对 DES 的一些缺点，也有很多改进方式，例如我们很熟悉的 3DES，也就是利用 DES 进行反复加密，进行三轮的扩散和混淆可以在一定程度上增加破解难度，因为这样增加了密钥的空间，使穷举变得几乎不可能。同样，在实际应用场景中我们还可以摒弃 ECB 模式转而使用 CBC 模式或者 PCBC 模式等，让敌手无法利用连续的两个信息进行破击，这样的分组密码体制的工作模式也极大程度上增强了分组密码体制的安全性。

虽然对称加密算法的安全性随着计算机硬件和算力的发展变得主键不再十分安全，但是他的应用场景依然很广，在一些对数据隐私要求不是非常严格且对实时性要求很高，数据信息的有效性过期很快的场景依然有着广泛的应用，只要我们针对不同的加密方式充分发挥他的优点就能够做到扬长避短。

3 非对称密钥的优缺点分析

3.1 优点

3.1.1 更加安全

相较于对称加密算法，非对称加密算法明显是更加安全的，因为非对称加密算法一般都是基于难解性问题定义的，例如基于圆锥曲线对数的难解性问题，这种难解性问题是有严格的数学证明的，可以在理论上充分保证其安全，一般这种数学问题的穷举空间都是十分庞大的，即使在计算机算力大幅

度进步的今天想要穷举破解对称加密算法的密钥所需要的时间依然很长，很容易就会超过秘密信息情报的有效期。

3.1.2 同步更新密钥简便

对于对称密钥来说，其中一个非常困哪的点就是密钥交换很不方便，因为在实际应用中，是不能长期使用同一个密钥的，但是密钥的更换要使用绝对安全的通道，这样的通道在实际中是不存在的，但是对于公钥来说却不存在这样的问题，因为如果要更改私钥，只需要将对应的公钥公开出去就能够完成私钥的更新，同步更新密钥变得非常简便。

3.1.3 应用场景的增加：可以实现数字签名

随着数字文件的传输越来越广泛，可能会存在一些重要文件在传输过程中需要进行数字签名的场景，这个时候公钥加密体制就会派上用场，非对称加密算法可以通过数字签名的方式确保数据的完整性和真实性，数字签名可以保证数据来源的真实性，证明数据的完整性，并且防止数据被篡改，能够在更广泛的应用场景中实现可靠的数据交换。

3.2 缺点

3.2.1 运算速度慢

由于非对称加密算法的正确性普遍依赖于复杂的数学原理，所以其计算量非常大会占用很多 CPU 资源，所以并不适用于所有的应用领域，在一些对实时性要求很高的应用场景以及一些非特定嵌入式场景就不太使用，而且不太适合进行大规模的数据加密。

3.2.2 容易受到中间人攻击

非对称加密算法在进行密钥交换时，容易受到中间人攻击，攻击者可以截获数据，篡改密钥的公共部分，导致通信双方使用的密钥不同，从而直接威胁到通信的安全性。而且很容易将很多已经过时的消息重复传输，容易造成不安全信息传递。

3.2.3 公钥认证问题

尽管公钥可以方便地进行分发，但在使用非对称加密算法时，要注意公钥的信任和认证问题，避免出现伪造公钥等恶意攻击。

3.3 改进

针对非对称加密算法存在的问题，可以采取以下方法进行解决：

3.3.1 加强密钥管理

对于非对称加密算法，密钥管理是一项非常重要的工作。为了避免密钥被泄露，可以采取如下措施：加密存储密钥、定期更换密钥、限制密钥的使用权限等方法。

3.3.2 采用更高效的算法

为了解决非对称加密算法在计算速度方面存在的问题，可以使用更高效的算法来加密和解密数据，从而提高加密和解密的效率，例如采用椭圆曲线加密算法。

3.3.3 使用混合加密算法

为了克服非对称加密算法与对称加密算法各自局限的问题，可以将两种算法结合起来，利用非对称加密算法来解决密钥的分布问题，再利用对称加密算法来加密大量数据，以达到更高的安全性和效率。

3.3.4 动态生成密钥

与传统的密钥方式不同，动态生成密钥可以解决传统密钥方式的缺点，但也存在计算量大的问题，因此需要在实现效率和安全性之间做出取舍。

而针对中间人攻击问题，可以采用数字证书和数字签名技术来进行认证和验证，加强安全性。总之，通过综合采取以上几种解决方案，可以进一步保障非对称加密算法的安全性、效率和便捷性。