基于 DES 和 RSA 加密技术的大数据加密传输技术的算法研究

张 乐
(钟山职业技术学院,江苏 南京 210049)

摘 要: 近年来,随着科学技术的不断发展,一些网络安全事件频发,人们对网络信息安全要求也越来越高,因此数据加密技术被广泛应用于各行各业来保护一些商业信息和数据。当前应用较为广泛的就是 DES 和 RSA 两种加密技术。其中,DES 算法虽然具有速度较快的优点,但是其安全性、可靠性和密钥固定性都较低,这就已经不能满足当前人们对数据加密技术的安全性的要求。而 RSA 算法虽然具有较好的安全性,但是其运算速度较慢,这主要是因为其密钥的长度不固定。针对两者的优缺点,一些研究机构提出了将 DES 加密技术和 RSA 加密技术相结合创新出一种新的加密技术,接下来,文章将就这个综合加密技术的算法进行详细的研究和探讨。

关键词: DES 加密技术; RSA 加密技术; 大数据加密传输技术; 算法研究

1 DES 加密技术算法

DES 是一种较为标准的加密方式,其计算的方式也可以被认为是分组加密,具体来说就是先将数据按照 64 bit 进行分组,之后分了组的数据进行加密操作,检验使用的是 8 bit 的奇数偶数,其密钥的而长度是 56 bit字节。在用 DES 进行计算时,输入端是 64 bit 的明文,输出端是 64 位的密文。这种算法在对数据加密和解密时使用的是同一计算方法,密钥是保证其安全性的关键。执行过程中,DES 按照上述所说先对 64 bit 的明文进行分组加密,这个过程一般是通过转换器来实现的,也就是明文分为左右两组,每组的字节长度是 32 bit,然后在进行 16 次轮换的计算,进而实现加密,预算的整个操作和过程被称为 f,这个预算的主要目的就是使密钥和要传输的数据结合,在两组长度为 32 bit 的分组数据进行 16 次的轮换计算后,这两组数据就在此进行组合。这一步骤完成后,结合的数据经由另一个转换器输出,而这个输出过程的计算和前面的计算过程正好是相反的,经过两次转换整个算法就完成了。其中,在每个轮次处理中,密钥会移动一定的距离,具体来说就是在 56 bit 中任意选取 48 bit,然后利用扩展器将右边的数据形成一个 48 bit 的信息,同时完成和 48 bit 密钥相互结合的目的,然后再用 s 盒结合后的密钥进行处理和转化就可以得到 32 bit 的新数据。通过这种方式可以完成加密的运算,接着另一边的 32 bit 也进行同样的操作。在实际的加密过程中,两边的加密步骤是同时进行的,并且加密形成后两边的数据换了位置,这主要就是利用了异或运算,函数 f 和左边的 32 bit 数据相结合后相乘新的右半边部分,加密之前的右半边在加密之后就变成了新的左半边数据,将这个过程重复进行 16 次,就可以实现 DES 的 16 轮次的计算。

2 RSA 加密技术算法

RSA 加密技术算法和 DES 加密技术算法不同,RSA 有两个不同的密钥,一个是公共密钥,另一个是私有的密钥,在加密的过程中,一般将公共密钥作为加密的密钥,将私有的密钥作为解密的密钥。在 RSA 算法中的密钥有 40~2 048 bit,和 DES 不同 RAS 将明文分解为“块”,这些“小块”的大小是可以变化的,但是前提是在设置长度时不能超过密钥的长度。RAS 算法的主要思路就是将明文分解成“小块”,这些“小块”的长度和密钥的长度要保持相同,可以知道密钥长度越长其加密效果也就越好,但同时进行解密时的操作步骤也就越复杂。所以,这种加密技术在使用过程中就呈现出安全性较高,但不够快速,其应用性较差的特点,在充分考虑到其安全性和应用性的前提下,一般采用 64 bit。在利用 RAS 算法加密时首先要对安全大素数进行选取,并将其命名为 P 和 Q,为了进一步增强加密技术的安全性,一般都将上面这两个安全大素数设置成相同的长度。计算 $n=p\times q$,而 n 要大于 512 bit,这主要就是为了进一步确保 RES 加密的安全性,因为 RES 的计算是在因子分解的大数的基础上建立起来的; 接着,对 n 的欧拉函数进行计算,要用到的公式是 $\varphi(n)=(p-1)(q-1)$,$\varphi(n)$ 计算出来是应该小于或者等于 n 的,并且和为互素数; 再然后就是从 $[0,\varphi(n)-1]$ 的区间中任意选取加密的密钥 e; 最后就是要利用 *Euclid* 法对密钥的解密 d 进行求解,并且 $de=1(mod\varphi(n))$,其中 d 和 n 为互质,经过计算得出来的 e 和 n 就是进行加

基金项目: 2018 年江苏高校哲学社会科学研究基金项目; 项目名称: 注册招生制度下高职院校毕业设计质量保障和评估体系的研究与实践; 项目编号: 2018SJA0723。

作者简介: 张乐(1981—),女,江苏扬州人,讲师,硕士; 研究方向: 计算机技术及应用。

密的公共密钥,而 d 就是进行解密的私有密钥。RSA 算法的加密和解密:如果加密的信息是 m,那就将 m 看作是具有一定长度的整数,如果 n 小于 m,就先将 m 分成数个长度相等的“小块”,并将其命名为 m_1、m_2、m_3……m_i,长度为 s 并且满足 2^s 小于等于 n 的前提条件,同时保证 s 要尽量大。在上述步骤结束后再对数据块进行加密,在这个过程中 m_i 产生的密文是 $c_i = m_i^e \pmod n$,分块均进行解密时和 c_i 配合的明文是 $m_i = c_i^d \pmod n$。

3 DES 算法和 RAS 算法的结合

RAS 算法主要遵循以下原则,就是在对资料数据 M 和密钥 M 进行处理时,加减法所用的时间为 $0(M)$,乘除法所用的时间为 $0(M^2)$,在对 $a^b \bmod c$ 进行计算时需要的时间是 $0(M^3)$,依次类推,对 M 为数据信息进行计算时所用的时间为 $0(M^3)$。在实际的操作过程中,当资料的长度在 512~1 024 bit 时,就要想到其加密的安全性,但是这样下来整个 RAS 算法的计算量是非常的大的。可以看出,当要进行加密的数据资料过大,采用 RAS 算法将会消耗大量的时间,其时间是 DES 算法的 M 多倍。除此之外,当加密的数据资料过大,利用 RAS 算法产生密钥所需要的时间也是非常长的,加入有 M 列密钥,两个相连的质数的平均间隔是 $0(M)$。表 1 是对一个测试机进行加密的结果,从表 1 可以看出 RAS 需要的时间长,但安全性高,DES 需要的时间短,但是安全性低。

表 1 测试结果统计

算法	运行时间/ms	加密时间/ms	解密时间/ms	安全
DES 算法	20 000	74 650	5 680	低
RAS 算法	20 000	3 234 660	4 128 460	高

采用 DES 和 RAS 相结合,假设发送的信息是 A,其加密密钥为 kea,解密密钥为 kda,接收方为 B,加密密钥为 keb,解密密钥为 kdb,其结合方式如下:(1)发送数据的一方先生成 DES 密钥 K;(2)发送数据的一方进行服务器上传时采用的是 RAS 算法的公共密钥 Keb,然后利用这个公共密钥对上面说的密钥 K 进行加密的处理;(3)发送的一方将编号的信息分别用发送方的解密密钥为 kda 和接收方的解密密钥为 kdb 进行签名以便在解密的过程中进行辨别;(4)发送一方用 K 将数据加密并形成文件,将这个文件和 CK 一起形成完整的加密数据发送给接收的一方;(5)在收到 C 后,接收方先利用本来的解密密钥进行解密,将 C 中的 K 解出,之后再用 K 对明文和签名信息进行解密;(6)接收方将发送者的公开密钥和自己的原本的解密密钥对签名的信息进行识别和处理,形成新的签名信息发送给另一方;(7)两方在完成这一系列接收和处理操作后就可以将 DES 的密钥 K 删掉。密钥加密过程如图 1 所示。

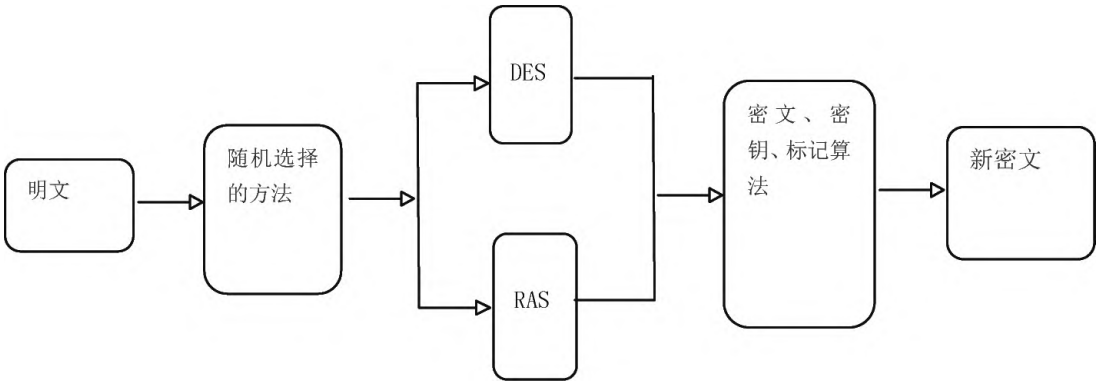

图 1 密钥加密的过程

4 基于 DES 和 RSA 加密技术的大数据加密传输技术

4.1 DES 算法和 RAS 算法实现的过程

在实际的数据加密过程中,往往用 DES 算法来对对称数据进行加密,用 RAS 算法对非对称数据进行加密。前者在进行加密的过程中采用的还是 DES 的 64 位加密分组的形式,密钥的长度还采用 56 位,进行 16 轮次的计算和编制。但是,这里为了进一步提高算法的安全性,进行了相应的技术改进,利用 3 个密钥来进行逐层加密,假设这 3 个密钥分别为 K_1,K_2,K_3,明文为

P,密文为 C,那么 $C=EK_3[DK_2[EK_1[P]]]$,可以看出,虽然计算的时间增加了,但是其安全性也得到了提升。其实,DES 算法主要的步骤有 3 个:密钥生成、计算加密、解密,这种软件形式的加密比硬件形式的加密要慢,但是其经济性、可行性和应用范围都较好。

用 RAS 算法对非对称数据进行加密,其可行性和实用性更高,它不仅能够对数据本身进行加密也能够对数字签名进行维护,这种 RAS 算法可以对那些二次加密的软件进行传输,可以在一定程度上提高数据传输的安全性。

4.2 数据安全传输

整个加密过程中最重要的模块就是数据传输模块,首先数据传输模块和中央控制器形成关联并创建相应的窗口,其功能就是让所有的部件和控制器进行数据传输,另一方面这些控制器也可以通过窗口进行指令的传达。那么如何保证这个数据传输过程的安全性,实现安全传输,就要通过相应的加密算法实现。DES 利用前面说过的 3 个步骤实现了平台的跨越性,并将 C 语言作为其加密语言,RAS 的安全传输功能主要就是在发送和接收的过程中设定 TCP 传输协议,同时生成可以跨越平台使用的代码。

5 结语

综上所述,DES 和 RAS 作为两种较为常用的加密算法各有优缺点,在实际的加密过程中,可以将两者的优点结合起来,形成一种真正实现大数据信息传输的安全、高效、快捷的混合加密体制,为互联网和大数据的广泛应用提供安全的环境。

[参考文献]

[1] 杨以光,于会智.基于 AES 和 RSA 加密的数据安全传输技术[J].电脑知识与技术,2006(8):84-86.
[2] 佟晓筠,王蠡,郭长勇,等.基于 RSA 等算法软件加密技术的研究与实现[J].微处理机,2003(6):22-25.
[3] 张乐乐.数字签名加密技术的改进方案[J].科技资讯,2009(9):23-23.
[4] 王印明,李阳.一种基于 DES,RSA 的随机加密算法[J].计算机技术与发展,2012(4):235-237.
[5] 佟晓筠,王蠡,杜宇,等.基于软件安全混合加密技术研究[J].计算机工程,2004(23):98-100.
[6] 杜效伟.基于 AES 和 RSA 的数据加密技术方案[J].许昌学院学报,2008(2):80-84.
[7] 杨超.数据加密技术在计算机网络信息安全中的应用[J].中国科技信息,2021(7):46-47.
[8] 史文强,张劲松,牟春苗.基于 WiFi 的数据加密传输系统设计[J].信息与电脑,2021(22):179-181.
[9] 窦立莉.加密技术及典型加密算法[J].硅谷,2009(23):118.
[10] 耿欣月.基于 DES 算法的文件加密研究[J].信息与电脑,2020(3):44-46.

(编辑 傅金睿)

Research on algorithms of big data encryption and transmission technology based on DES and RSA encryption technology

Zhang Le
(Zhongshan Vocational College, Nanjing 210049, China)

Abstract: In recent years, with the continuous development of science and technology, some network security incidents occur frequently, people's requirements for network information security are becoming higher and higher, so data encryption technology is widely used in all walks of life to protect some business information and data. DES and RSA encryption technologies are widely used at present. DES algorithm has the advantages of high speed, but its security, reliability and key stability are low, which can not meet the current security requirements of data encryption technology. Although RSA algorithm has good security, its operation speed is slow, mainly because the length of its key is not fixed. In view of the advantages and disadvantages of both, some research institutions put forward the combination of DES encryption technology and RSA encryption technology to innovate a new encryption technology. Next, this paper will carry out detailed research and discussion on the algorithm of this comprehensive encryption technology.

Key words: DES encryption technology; RSA encryption technology; big data encryption transmission technology; algorithm research