

一种基于多密码体制的混合加密算法

杨宏宇*, 宁宇光, 王 玥

(中国民航大学 计算机科学与技术学院, 天津 300300)

摘要: 针对混合加密算法构造方法固定的问题, 提出了一种基于 RSA 和 Hill 的多密码体制混合加密算法模型. 首先, 根据生成的一系列随机数分割明文, 将混合加密算法中会话密钥转换为明文的随机分割数, 并使用 RSA 密码对其进行加密. 然后, 改进 Pascal 矩阵生成算法, 用该算法生成的 Pascal 矩阵代替 Hill 密码的密钥对明文加密. 安全性分析和实验结果表明, 该加密算法具有较强的抗攻击性和较好的加密效率.

关键词: 混合加密; 随机分割; 多密码体制; 会话密钥; Pascal

中图分类号: TP309.7

文献标识码: A

doi: 10.7511/dllgxb201801015

0 引言

为解决对称密码密钥配送难和公钥密码加密速度慢的问题, 混合密码系统被提出并且广泛使用. 混合密码系统组成机制包含如下 4 个过程: 用对称密码加密明文、通过伪随机数生成器生成对称密码加密中使用的会话密钥、用公钥密码加密会话密钥、从外部赋予公钥密码加密时使用的密钥^[1].

Shoup^[2]通过提出 KEM-DEM 结构形式化定义了混合加密模型. 但是一些密码体制由于密钥形式或安全性无法依据 KEM-DEM 结构与其他密码构成混合密码, 所以符合该结构的密码体制较少.

基于 RSA 和 Hill 的混合密码构建仍处于探索阶段, 不少研究已经开始将 RSA 与 Hill 两种密码体制配合使用. Rahman 等^[3]提出的 Hill+ 算法通过引入随机矩阵作为密钥增强了 Hill 密码对已知明文攻击的抵抗性. 但是该算法仅对加密矩阵进行了改进, 需要复杂的代数运算. Goel 等^[4]通过在 RSA 密码加密前对明文进行 Hill 加密, 增强了 RSA 密码对暴力攻击的抵抗性. 但该方法没有构造混合密码, 仍存在对称密码密钥配送难和公钥密码加密速度慢的问题. 李文锋^[5]提出了基于有限域矩阵构造技术的 RSA-Sign-Hill

算法, 该算法用生成 Hill 密码加密矩阵时产生的关键数字 l 作为会话密钥, 导致其会话密钥过于单一, 生成加密矩阵算法的代价较高, 无法抵抗已知明文攻击等密码分析手段.

国内外对 Hill 密码的研究重点是对其加密矩阵的改进, 但 Hill 密码属于古典密码, 存在定长分割明文产生哑元、生成加密矩阵时间复杂度两个固有问题. 目前, 针对这两个固有问题的研究已经取得了一定的成果. 刘海峰等^[6-7]通过设定加密矩阵满足行和相等性质解决了哑元问题. 但加密矩阵的约束增加, 导致 Hill 密码密钥空间减小, 其抗攻击性减弱. Putera 等^[8]利用遗传算法改进 Hill 密码的密钥生成, 提高密钥生成速度. 但该方法仍然局限于改进 Hill 密码的加密矩阵.

上述研究并未从本质上提高 Hill 密码的安全性. 针对上述问题, 本文的研究思路是从 Hill 密码加密流程分析入手, 将其规律分割明文转换为随机分割明文, 不再针对 Hill 密码加密矩阵进行改进, 而将其密钥从加密矩阵转换为对明文的随机分割数, 通过加密随机分割数增强 Hill 密码的安全性. 为此, 本文提出明文随机分割的方法, 将 RSA 密码与 Hill 密码融合, 设计 RSA-Hill 混合加密算法. 与以往的混合加密构造方式不同, 本文将会话密钥转换为明文的随机分割数, 用

Pascal 矩阵代替 Hill 密码的密钥隐藏明文信息, 并采用 RSA 密码加密明文随机分割数以保证算法的安全性.

1 多密码体制分析

1.1 问题分析

多密码体制是将两种或两种以上的密码相结合, 并使各密码相互兼容的一种方案. 现已有较为成熟的多密码混合加密方案, 如 DES-RSA^[9]、AES-ECC^[10] 等. 但对于 RSA 和 Hill 密码, 由于 Hill 密码的密钥为随机矩阵, 二者结合难度较大, 根据 KEM-DEM 结构模型, 构建基于 RSA 和 Hill 混合密码存在以下两个难点:

(1) 若基于 RSA 和 Hill 混合加密算法中会话密钥是行列式为 ± 1 的随机矩阵且每一次需要的随机矩阵阶数不固定, 则采用伪随机数生成器无法高效生成会话密钥.

(2) 混合密码体制使用公钥密码加密会话密钥. 若会话密钥是矩阵, 则 RSA 等公钥密码无法加密数据量大且具有结构的会话密钥.

针对上述两个难点, 本文利用明文随机分割方法将 RSA 和 Hill 相结合. 若分割明文的随机数作为会话密钥, 则伪随机数生成器快速、高质量生成会话密钥的同时, 也可使用 RSA 密码对该密钥加密. 该混合加密算法中密钥空间的改变, 实现了一次一密混合密码系统.

1.2 密钥空间分析

Hill 加密算法的密钥空间

$$\mathbf{K}_H = \{ \mathbf{H}_{m \times m} \mid m \in \mathbf{Z}^+, |\mathbf{H}_{m \times m}| = \pm 1 \} \quad (1)$$

设 n 为明文长度, 基于 RSA 和 Hill 混合加密算法的密钥空间

$$K = \left\{ x_1, x_2, \dots, x_l \mid 0 \leq x_m \leq n, \sum_{m=1}^l x_m = n, m \in [1, l], x_m \in \mathbf{Z}^+ \right\} \quad (2)$$

Hill 加密算法中密钥是随机选取的, 但为保证加密矩阵是可逆的且逆矩阵中的元素全部为整数, 使得解密后可以得到正确的明文, 密钥的选取要满足加密矩阵是非退化的且行列式为 ± 1 ^[11]. 对于密钥空间 K , 每一次加密过程中伪随机数生成器可以有效生成随机密钥, 并且可用 RSA 密码对其加密.

由于密钥空间 K 的存在, 可以避免对 Hill 密码中加密矩阵进行改进. 本文选用 Pascal 矩阵代

替 Hill 密码的密钥, Pascal 矩阵的取值空间

$$\mathbf{K}_P = \{ \mathbf{P}_{m \times m} \mid m \in \mathbf{Z}^+ \} \quad (3)$$

根据式(1)、(3)可知, \mathbf{K}_P 是 \mathbf{K}_H 的子集. 若密钥空间减小, Pascal 矩阵则无法作为 Hill 密码的密钥. 但在基于 RSA 和 Hill 混合加密算法中会话密钥不再是 Pascal 矩阵, 而是明文的随机分割数. 使用 Pascal 矩阵代替 Hill 密码的密钥, 其优点是避免了生成加密矩阵时大量复杂的运算^[11], 解决了密钥传输困难等问题. 通过对 Pascal 矩阵生成算法的改进, 可以提高混合密码加解密的速度.

2 Pascal 公式的推广

从实现方法上看, Pascal 公式是依据相邻两行间的关系生成 Pascal 矩阵, 且不局限于逐行生成^[12]. 但 Pascal 公式还可以推广, 得到更一般的形式.

2.1 假设

Pascal 公式的组合意义证明以及由组合意义推导出的一般性公式第 1 步都是在集合 S 中任取 $i (1 \leq i \leq k)$ 个元素, 所以不妨以 S 中选取的元素个数划分 Pascal 公式的阶数.

$$\binom{n}{k} = \binom{n}{k}, \text{ 将其定义为 } 0 \text{ 阶 Pascal 公式;}$$

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}, \text{ 将其定义为 } 1 \text{ 阶}$$

Pascal 公式;

$$\binom{n}{k} = \binom{n-2}{k-2} + 2 \binom{n-2}{k-1} + \binom{n-2}{k}, \text{ 将其定}$$

义为 2 阶 Pascal 公式;

.....

$$\binom{n}{k} = \sum_{t=0}^i \binom{i}{t} \binom{n-i}{k-t}, \text{ 将其定义为 } i \text{ 阶 Pascal}$$

公式.

2.2 i 阶 Pascal 公式证明

i 阶 Pascal 公式为

$$\binom{n}{k} = \sum_{t=0}^i \binom{i}{t} \binom{n-i}{k-t} \quad (4)$$

证明 在 S 中选取 $i (1 \leq i \leq k)$ 个元素 (x_1, x_2, \dots, x_i) , S 的 k -组合的集合划分成 2^i 种集合. 用 1 表示 x_i 在集合中, 用 0 表示 x_i 不在集合中. 所以集合的划分情况如下:

(1) $(0, 0, \dots, 0)$ 说明 i 个元素中没有有一个元素在 S 的 k -组合中, 用 $\binom{n-i}{k}$ 表示集合的大小.

(2)(0,0,⋯,0,1,0,0,⋯,0)说明 i 个元素中只有一个元素在 S 的 k -组合中,而这个元素的选取有 $\binom{i}{1}$ 种可能,所以可以用 $\binom{i}{1}\binom{n-i}{k-1}$ 表示集合的大小.

(3)(1,0,⋯,0,1,⋯,1,0,⋯,0)说明 i 个元素中有 j 个元素在 S 的 k -组合中,而这个元素的选取有 $\binom{i}{j}$ 种可能,所以可以用 $\binom{i}{j}\binom{n-i}{k-j}$ 表示集合的大小.

(4)(1,1,⋯,1)说明 i 个元素全在 S 的 k -组合中,而这个元素的选取有 $\binom{i}{i}$ 种可能,所以可以用 $\binom{i}{i}\binom{n-i}{k-i}$ 表示集合的大小.

综上所述,根据双计数原理可得

$$\binom{n}{k} = \sum_{i=0}^k \binom{i}{t} \binom{n-i}{k-t}$$

2.3 分析

(1)从 1 阶 Pascal 公式到 2 阶 Pascal 公式、3 阶 Pascal 公式、⋯、 i 阶 Pascal 公式中 n 的规模依次减小,当需要生成阶数较大的 Pascal 矩阵时,可以利用相对高阶的 Pascal 公式,以减小运算复杂度.

(2)在生成 Pascal 矩阵时运用 i 阶 Pascal 公式,可以消除行数的限制.即在生成 Pascal 矩阵第 i 行的数据时可以依赖 j ($1 \leq j < i$) 行的数据,使得算法更加灵活,能适应更复杂的运行环境.

(3)在使用 i 阶 Pascal 公式时,由于公式本身取值范围的限制,必须先给出前 i 行数据作为生成所需阶数 Pascal 矩阵的基础.

3 基于 RSA 和 Hill 的混合加密算法

3.1 RSA-Hill 混合加密算法

RSA-Hill 混合加密流程设计如下:

(1)已知明文 M ,对照字符表(如表 1 所示)得到将要加密的数字明文,计算明文长度 n ;

(2)生成一系列随机数 n_1, n_2, \dots, n_k ,且 $n = n_1 + n_2 + \dots + n_k$;

(3)按生成的随机数将明文 M 划分为 M_1, M_2, \dots, M_k ,生成对应的 Pascal 矩阵 P_1, P_2, \dots, P_k ;

(4)明文加密计算 $C_1 = M_1 P_1, C_2 = M_2 P_2, \dots, C_k = M_k P_k$,得到加密后的密文矩阵,将密文矩阵转化为行向量并组合在一起成为最终密文发送到

接收方;

(5)用 RSA 加密算法对随机数加密和传送;

(6)解密时先用 RSA 算法解密随机数,再依据随机数按 Hill 算法解密.

表 1 字符表

Tab. 1 Character table

字符	编码	字符	编码	字符	编码	字符	编码
0	0	g	16	w	32	M	48
1	1	h	17	x	33	N	49
2	2	i	18	y	34	O	50
3	3	j	19	z	35	P	51
4	4	k	20	A	36	Q	52
5	5	l	21	B	37	R	53
6	6	m	22	C	38	S	54
7	7	n	23	D	39	T	55
8	8	o	24	E	40	U	56
9	9	p	25	F	41	V	57
a	10	q	26	G	42	W	58
b	11	r	27	H	43	X	59
c	12	s	28	I	44	Y	60
d	13	t	29	J	45	Z	61
e	14	u	30	K	46	#	62
f	15	v	31	L	47	*	63

3.2 算法分析

根据图 1 可知,计算机在运行 RSA-Hill 混合加密算法时,不再需要生成行列式为 ± 1 的随机矩阵 A ,即 $\det A = \pm 1$,仅需要生成一系列随机数.通过这种方式能提高算法的执行效率和性能,减少计算机系统资源的消耗.

在 RSA-Hill 混合加密算法中,通过满足 $n = n_1 + n_2 + \dots + n_k$ 条件的一系列随机数分割明文,可以避免 Hill 密码中因定长分割明文所产生的哑元问题.同时,由于随机数的个数要少于明文数,并且每一次对明文加密生成的随机数都不一样.从这个角度上讲,该算法实现了一次一密.

3.3 应用实例

(1)对给定明文 M : Attack time at 5 PM,按照表 1 得到数字明文如下:

36 29 29 10 12 20 29 18 22 14
10 29 5 51 48

通过计算可得明文长度 $n = 15$;

(2)生成随机数:4 3 7 1;

(3)用随机数对明文进行划分:

$$M_1 = (36 \ 29 \ 29 \ 10)^T$$

$$M_2 = (12 \ 20 \ 29)^T$$

$$M_3 = (18 \ 22 \ 14 \ 10 \ 29 \ 5 \ 51)^T$$

$$M_4 = (48)^T$$

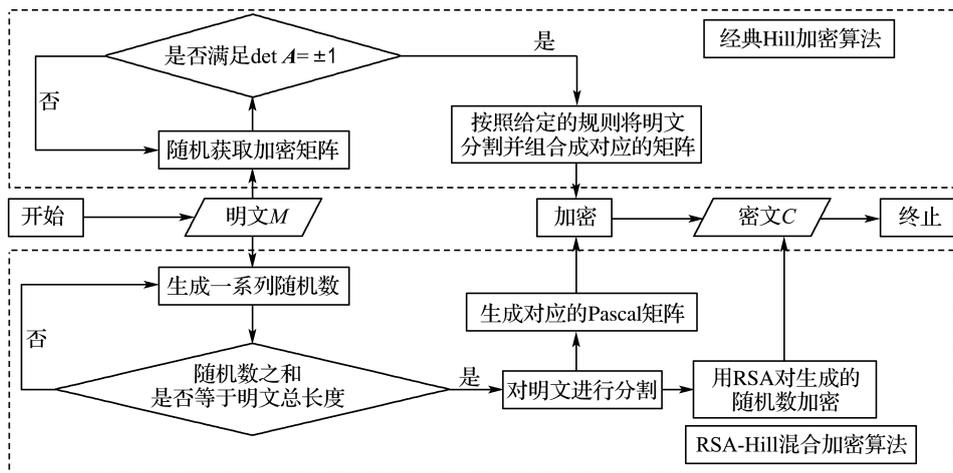


图 1 算法框架图

Fig. 1 Algorithm framework chart

对应生成的 Pascal 矩阵为 P_4, P_3, P_7, P_1 ;

(4)对明文进行加密计算:

$$C_1 = P_4 M_1 = (36 \ 1 \ 59 \ 28)^T$$

$$C_2 = P_3 M_2 = (12 \ 32 \ 17)^T$$

$$C_3 = P_7 M_3 = (18 \ 40 \ 12 \ 8 \ 3 \ 6 \ 52)^T$$

$$C_4 = P_1 M_4 = (48)^T$$

组合生成最终密文:36 1 59 28 12 32 17 18 40 12 8 3 6 52 48,则文字密文为 A1XsewhiEc836QM;

(5)用 RSA 加密体制对随机数加密,相关参数如下: $p=7, q=13, n=p \times q=91, \varphi(n)=(p-1)(q-1)=72, e=17$. 计算得到 $d=17$,加密后的密文为 23 61 63 1.

解密过程为上述过程的逆过程.

4 实验与安全性分析

为验证本文加密算法的性能,在 PC 机上搭建实验环境.(1)硬件配置:Inter Core i3-2350M CPU @ 2.30 GHz,4.0 GB RAM.(2)软件环境:Windows 7 64 位操作系统,Matlab R2010b.

4.1 Pascal 矩阵性能分析

假设明文长度为 n ,字母占 1 B,则明文大小为 n B,生成一系列随机数 n_1, n_2, \dots, n_k ,且满足 $n = n_1 + n_2 + \dots + n_k$. 首先根据明文长度确定 k 值,生成一系列满足上述条件的随机数,然后选择 i 阶 Pascal 公式生成 Pascal 矩阵.由于 Pascal 矩阵的个数等于随机数的个数,Pascal 矩阵的阶数等于随机数的值,所以根据随机数 $n_i (i=1, 2, \dots, k)$ 的值生成与其相等阶数的 k 个 Pascal 矩阵.

在满足 $n = n_1 + n_2 + \dots + n_k$ 的条件下确定 k 值的方法有两种:

方法 1 选择固定个数的随机数;

方法 2 根据明文长度确定随机数个数,如 $k = n^{1/2}$.

上述两种方法对不同明文长度生成其所需 Pascal 矩阵的耗时情况如表 2 所示.当选用方法 1 时, $k=150$;当选用方法 2 时, $k=n^{1/2}$.

表 2 不同明文长度生成 Pascal 矩阵耗时
Tab. 2 Time consuming of generating Pascal matrix with different plaintext sizes

n/KB	t/s	
	$k=150$	$k=n^{1/2}$
1	0.326	0.311
3	1.473	1.515
5	3.496	3.303
7	4.967	4.945
512	7.396	15.136
1 024	9.665	19.763

影响 Pascal 矩阵生成耗时的因素包括:

(1)Pascal 矩阵的个数.因明文长度 n 增加,根据方法 2,随机数的个数相应增加,所以 Pascal 矩阵的个数也会增加.

(2)Pascal 矩阵的阶数.在明文长度 n 确定的情况下,随机数的个数 k 也可确定;若明文长度增加,则 $n_i (i=1, 2, \dots, k)$ 也会增加,即 Pascal 矩阵的阶数越高,生成矩阵所需时间越长.

从表 2 可知,对于较小的文本,为了增加密文的抗攻击性,可选择方法 2 确定 k 值;而对于较大

的文本,为了减少明文的加密时间,可选择方法 1 确定 k 值.

4.2 各算法对不同大小文件加密耗时对比

本实验将 RSA-Hill 混合加密算法与文献 [13] 中提到的 DES、AES、DES-RSA 加密算法对不同大小文件的加密耗时进行对比. 在 Matlab 中实现了 RSA-Hill 混合加密算法对大小为 1、2、3、4 和 10 MB 文件进行加密,根据 4.1 节分析选用方法 1 确定 k 值,即 $k=150$. 记录并统计对不同大小文件的加密耗时,4 种加密算法对不同大小文件的加密耗时如图 2 所示.

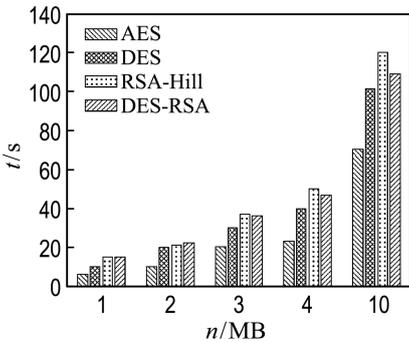


图 2 各算法对不同大小文件的加密耗时对比

Fig. 2 Encryption time consuming comparison of different algorithms for different sizes of files

由图 2 可知,当文件大小不大于 3 MB 时, RSA-Hill 混合加密算法的加密耗时与 DES、DES-RSA 算法差别不大. 当文件大小为 4 MB 时, RSA-Hill 混合加密算法的加密耗时大于 DES、AES 算法,但与 DES-RSA 混合加密算法基本相当. 原因是对于大文件, RSA-Hill 混合加密算法加密所需 Pascal 矩阵的阶数较高,矩阵运算的耗时也会相应较长. 所以 RSA-Hill 混合加密算法适合加密小于 4 MB 的文件.

4.3 攻击实验与安全性分析

本实验主要验证经 RSA-Hill 混合加密算法加密后的密文还原程度. 实验样本为 1 KB 大小的明文, k 值的确定采用 4.1 节的方法 2.

假设攻击者可获得加密后的密文信息,在实验中所设计的攻击步骤如下:

步骤 1 获取加密后的数据块,将其合并为密文向量;

步骤 2 攻击者已知明文是由不同阶数 Pascal 矩阵加密的且明文长度为 n ,但明文的分割信息未知;

步骤 3 根据明文长度,确定 Pascal 矩阵阶数 O 的区间范围;

步骤 4 用该区间范围内的所有 Pascal 矩阵对密文向量尝试解密;

步骤 5 统计还原出的单词数占总单词数的比例 F .

图 3 显示了不同阶数 Pascal 矩阵对明文信息还原的比例. 由图 3 可知,还原明文信息的比例最高接近 4.0%,所以尝试使用不同阶数 Pascal 矩阵破解密文的方案不可行. 但 30 阶 Pascal 矩阵可以还原的明文单词数最多,因为 $n=1\ 024\ \text{B}$, $k=32$,随机分割数中生成 30 的概率要比其他数大,所以用相应逆矩阵解密获得的信息可能会更多. 如果在加密之前对明文向量进行一系列变换,可还原的有效单词数会更少,还原明文的比例会更小. 所以,暴力破解无法有效还原明文.

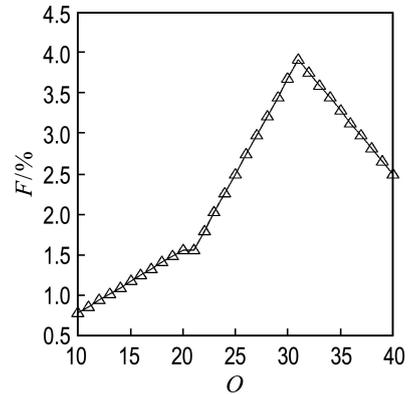


图 3 不同阶数 Pascal 矩阵还原明文的比例

Fig. 3 The percentage of reducing plaintext for different order Pascal matrix

5 结 语

本文提出了一种基于 RSA 和 Hill 的混合加密算法. 通过随机分割明文解决了构建 RSA-Hill 混合加密算法的两个难题. RSA-Hill 混合加密算法不再对 Hill 密码的加密矩阵进行复杂的改进,将会话密钥转换为明文的随机分割数,实现了一次一密的加密流程,避免了哑元的出现. 该混合加密算法具有较强的攻击性和较好的加密效率.

未来的研究重点是对 RSA-Hill 混合密码的安全性进行形式化定义和证明.

参考文献:

[1] 结城浩. 图解密码技术[M]. 周自恒,译. 北京:人

- 民邮电出版社, 2015.
- HIROSHI Yuki. **Graphic Cryptography Technology** [M]. ZHOU Ziheng, trans. Beijing: Posts & Telecom Press, 2015. (in Chinese)
- [2] SHOUP V. A proposal for an ISO standard for public-key encryption (version 2.1) [J]. **International Association for Cryptologic Research**, 2001:1-52.
- [3] RAHMAN M N A, ABIDIN A F A, YUSOF M K, *et al.* Cryptography: A new approach of classical Hill cipher [J]. **International Journal of Security and Its Applications**, 2013, **7**(2):179-190.
- [4] GOEL A S, PUGLIA D, LUNAWAT S, *et al.* Enhancing security by adding Hill cipher to modified RSA algorithm [J]. **International Journal of Applied Engineering Research**, 2014, **9**(9):1053-1061.
- [5] 李文锋. 基于 RSA 和 Hill 密码体系的文件加密系统的研究和实现[D]. 赣州: 江西理工大学, 2007.
- LI Wenfeng. The research and implementation of file encryption system based on RSA and Hill cryptosystem [D]. Ganzhou: Jiangxi University of Science and Technology, 2007. (in Chinese)
- [6] 刘海峰, 何立勇, 郭改慧, 等. Hill 密码体系中的加密矩阵与哑元[J]. 西南大学学报(自然科学版), 2014, **36**(11):138-142.
- LIU Haifeng, HE Liyong, GUO Gaihui, *et al.* The dummy and encryption matrix in the Hill coding system [J]. **Journal of Southwest University (Natural Science Edition)**, 2014, **36**(11):138-142. (in Chinese)
- [7] 万福永, 戴浩晖. Hill₂ 密码体系加密过程中的哑元问题[J]. 数学的实践与认识, 2007, **37**(8):87-90.
- WAN Fuyong, DAI Haohui. The design of dummy variable in Hill₂ coding system [J]. **Mathematics in Practice and Theory**, 2007, **37**(8):87-90. (in Chinese)
- [8] PUTERA A, SIAHAAN U, RAHIM ROBLI. Dynamic key matrix of Hill cipher using genetic algorithm [J]. **International Journal of Security and Its Applications**, 2016, **10**(8):173-180.
- [9] 翁云翔. 基于 DES 和 RSA 的混合加密算法研究与设计[J]. 电子设计工程, 2016, **24**(17):42-44, 47.
- WENG Yunxiang. Research and design of hybrid encryption algorithm based on DES and RSA [J]. **Electronic Design Engineering**, 2016, **24**(17):42-44, 47. (in Chinese)
- [10] 刘帅, 王平, 邢建春, 等. 混合加密算法的改进和设计方案[J]. 微型机与应用, 2016, **35**(8):15-17.
- LIU Shuai, WANG Ping, XING Jianchun, *et al.* Improvement and design of hybrid encryption algorithm [J]. **Microcomputer & Its Applications**, 2016, **35**(8):15-17. (in Chinese)
- [11] 王容, 廖群英, 王云莹, 等. Hill 加密算法的改进[J]. 四川师范大学学报(自然科学版), 2015, **38**(1):8-14.
- WANG Rong, LIAO Qunying, WANG Yunying, *et al.* Improvement of Hill encryption algorithm [J]. **Journal of Sichuan Normal University (Natural Science)**, 2015, **38**(1):8-14. (in Chinese)
- [12] BRUALDI R A. **Introductory Combinatorics** [M]. 5th ed. Upper Saddle River: Person Education Inc., 2009.
- [13] 吴明航. DES 和 RSA 混合加密算法的研究[D]. 哈尔滨: 哈尔滨工业大学, 2013.
- WU Minghang. Research on DES and RSA hybrid encryption algorithm [D]. Harbin: Harbin Institute of Technology, 2013. (in Chinese)

A hybrid encryption algorithm based on multi-crypto system

YANG Hongyu*, NING Yuguang, WANG Yue

(College of Computer Science and Technology, Civil Aviation University of China, Tianjin 300300, China)

Abstract: Aiming at the problem that constructing methods in hybrid encryption algorithms are fixed, a multi-crypto system hybrid encryption algorithm model based on RSA and Hill is proposed. Firstly, the plaintext is divided by a series of random numbers which are encrypted by the RSA cipher as a session key in the hybrid encryption algorithm. Then the key of Hill cipher is replaced by Pascal matrix whose generation algorithm has been improved. Security analysis and experimental results show that this encryption algorithm has better encryption efficiency and stronger anti-attack capacity.

Key words: hybrid encryption; random division; multi-crypto system; session key; Pascal