基于 RSA 的随机加密算法与安全可靠度分析

赵泽茂

(河海大学常州校区计算机及信息工程学院,江苏 常州 213022)

摘要:引入奇、偶扩展明文的概念,给出基于 RSA 的随机加密算法;给出加密安全空间、安全可靠度等定义,得出了保密安全特性的一些基本结论.

关键词:DES;RSA;加密;解密;密钥;随机比特;信息扩展率;安全可靠度

中图分类号:TP393.08 文献标识码:A 文章编号:1000-1980(2002)04-0075-03

公开密钥密码体制的主要思想是加密算法、加密密钥公开,解密密钥保密,这样便于网络通信.要破译密码依赖于解密密钥,是否能找到解密密钥又取决于大素数的分解理论等一些数学难题,正因为一些数学难题尚未解决从而达到保密之目的.因此基于公钥密码思想的 RSA 倍受密码研究者的重视,但随之而来的却是各种攻击,RSA 体制受到挑战,安全性受到威胁.随着公钥体制的一些缺点开始暴露并受到攻击,S Goldwasser 和 S Micali[1] 设计了新的加密方案——概率加密方案,首次将随机比特应用于公钥密码体制.但他们的概率加密方案是建立在‘不可逼近陷门谓词’的基础上的,每传送 1bit 密文需传送 400 ~ 500 bit 密文,信息扩展率太大,实际中几乎不可能应用.以后 Blum M[2] 应用一次一密的思想提出一种信息扩展率为 $1-\delta$ 的概率加密方案,He J[3] 改进了这一体制,给出一种新方法,但这类体制借助于序列密码的思想,仅仅在每次传送密文的同时传送密钥种子,因而其安全性无法证明.刘花云等[4] 提出了一种基于 RSA 的概率加密,利用随机比特来填充明文,但要求通信双方需要秘密约定随机比特填充的位置.本文根据随机比特填充的思想,对明文在奇、偶位置填充随机比特,形成扩展明文,再应用 RSA 密码体制进行加解密,并进行了理论上的分析.同时引入保密安全可靠度的概念,对加密算法的可靠度进行了较详细的讨论.

1 随机加密算法

定义 1 RSA 体制中,m 比特明文记为:$p=(p_1,p_2,\cdots,p_m)$,其中 $p_i=0$ 或 1,$i=1,2,\cdots,m$,随机产生 m 个比特 $q_i=0$ 或 1,把随机比特 q_i 与 p_i 配对,q_i 在前,p_i 在后,形成一个新的明文,称这个过程为奇比特明文填充,所产生的明文称为奇扩展明文,记为 $p_{odd}=(q_1,p_1,\cdots,q_m,p_m)$ 如果把 p_i 排在前,q_i 排在后,则称为偶比特明文填充,所产生的明文称为偶扩展明文,记为 $p_{even}=(p_1,q_1,\cdots,p_m,q_m)$.

随机加密算法步骤:设通信双方为 A 和 B,A 要向 B 发送明文 M,先把 M 分组,使每组比特数为 m.为叙述方便,以下约定每次发送的明文是一比特流,即 0,1 符号串,发送的数据包每组含比特数目仍为 M.

a. 根据双方约定,在明文 M 上作奇比特填充,生成 $2m$ 比特的扩展明文 M'.

b. A 用 B 的公钥 e 加密 M',生成密文 **C**:$\mathbf{C}=(M')^e \bmod(N)$,$A$ 将密文 **C** 发送给 B.

c. B 接收到密文 **C**,用其密钥解密:$M'=C^d \bmod(N)$,得到扩展明文 M',然后再根据约定去掉奇数位置上的随机比特,得到真正的明文 M.

由于随机加密算法是针对 0,1 符号串进行的,在应用 RSA 进行模运算时视作二进制数进行处理,接受方收到扩展明文后,还需进行再解密才可以恢复真正的明文.因此在网络通信中,基于 RSA 的加密本身就有相当的难度.

这种算法具有明显的缺点:随机比特在明文中填充,使得需要传输的比特流增加,信息扩展率达到 1/2,因而影响了信息的传输速率,信息传输速度慢.不过基于 RSA 的算法慢的主要原因是需要大量的模乘运算,

收稿日期:2001-05-18

作者简介:赵泽茂(1965—),男,四川蓬溪人,副教授,硕士,从事数据挖掘、视景可视化及密码学研究.

而随机比特填充加密算法主要用于身份验证、数字签名等,由于基于 RSA 的身份验证、数字签名等的模乘运算比较少,速度较快,也是可以接受的.

2 安全可靠度分析

引入衡量、评价加密算法安全性或者说可靠性的量化指标,用以刻画加密算法的安全性程度,抗攻击的可靠性强度,旨在从量化方面探索评价网络安全的数学模型,对其可靠性进行精确描述.

要刻画公钥密码体制加密算法的安全性程度,涉及到该算法本身的破译难度、遭到攻击的次数,即攻击的组织或人数、公开通信的时间长短、密钥的保密安全系数大小等.以下讨论问题不是从攻击密码算法本身进行技术细节来分析,而是从概率的观点来试图分析加密算法的可靠度.为此,作如下假定并引入有关定义.

记号约定:加密算法集合 $\mathbf{E}=\{E_1,E_2,\cdots,E_a\}$,敌手集合为 $\mathbf{S}=\{S_1,S_2,\cdots,S_r\}$,假定敌手相互独立地破译,互不影响,且敌手的元素个数 $|\mathbf{S}|=r$,比特数目为 num 的明文记为 M^{num},加密后的密文记为 C^{num},通信的特定时间范围记为 T^t,设密钥绝对安全.

定义 2 称集合 $\mathbf{SA}=\{E_j,C^{num},T^t,S_i\}$ 为加密安全空间,用以表示明文 M^{num} 采用加密算法 E_j 得到密文 C^{num},时间范围为 T^t,攻击手为 S_i 形成的集合.

定义 3 设加密安全空间为 $\mathbf{SA}=\{E_j,C^{num},T^t,S_i\}$,如果被 S_i 攻破的概率为 $1-p_i^{(j)}$,则称该加密算法 E_j 在这一特定时间段 T^t 内,密文 C^{num} 相对于该敌手的安全可靠度为 $p_i^{(j)}$.

定义 4 设敌手集合为 $\mathbf{S}=\{S_1,S_2,\cdots,S_r\}$,又称为攻击群体 S,在某一种加密算法 E_j 下,若一定比特数目的密文 C^{num} 在特定时间段 T^t 内相对于敌手 S_i 的安全可靠度为 $p_i^{(j)}$,称 $p^s_{(j)}=\min\limits_{1\leqslant i\leqslant r}p_i^{(j)}$ 为该加密算法 E_j 在特定时间段 T^t 内,密文 C^{num} 相对于攻击群体 S 的安全可靠度;若密文的比特数为任意长度,其余条件不变,设相应的安全可靠度与密文比特数的长度成反比,密文 C 相对于攻击群体 S 的安全可靠度为 $p^{cs}_{(j)}=k_c^j p^s_{(j)}$,其中的比例系数 k_c^j 称为文本比例系数.

定义 5 在定义4的条件下,设加密安全空间 $\mathbf{SA}=\{E_j,\mathbf{C},\mathbf{T},\mathbf{S}\}$,该系统的安全可靠度与保密时间的长短成反比,其可靠度定义为 $p^{tcs}_{(j)}=k_t^j p^{cs}_{(j)}$,其中的比例系数 k_t^j 称为时间比例系数.

定义 6 设加密安全空间 $\mathbf{SA}=\{\mathbf{E},\mathbf{C},\mathbf{T},\mathbf{S}\}$,加密采用各算法的概率为 $p(E_j)=p_j^0$,且 $\sum\limits_{j=1}^{a}p_j^0=1$,则该系统的安全可靠度定义为 $p^{etcs}=\sum\limits_{j=1}^{a}p_j^0p^{tcs}_{(j)}$.

引理 1 若敌手集合 $\mathbf{S}^{(1)}\subset\mathbf{S}^{(2)}$,则密文 C^{num} 相对于 $\mathbf{S}^{(1)}$ 的安全可靠度 $p^{(1)}\geqslant$ $\mathbf{S}^{(2)}$ 的安全可靠度 $p^{(2)}$.

证明 设 $|\mathbf{S}^{(1)}|=r^{(1)}$,$|\mathbf{S}^{(2)}|=r^{(2)}$,

因为 $p^1=\min\limits_{1\leqslant i\leqslant r^{(1)}}p_i$,$p^{(2)}=\min\limits_{1\leqslant i\leqslant r^{(2)}}p_i$ 且 $r^{(1)}\leqslant r^{(2)}$

所以 $p^{(1)}\geqslant p^{(2)}$

引理2 若对同一明文加密得密文 C^{num1} 的长度 $num1\leqslant$ 密文 C^{num2} 的长度 $num2$,则密文 C_2^{num2} 相对敌手 S_i 的安全可靠度 $p^{(2)}\geqslant$ 密文 C_1^{num1} 相对于敌手 S_i 的安全可靠度 $p^{(1)}$.

引理 3 设加密安全空间 $\mathbf{SA}_k=\{E_j,C^{num},T^k,S_i\}$,$k=1,2$,满足条件 $T^1\leqslant T^2$,则密文 C^{num} 相对于敌手 S_i 的安全可靠度 $p^{(1)}\geqslant p^{(2)}$.

定理 1 对一般加密安全空间 $\mathbf{SA}=\{\mathbf{E},\mathbf{C},\mathbf{T},\mathbf{S}\}$,其中集合 E 为加密算法,C 为密文集合,T 为时间集合,S 为敌手集合,则安全可靠度 p^{etcs} 与 S,T 成反比,与 E,C 成正比.

证明 由定义 2 ~ 6 及引理 1 ~ 3 得 $p^{etcs}=\sum\limits_{j=1}^{a}p_j^0k_t^jk_c^j\min\limits_{1\leqslant i\leqslant r}p_i^{(j)}$,易说明定理之结论成立.

定理 2 设加密算法采用 RSA,公开(e,N),大素数 p,q,私钥 d 保密,为叙述方便,仍用 E_j 表示该算法,此时加密安全空间 $\mathbf{SA}=\{E_j,\mathbf{C},\mathbf{T},\mathbf{S}\}$,设基于大数分解的模余运算寻找解密密钥是随机进行的,解密密钥的个数为有限个,记为 $\mathbf{d}=\{d_1,d_2,\cdots,d_b\}$,且 $p(d_l)=1/b$,$l=1,2,\cdots,b$,则安全可靠度为 $p^{tcs}_{(j)}\approx k_t^jk_c^j(1-1/b)^r$ 且当 $r\neq b$ 时,$\lim\limits_{r\to+\infty}p^{tcs}_{(j)}=0$.

证明　根据题意不妨假设每位敌手 S_i 破译的概率均为 $p(d_l)=1/b$，r 位敌手均不能破译的概率为 $p=p(\bigcap_{i=1}^{r}\bar{s}_i)=(1-1/b)^r$，考虑到密文的大小及时间的长短对安全可靠度的影响，按上述思想题设，安全空间的可靠度 $p_{(j)}^{tcs}\approx k_l^j k_c^j(1-1/b)^r$.

因为 $0<1-1/b<1$，所以当 $r\neq b$ 时，$\lim\limits_{r\to+\infty}(1-1/b)^r=0$，从而 $\lim\limits_{r\to+\infty}p_{(j)}^{tcs}=0$.

3　结　　语

本文首先将随机比特流填充明文形成扩展明文再进行加密，无疑增加了破译的难度，增强了抗攻击的能力，提高了保密安全可靠度，虽然扩展明文影响了信息的传输速率，不过基于 RSA 的身份验证、数字签名等，是可以接受的. 其次，引入衡量、评价加密算法安全性的安全可靠度定义，用以刻画加密算法的安全性程度，从敌手数量、时间长短、密文文本大小、算法策略等方面刻画加密安全空间，并得出一些反映保密安全特性的量化结论. 尽管这些探索是初步的，但从数学公理化、安全理论基础研究的角度进行分析是值得的.

参考文献：

[1] Goldwasser S, Micali S. Probabilistic encryption[J]. Journal of Computer and System Science, 1994, 28: 270 ~ 299.

[2] Blum M, Goldwasser S. An efficient probabilistic public-key encryption scheme which hides all partial information[A]. In: Blakley G R, Chaum D, eds. Advances in Cryptology: Proceedings of CRYPTO 84, Volume 196 of Lecture Notes in Computer Science[C]. New York: Springer-Verlag, 1985. 289 ~ 299.

[3] HE Jing-min, LU Kai-cheng. A new probabilistic encryption scheme[A]. In: Christoph G Günther, eds. Advances in Cryptology: EUROCRYPT 88, Volume 330 of Lecture Notes in Computer Science[C]. Heidelberg: Springer-Verlag, 1988. 415 ~ 418.

[4] 刘花云，罗静，胡子濮. 基于 RSA 的概率加密[J]. 西安电子科技大学学报，1997，24(4): 554 ~ 559.

RSA-based random encryption algorithm and analysis of its dependability

ZHAO Ze-mao

(*College of Computer & Information, Hohai Univ. Changzhou Branch, Changzhou* 213022, *China*)

Abstract: A random encryption algorithm based on RSA is developed by use of the concept of odd and even plaintext expansion. The definitions of encryption security space and security dependability are given to describe the security indexes for the encryption algorithm, and some basic conclusions on cipher security are drawn.

Key words: DES; RSA; encryption; decryption; key to decryption; random bit; ratio of information expansion; security dependability