一种改进的对称密钥动态生成算法及应用①

付永贵，马尚才

(山西财经大学 信息管理学院，太原 030006)

摘 要：针对目前对称加密算法对称密钥传输不安全的现状，提出了基于初始密钥和动态密钥合成函数矩阵的改进密钥生成算法，在不牺牲计算速度的前提下有效地实现了密钥传输的安全性。最后，通过实例说明了这一改进的对称密钥动态生成算法的实现模式和实现过程。本研究结论是这种改进的对称密钥动态生成算法原理简单，效率高，适于加密领域作进一步的研究和推广使用。

关键词：动态密钥生成算法；对称密钥；初始密钥；合成密钥；密钥合成函数矩阵

Improved Dynamic Generation Algorithm of Symmetric Key and Its Application

FU Yong-Gui, MA Shang-Cai

(College of Information Management, Shanxi University of Finance and Economics, Taiyuan 030006, China)

Abstract: The text aim the currently unsafe transport situation of the symmetric key of symmetric encryption algorithm, presenting the improved key generation algorithm based on the initial keys and key synthesis function matrix.premising the key transmission security effectively without sacrificing computing speed. Finally, the text illustrates the implementation model and implementation process of this improvement dynamic generated symmetric of symmetric key by an example. The text study conclusion is this improved symmetric key dynamic generation algorithm principle is simple, efficiency is high, suitable for the field of encryption research and extension for further use.

Keywords: dynamic key generation algorithm; symmetric key; initial key; synthesis key; key synthesis function matrix

1 引言

随着信息技术的飞速发展，网络已经成为人们生活不可或缺的一个组成部分，网络攻击技术的不断提高也给网络系统中信息的安全有效传输、存储和处理提出了更高的要求。目前针对信息安全问题解决的方案很多，其中密码技术是技术体系比较完善也使用相对广泛的一种信息安全技术。密码技术大致可以分为对称加密技术和非对称加密技术两类，这两类加密技术各有优劣。对称加密技术要求加密者和解密者之间有一条安全的密钥传输通道，缺点是这条传输通道所传输的密钥经常被捕获。非对称加密技术加解密采用不同的密钥，缺点是这种加密技术密钥太长，不适合长的传输报文的加密。

针对对称加密技术密钥传输的不安全性学者们提出了多种解决方案。本人查阅了大量的中外文文献资料，对国内外有关对称加密算法的研究进行了分析、总结，发现学者们提出的对称加密算法改进思路一定程度上虽然能够提高密钥传输的安全性，但是以牺牲计算速度和存储效率为代价的，并且由于其运算模式比较固定，一定程度上其安全隐患仍然很高。据此本人提出了基于初始密钥和动态运算函数矩阵来合成密钥的改进思路，在不牺牲计算速度的前提下大大提高了对称密钥传输的安全性，截止发文前，本人搜索了大量相关的网络数字文献资料，尚未发现有类似本文所提及的对称密钥改进算法研究的。

① 收稿时间:2010-10-07;收到修改稿时间:2010-11-16

2　目前通用的信息加密模式

鉴于对称加密算法和非对称加密算法各自的优缺点，目前的加密体制一般是采用对称加密密钥对发送的报文进行加密，非对称加密算法对对称密钥进行加密后由发送方向接收方分批传输的模式，非对称加密算法主要是 RSA 加密算法。其加密原理如图 1 所示。

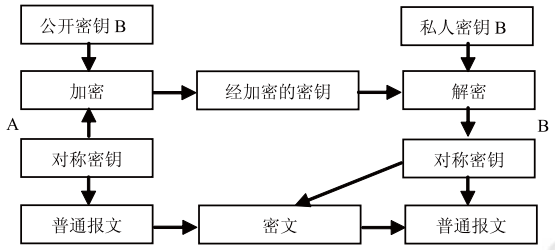

图 1　目前通用的信息加密模式[1]

其加密原理是：

（1）发送方 A 使用对称加密算法对普通报文进行加密得到密文，然后将密文传输给 B。

（2）发送方 A 使用接收方的公开密钥对对称密钥进行加密，得到加密后的密钥，通过一条密钥传输通道传输给 B。

（3）接收方 B 使用自己的私人密钥 B 对 A 传输过来的经加密的密钥进行解密，获得对称密钥。

（4)接收方 B 使用解密后的对称密钥对密文进行解密，获得普通报文。

从以上模式来看，对称密钥固定，没有通过动态的生成算法来生成，而且对称密钥一次全部由安全传输通道传输，网络安全攻击者如果经过长时间的搜索分析很容易获得对称密钥。

3　改进对称密钥生成算法的加密模式

基于以上分析，在参阅了大量的文献资料和多年教学研究的基础上[2-6]，本人提出基于初始密钥和动态密钥合成函数的对称密钥生成算法：由发送方和接收方各自生成一个初始密钥(为了表述方便起见，本文假设初始密钥是一随机数，这种假设对本文算法改进的研究没有任何影响)，收发双方共享一个密钥合成函数矩阵，由接收方从这一函数矩阵中选定一密钥生成函数对两个初始密钥进行函数运算，生成一个合成密钥，这一合成密钥就是最终加密报文的密钥，其改进思路如下：

（1）在发送方 A 与接收方 B 之间建立一个大的密钥合成函数矩阵 P，这一矩阵 P 由 A，B 共享。同时针对不同的接收方 $B_{甲}$和 $B_{乙}$，发送方将有不同的密钥合成函数矩阵 $P_{甲}$和 $P_{乙}$。

$$P=\begin{pmatrix} f_{00} & f_{01} & \cdots\cdots & f_{09} \\ f_{10} & f_{11} & \cdots\cdots & f_{19} \\ \cdots\cdots & & & \\ f_{90} & f_{91} & \cdots\cdots & f_{99} \end{pmatrix}$$

（2）发送方 A 与接收方 B 建立通信连接，首先由接收方 B 生成一大的随机数 X，这一随机数 X 中将包含 B 生成的初始密钥 X0 以及 B 从函数矩阵 P 中选取的密钥合成函数 f_{ij}（i,j 由 B 选取，且 i=0,1,…,9；j=0,1,…,9）的相关信息 X_1；B 使用 A 的公开密钥 $Key(A_0)$对 X 进行加密得到 X 密，通过密钥传输通道传给 A。

（3）发送方 A 接收到 X 密后使用自己的私人密钥 $Key(A_1)$对 $X_{密}$解密后得到 X，从中提取出 X0 和 X_1，由 X_1 找到密钥合成函数矩阵 P 中对应的函数 fij，然后 A 生成另一随机数 Y，这一随机数 Y 作为 A 生成的初始密钥 Y，A 使用 X_0 与 Y 做函数运算 f_{ij} 得到合成密钥 K，即 $K=f_{ij}(X_0,Y)$。

（4）发送方 A 使用 K 对报文 T 进行加密得到 T 密，将这一加密报文 $T_{密}$传输给 B。同时使用 B 的公开密钥 $Key(B_0)$对 Y 进行加密得到 $Y_{密}$，通过密钥传输通道传给 B。

（5）接收方 B 接收到 $T_{密}$和 $Y_{密}$后，使用自己的私有密钥 $Key(B_1)$对 $Y_{密}$解密后得到 Y，从自己的密钥合成函数矩阵 P 中找到 f_{ij}，将 X_0 与 Y 做函数运算 f_{ij} 得到合成密钥 $K=f_{ij}(X_0,Y)$，使用 K 对 T 密进行解密得到报文 T。

其加密原理如图 2 所示。

从图 2 中可以看出发送方和接收方各生成一大的随机数，初始密钥由双方共同决定，密钥合成算法由接收方选择，这样攻击者一般很难同时捕获到两个初始密钥，而且密钥合成函数并不在安全通道上传输，攻击者即使捕获到两个初始密钥也无法计算出合成密钥。在改进对称密钥生成算法中发送方对应不同的接收方将有不同的密钥合成函数矩阵，即使某一接收方泄露了自己的密钥合成函数矩阵和加密机理也并不影响发送方与其他的接收方进行安全的信息传输。

改进的对称密钥动态生成算法从流程上相对于目前通用的信息加密模式来说增加了一次接收方向发送

方发送初始密钥的过程及这一初始密钥的加解密过程，但由于密钥传输时间相对于整个加解密过程可以忽略不计，而且对初始密钥使用非对称加密算法进行加解密时间相对于长传输报文的加解密来说也可以忽略不计，所以改进的对称密钥动态生成算法从时间上来说几乎没有什么增加，这一时间的增长几乎为零。改进的对称密钥动态生成算法相对于目前通用的信息加密模式来说只是增加了合成密钥生成算法可选择的范围，而合成密钥的算法可以通过软件来实现，对计算机性能不会有额外的要求，所以从物理空间的角度这一改进的对称密钥动态生成算法对系统的要求也没有什么额外的增加。

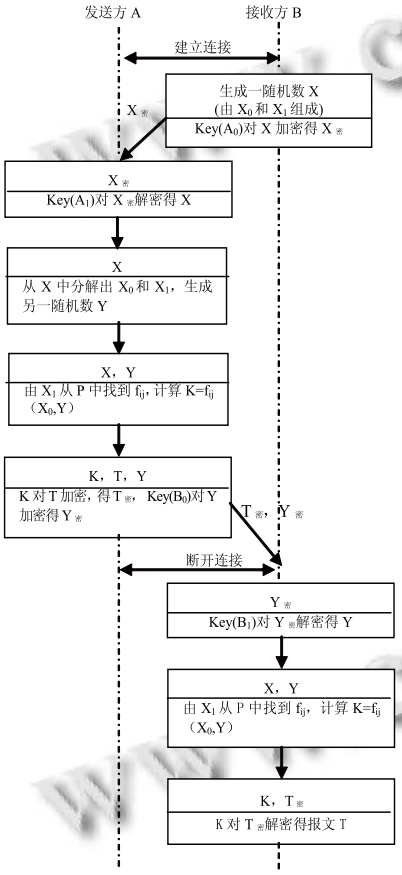

图 2 改进对称密钥生成算法加密原理图

4 实例分析

军事指挥作战系统是对信息传输、存储的安全性要求非常高的一个系统，该系统在指挥作战时要求信息传输的绝对安全性和保密性。传统的信息加密技术由于密钥生成的固定化，密钥传输方式直接性显然不能满足这一系统的信息传输要求。假设一个军事指挥作战系统由 1 个作战总部和 N 个作战指挥基点及相应的作战设备和网络信息传输设备等组成，现绘出其系统模拟结构图如图 3 所示。

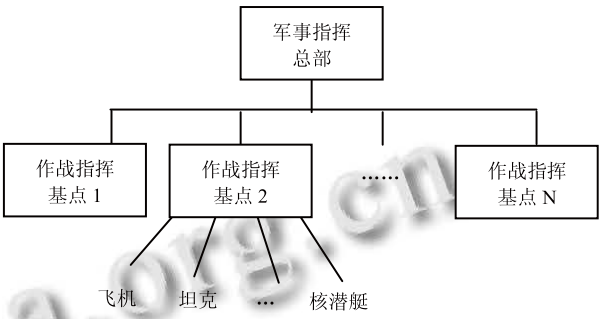

图 3 军事指挥作战系统模拟结构图

下面使用本文改进对称密钥生成算法实现军事指挥作战系统信息的安全加密和密钥的安全传输。本文以下使用的数据均是模拟数据，这里所用的模拟数据对问题的分析与真实数据没有任何区别。设军事指挥总部为 A，各作战指挥基点为 B_1，B_2，…，B_N，A 与 B_1 之间的密钥合成函数矩阵为 P_{B1}，A 与 B_2 之间的密钥合成函数矩阵为 P_{B2}，且：

$$P_{B1}=\begin{pmatrix} f_{00/B1} & f_{01/B1} & \cdots\cdots & f_{09/B1} \\ f_{10/B1} & f_{11/B1} & \cdots\cdots & f_{19/B1} \\ \cdots\cdots & & & \\ f_{90/B1} & f_{91/B1} & \cdots\cdots & f_{99/B1} \end{pmatrix}$$

$$P_{B2}=\begin{pmatrix} f_{00/B2} & f_{01/B2} & \cdots\cdots & f_{09/B2} \\ f_{10/B2} & f_{11/B2} & \cdots\cdots & f_{19/B2} \\ \cdots\cdots & & & \\ f_{90/B2} & f_{91/B2} & \cdots\cdots & f_{99/B2} \end{pmatrix}$$

（1）若 A 要向 B1 发送信息，则 B_1 先向 A 发送一个大的随机数 X，设 X 取 128bit(X_0)+8bit(X_1)。为了便于理解，这里把 $X_{0/B1}$ 每八位记为一段，转化成十进制记为 $K_{00/B1}$,$K_{01/B1}$,K02/B1,K03/B1,K10/B1,K11/B1,$K_{12/B1}$,$K_{13/B1}$,$K_{20/B1}$,$K_{21/B1}$,$K_{22/B1}$,$K_{23/B1}$,$K_{30/B1}$,$K_{31/B1}$,$K_{32/B1}$,$K_{33/B1}$，每一段的取值为 0-255，用矩阵作记并设初值，记做：

$$X_{0/B1}=\begin{pmatrix} K_{00/B1} & K_{01/B1} & K_{02/B1} & K_{03/B1} \\ K_{10/B1} & K_{11/B1} & K_{12/B1} & K_{13/B1} \\ K_{20/B1} & K_{21/B1} & K_{22/B1} & K_{23/B1} \\ K_{30/B1} & K_{31/B1} & K_{32/B1} & K_{33/B1} \end{pmatrix}=\begin{pmatrix} 191 & 131 & 101 & 63 \\ 115 & 144 & 25 & 101 \\ 127 & 210 & 140 & 31 \\ 12 & 130 & 147 & 58 \end{pmatrix}$$

$X_{1/B1}$ 的 8bit 分成两部分，前四位记做 i,后四位记

做 j,也分别转化为十进制位，并且 i,j 取值为 0-9。设 $X_{1/B1}$=00110101，则 i=3，j=5,对应 PB1 中的加密函数为 f35/B1。

（2）A 接收到 B 发送过来的随机数 X 以后，按照相应的规则将其拆分成 $X_{0/B1}$ 和 $X_{1/B1}$，通过 $X_{1/B1}$ 从自己的 P_{B1} 密钥合成函数矩阵中找到相应的密钥合成函数 $f_{35/B1}$，然后自己生成另一 128bit 的随机数 Y，赋初值记做：

$$Y=\begin{pmatrix} K_{00/Y} & K_{01/Y} & K_{02/Y} & K_{03/Y} \\ K_{10/Y} & K_{11/Y} & K_{12/Y} & K_{13/Y} \\ K_{20/Y} & K_{21/Y} & K_{22/Y} & K_{23/Y} \\ K_{30/Y} & K_{31/Y} & K_{32/Y} & K_{33/Y} \end{pmatrix}=\begin{pmatrix} 63 & 211 & 138 & 68 \\ 109 & 23 & 25 & 141 \\ 240 & 208 & 112 & 1 \\ 77 & 105 & 149 & 81 \end{pmatrix}$$

设 $f_{35/B1}$ 函数运算关系是对 $X_{0/B1}$ 和 Y 按位做逻辑异或(⊕)运算，则合成密钥 $K=f_{35/B1}(X_{0/B1},Y)=X_{0/B1}\oplus Y$。其运算过程为：$K=f_{35/B1}(X_{0/B1},Y)=$

$$\begin{pmatrix} 191 & 131 & 101 & 63 \\ 115 & 144 & 25 & 101 \\ 127 & 210 & 140 & 31 \\ 12 & 130 & 147 & 58 \end{pmatrix}\oplus\begin{pmatrix} 63 & 211 & 138 & 68 \\ 109 & 23 & 25 & 141 \\ 240 & 208 & 112 & 1 \\ 77 & 105 & 149 & 81 \end{pmatrix}=\begin{pmatrix} 128 & 80 & 239 & 123 \\ 30 & 135 & 0 & 232 \\ 143 & 2 & 252 & 30 \\ 65 & 235 & 6 & 107 \end{pmatrix}$$

如果 B_2 基点捕获到 A 发送给 B_1 的随机数 Y 及 B_1 发送给 A 的随机数 X，通过 X 从自己与 A 共享的密钥合成函数矩阵 P_{B2} 中找到对应的密钥合成函数 $f_{35/B2}$，由于 $f_{35/B1}$ 与 $f_{35/B2}$ 有不同的函数运算关系，其运算结果将大不相同。设 $f_{35/B2}$ 的函数运算关系为先对 X_0 中的第 0-3 行左循环移位，移动的位数分别为 0-3 字节（其运算关系记做 LR），然后与 Y 按位做逻辑取与（∧）运算，则合成密钥 $K'=f_{35/B2}(X_{0/B1},Y)=(LR(X_{0/B1}))\wedge Y$。其运算过程为：$K'=f_{35/B2}(X_{0/B1},Y)=$

$$\begin{pmatrix} 191 & 131 & 101 & 63 \\ 115 & 144 & 25 & 101 \\ 127 & 210 & 140 & 31 \\ 12 & 130 & 147 & 58 \end{pmatrix}\wedge\begin{pmatrix} 63 & 211 & 138 & 68 \\ 109 & 23 & 25 & 141 \\ 240 & 208 & 112 & 1 \\ 77 & 105 & 149 & 81 \end{pmatrix}$$

先循环左移 1 字节

先循环左移 2 字节

先循环左移 3 字节

$$=\begin{pmatrix} 63 & 131 & 0 & 4 \\ 101 & 19 & 16 & 9 \\ 128 & 16 & 112 & 0 \\ 0 & 1 & 16 & 0 \end{pmatrix}$$

从以上运算结果来看明显 K≠K'，从中也说明 B2 基点无法获得 A 传输给 B1 基点的对称密钥。

从以上实例可以看出，将改进的对称密钥生成算法运用到军事指挥作战系统将会大大提高密钥传输和保管的安全性，在整个运算过程中军事指挥总部与各指挥作战基点双方都产生了随机的初始密钥，而且初始密钥的传输是分开进行的，而真正的合成密钥和密钥合成函数并未在安全通道进行传输，针对不同的指挥作战基点军事指挥总部和各基点有不同的共享密钥合成函数矩阵，这就确保即使某一指挥作战基点捕获了另一基点的初始密钥信息也并不能得到其真正的合成密钥，这进一步提高了军事指挥作战系统各个指挥作战基点之间作战信息的相互保密性。

5　结语

目前对称加密技术的研究已经很多，但大多都是以牺牲加密计算速度和存储效率为代价的，比如通过改进加密算法，使加密算法复杂化或者委托多个可信方管理密钥等等。本人在阅读大量的文献资料，加之多年教学经验的基础上提出了由发送方和接收方各生成一初始密钥由共享密钥合成函数矩阵中选取一密钥合成函数将两初始密钥合成一合成密钥的构想，在不牺牲加密计算速度的情况下一定程度上提高了密钥传输的安全性。目前该算法的实现还需要相应的管理体系和技术支持，本人将在以后不断地进行相应的研究。

参考文献

1 邵兵家.电子商务概论.第 2 版.北京:高等教育出版社,2006.224–226.

2 吴素研,李瑛,胡祥义,杜丽萍.基于组合对称密钥带加密数字签名方法的研究.电子科技大学学报,2009,38(11):76–78.

3 Daitt PAK, Hong CS. A resource-optimal key predistribution scheme with enhanced security for wireless sensor networks. Management of convergence networks and services, LNCS 4238, 2006: 546–549.

4 冯登国,赵险峰.信息安全技术概论.北京:电子工业出版社,2009.20–36.

5 刘颖.密钥管理基础设施中的非对称密钥管理系统设计[硕士学位论文].上海:上海交通大学,2008.

6 Barford P, Yegneswaran V. An inside look at botnets. Advances in Information Security-Malware Detection. Berlin, Germany: Springer-Verlag, 2007:171–191.