 DOI: https://doi.org/10.12345/bdai.v6i4.30567

Exploration of Hill Encryption Algorithm

Guangbin Jia

Agricultural Science and Technology Park Service Center, Tongchuan District, Dazhou City, Dazhou, Sichuan, 635000, China

Abstract

Various encryption algorithms are constantly emerging, and the Hill cipher is a notable asymmetric encryption algorithm. The Hill cipher essentially treats plaintext as a set of vectors, which are then transformed into ciphertext vectors through linear transformations under modular operations, thereby achieving data encryption. Since Lester Hill proposed this algorithm in 1929, nearly a century has passed. At that time, electronic computers had not yet been developed, and calculating high-order large modulus inverse matrices by hand was extremely time-consuming and labor-intensive. After the advent of the computer age, the academic community has generally focused on English encryption using this algorithm under modulo 26, while neglecting the use of high-order matrix large modulus encryption. Therefore, this paper employs electronic computers to encrypt plaintext data using high-order matrix large modulus operations, thereby extending the Hill cipher to full-character data encryption and network data transmission encryption.

Keywords

Hill encryption; linear transformation; high-order large modulus

希尔加密算法探究

贾光斌

达州市通川区农业科技园区服务中心，中国·四川 达州 635000

摘　要

现在各种形式的加密算法层出不穷，其中希尔加密算法就是一种很不错的非对称加密算法。希尔加密算法的实质就是将明文看作是一组向量，然后经过模运算下的线性变换将明文向量组映射成密文向量组实现数据加密。自从1929年以来，勒斯特尔·希尔提出这一算法已经近一百年时间过去了。由于当时电子计算机还没有出现，高阶大模逆矩阵仅凭人工手算太费时费力。人类进入计算机时代后，学术界普遍关注这一算法在模26下的英文加密，长期忽视采用高阶矩阵大模下加密。因此本文运用电子计算机完成采用高阶矩阵大模运算下对明文数据加密，从而实现将希尔加密算法推广到全字符型数据加密及互联网络数据传输加密等领域。

关键词

希尔加密；线性变换；高阶大模

1 引言

在所有的加解密算法里，第一步首先是建立 m 个有限的加密数据元素集合与数据代码集合整数环之间的一一映射关系，也就是制作一个密码本，建立一个密文代码映射关系。

第二步是在有限代码集合整数环 Z_m 中，将明文代码代码 P 一一映射成密文代码 C，换言之，就是在有限环 Z_m 里做模 m 的同余运算。这是所有的加密算法都必须遵循原则。加解密过程其实就是在有限环 Z_m 中做模 m 同余运算，加解密过程记作

$$(1)\quad C \equiv f_2(P) \pmod{m} \qquad P \equiv f_2^{-1}(C) \pmod{m}$$

如果这种映射是模加运算，解密就只需要做模减运算，此时加法逆元只需要前面加负号即可，加解密的密码绝对值相等，亦就是对称加密算法；如果这种映射是其他抽象运算，解密就需要做模逆运算，此时模逆元一般情况下不等于加密密码，这就是非对称加密算法。

对称加密算法实现起来相对较为简单，但是它做的其实就是有限环 Z_m 中的平移运算，根本上并没有改变明文的结构缺陷；非对称加密算法本身很复杂，同时改变了明文的结构缺陷，故不可能通过分析加密元素的频率特征破解密文。

2 希尔加密算法总述

希尔加密算法的基本思想是将明文代码 P 看作是 l 个 n 维向量组形成的矩阵，通过线性变换将它们转换为 l 个 n 维密文 C 向量组数据。令明文数据空间 P(Z_m) 为，将明文 P 看作是一组向量形成的矩阵，采用 n 维数据为单位进行代换，

【作者简介】贾光斌（1977–），男，中国四川盐亭人，硕士，工程师，从事通信与信息系统研究。

则形成多代码代换，根据对加密数据按列或按行分块成相应的的列向量或行向量，可以将明文 P 表示成

$$[\boldsymbol{P}_1,\ \boldsymbol{P}_2,\ \cdots,\ \boldsymbol{P}_l]^{\mathrm{T}}$$

希尔加密将明文看作是矩阵，此时加密映射 f_2 要求是线性可逆的，此时线性变换可以用 n 阶可逆矩阵 $GM_n(\mathbb{Z}_m)$ 描述为一一映射，记逆变换矩阵为 $GM_n^{-1}(\mathbb{Z}_m)$。可见希尔算法的核心在于求解模逆矩阵，本质就是矩阵乘法。解密只要作一次逆变换就可以了，密钥 K 就是变换矩阵本身。

由于希尔加密是以 n 维向量为最小单位，所以向量里的某些分量即便相等，经过线性变换后，对应的分量也不一定相等，所以这样就掩盖了明文的结构缺陷，使得攻击者不可能通过对密文进行频率特征分析破解。

2.1 希尔加解密原理

如前所述，上述（1）式在希尔加密里可以分别改写成矩阵形式

$$(2)\quad \boldsymbol{C} \equiv \boldsymbol{P}M_n \pmod{m} \qquad \boldsymbol{P} \equiv \boldsymbol{C}\,M_n^{-1} \pmod{m}$$

其中 M_n^{-1} 是 n 阶矩阵 M_n 的模 m 逆矩阵

解密时将密文 C 与加密矩阵的模逆矩阵相乘，从而对 n 维密文向量组做线性逆变换恢复明文。

记加密密钥为

$$K_e（M_n，\ m）$$

表示在模 m 下采用 n 阶矩阵 M 加密，解密密钥仿此类似。

从上面可以看出，希尔加密算法的秘钥 K_e 或 K_d 有三个参数，分别是加密矩阵 M_n 及其阶数 n 和加密模 m。

为了提高数据加密的安全性，需要采用高阶大模矩阵加密，因此希尔加密算法关键是寻求用尽可能小的算力提高加密矩阵的阶数和加密模数。

希尔算法的加解密流程

希尔加密过程大致分为以下五步完成：

1) 将明文转化为数字矩阵。将明文中的每个元素按照模内每个元素的映射关系转化为数字代码空间里对应的数值元素。

2) 矩阵分块。根据密钥矩阵的阶数 n，将明文数值元素序列排列成一个 l 行 n 列矩阵，形成明文矩阵 P，如果明文矩阵末尾不全，则须任意填充成一个完整的数字矩阵。

3) 加密矩阵生成。随机生成一个 n 阶矩阵作为加密矩阵，并对此做可逆性检测，只保留模可逆的矩阵作为加密矩阵，其判定准则是加密矩阵行列式 Δ 与加密模 m 互素。

4) 在模 m 下计算矩阵乘法。将明文矩阵左乘密钥矩阵实现数据加密完成密文转换。

5) 生成密文。将矩阵乘法运算的结果取模求余后的数值转换回对应的加密数据集里的元素形成密文。

解密是加密的逆过程，与之相仿也可分为接受密文、矩阵分块、计算密钥矩阵的模逆矩阵、计算模矩阵乘法、恢复明文等五步完成。只是需要求解密钥矩阵的模逆矩阵 $M_n^{-1} \pmod{m}$。

2.2 希尔加密算法对算力的要求

由于希尔加密算法里 n 阶加密矩阵的模 m 最大值等于其向量分量绝对值最大值，因此其加密模 m 最大值与计算机总字长 w 和处理器并联情况有关，所以此时希尔加密模最大值表达式为

$$m = \max_{1\le i,\ j\le n} |a_{ij}| = \sqrt{2^w}$$

受制于 IEEE 754 协议影响的软件计算精度上限为 10^{15}，此时加密模 m 最大值表达式为

$$m = \max_{1\le i,\ j\le n} |a_{ij}| = \sqrt{10^{15}} \in 区间(10^7,\ 10^8)$$

所以现在市面上一般配置的单 CPU 64 位字长 2GB 内存计算机就能进行 28 阶矩阵 7 位数模明文加密。

3 模逆矩阵

既然希尔加密算法的核心在于求解模逆矩阵，因为环里逆矩阵和伴随矩阵只是相差一个系数因子，所以首先需要求出模伴随矩阵。

3.1 模伴随矩阵

首先，我们仔细考察下线性代数里矩阵 $A[a_{ij}]$ 的求逆公式

$$(3)\ A^{-1} = \Delta^{-1}A^*$$

从式（1）可以看出，矩阵 A 的逆矩阵和其伴随矩阵只是相差一个系数因子矩阵行列式的倒数，即矩阵行列式的乘法逆元。

根据伴随矩阵的定义，伴随矩阵 A^* 是其代数余子式矩阵的转置矩阵。从此定义可知，矩阵转置运算只是行列位置的互换，不涉及元素运算，因此域上伴随矩阵的计算涉及矩阵元素间的运算的就只有代数余子式计算这一步。而依据行列式代数余子式展开定理，有如下递推公式

$$\Delta A_{ij,n} = \sum_{i,j=1}^{n} (-1)^{i+j} a_{ji} \Delta A_{ij,n-1}$$

从上式可以看出，代数余子式计算只涉及加、减、乘法运算，也就是说代数余子式运算在环里运算是封闭的，从而伴随矩阵在环里也是封闭的。将其两端同时做模 m 运算，可得

$$\Delta A_{ij,n} \pmod{m} = \sum_{i,j=1}^{n} (-1)^{i+j} a_{ji} \Delta A_{ij,n-1} \pmod{m}$$

$$\equiv \sum_{i,j=1}^{n} [(-1)^{i+j} \pmod{m}\ \ a_{ji} \pmod{m} \Delta A_{ij,n-1} \pmod{m}]$$

$$\equiv \sum_{i,j=1}^{n} (-1)^{i+j} a_{ji} \Delta A_{ij,n-1} \pmod{m}$$

依据初等数论的相关结论，上式中

$$A^* = \left[\sum_{i,j=1}^{n} (-1)^{i+j} a_{ji} \ \Delta A_{ij} \right] \Rightarrow \ A^* \ (\bmod \ m)$$

$$\equiv \left[\sum_{i,j=1}^{n} (-1)^{i+j} \ (\bmod \ m) \ a_{ji} \ (\bmod \ m) \ \Delta A_{ij} \ \ (\bmod \ m) \right]$$

$$\equiv \left[\sum_{i,j=1}^{n} (-1)^{i+j} a_{ji} \ \Delta A_{ij} \right] \ (\bmod \ m) \ \equiv \ A^* \ (\bmod \ m)$$

从而得出结论：模伴随矩阵在模运算下整数环里与实数域上表达式是一样的，可以随意交换伴随运算和模运算的次序。因此模伴随矩阵的求解只需要把实数域里的伴随矩阵取模求余即可，求解希尔加密矩阵的模逆矩阵关键在于求加密矩阵行列式的模逆元。

3.2 模逆元

依据初等数论知识，任意元 *a* 求解模 *m* 逆元理论上可以直接运用费马—欧拉定理（Fermat-Euler Theorem）直接求得。

但是仔细分析发现要求 *a* 的模逆元，需要知道模 *m* 的欧拉函数值，而这需要对 *m* 进行因式分解，求出其所有素因子方可，要对大数进行因子分解几乎是不可能的。因此需要寻找更加快速的算法计算整数环上的模逆元。

根据模逆元的定义，将定义式同余表达式改成等式形式后，把 a^{-1} 和 *-k* 看作是未知变量 *x*、*y*，就可以把上式看作是贝祖定理（Bezout Theorem，亦叫最大公约数表示定理）的一种表示形式。因此求解模逆元的问题可以转化为求解非齐次线性不定方程

$$(4) \ ax + my = \ 1$$

的整数解问题。

根据贝祖定理，上面（4）式要有整数解的充分必要条件是 *a* 与 *m* 互素，即

$$\gcd（a，\ m） = 1$$

再根据齐次线性方程解答存在定理，只要满足 *a* 与 *m* 不相等，且都不为 0，则（4）式方程对应的齐次方程一定存在一维的整数基础解系，再根据非齐次线性方程解的结构定理可得上述非齐次线性方程的通解表达式为

$\begin{cases} x = \ \bar{x} + mt \\ y = \ \bar{y} - at \end{cases}$，其中$\forall \ t \in \mathbb{Z}$，$(\bar{x}，\ \bar{y})$ 是线性方程（4）的特解

将上式中 *x* 的值对模 *m* 求同余运算可知，通过此法求得的特解无论怎样，都始终归属于一个剩余类里，即是要求的唯一模逆元。所以要求出（4）式方程的整数解必须先求出此方程的一个整数特解。

扩展欧几里得算法

为了求解上述非齐次线性方程的整数特解，我们介绍一种扩展欧几里得算法（Extended Euclidean Algorithm）。欧几里得（Euclid）算法在中国古书《九章算术》里也叫辗转相除法，西方最早记载于欧几里得所著《几何原本》里，故得名欧几里得算法。

欧几里得算法是通过余数不断地辗转相除求取任意两个正整数的最大公约数。扩展欧几里得算法是用欧几里得算法中每步迭代产生的商反向迭代求出上述方程（4）的一个整数特解。

依欧几里得算法可得递推公式

$$(5) \begin{cases} x_i \ = \ x_{i-2} - x_{i-1} q_{i-1} \ ，\ 初始值为 \ x_0 = 0，\ x_1 = 1 \\ y_i \ = \ y_{i-2} - y_{i-1} q_{i-1} \ ，\ 初始值为 \ y_0 = 1，\ y_1 = 0 \end{cases}$$

其中q_{i-1} 是欧几里得算法里第$i-1$ 步迭代产生的商

可以采用数学归纳法证明之。

证明：

欧几里得算法求两整数 *a* 与 *m* 的最大公约数是设定好初始值，令

$$\begin{cases} x_0 = 0 \\ y_0 = 1 \end{cases}，\ \begin{cases} x_1 = 1 \\ y_1 = 0 \end{cases}$$

则有

$$\begin{cases} m = \ r_0 \\ a = \ r_1 \end{cases}$$

于是

$$r_0 = \ r_1 \ q_1 + \ r_2$$

$$r_1 = \ r_2 \ q_2 + \ r_3，\ \cdots，\quad r_{i-1} = \ r_i \ q_i + \ r_{i+1}，\ \cdots，$$

$$r_{n-2} = \ r_{n-1} \ q_{n-1} + \ r_n，\quad r_{n-1} = \ r_n \ q_n \quad （i = 1，\ 2，\ \cdots，\ n）$$

可知

$$a \ x_{i-1} + m y_{i-1} = \ r_{i-1} \ ，\ i = 0，\ 1，\ 2，\ \cdots，\ n$$

因此

$$\begin{cases} x_0 = 0 \\ y_0 = 1 \end{cases}，\ \begin{cases} x_1 = 1 \\ y_1 = 0 \end{cases}$$

使得原方程式（4）成立，

假设第 *i*-1 步迭代式（5）使得原方程式（4）成立，即

$$a \ x_{i-1} + m y_{i-1} = \ r_{i-1} \ ，$$

其中 $x_i \ = \ x_{i-2} - x_{i-1} q_{i-1} \quad y_i \ = \ y_{i-2} - y_{i-1} q_{i-1}$

那么第 *i* 步迭代

$$a \ x_i + m y_i \ = \ a（x_{i-2} - x_{i-1} q_{i-1}） + m（\ y_{i-2} - y_{i-1} q_{i-1}）$$

$$= \ a x_{i-2} + m \ y_{i-2} - （a x_{i-1} + m y_{i-1}） \ q_{i-1}$$

$$= r_{i-2} - r_{i-1} \ \ q_{i-1} \ = r_i$$

因此结论成立，证毕。

综上所述，求解任意元 *a* 的模 *m* 逆元只需要设定好第 0 步和第 1 步的初始值（0，1），然后采用欧几里得算法里的商按照递推公式（5）逐步迭代，直到出现余数 r_n 为 0 即停止，并检查倒数第二步计算的余数 r_{n-1} 是否为 1。如果倒数第二步的余数为 1，则倒数第二步迭代的结果 x_{n-1} 即是非齐次线性方程（4）的整数特解，即我们要求的模逆元，否则元素 *a* 不存在模 *m* 逆元。

3.3 模逆矩阵存在的充分必要条件

如前所述，产生加密矩阵时首先必须检测其可逆性，否则加密后就不能解密，其加密矩阵可逆性的判定准则是加密矩阵的矩阵行列式Δ 与模 m 互素。即

$$\boldsymbol{\gcd（\Delta，\ m）= 1}$$

下面给出详细的证明。

证明：

由于任意矩阵 A 的伴随矩阵总是存在的，根据初等数论相关性质，任意矩阵的模伴随矩阵同样存在。所以，无论是域里还是环里的矩阵环，恒有下式成立

$$AA^* = \Delta E$$

从而推出

$$(6) \implies AA^* \equiv \Delta E \pmod{m}$$

先看充分性：

如果Δ与 m 互素，即

$$\gcd(\Delta, m) = 1$$

此时从数论相关性质可知，Δ的模 m 逆元一定存在，因此（6）式同余式两端可以同时乘以矩阵行列式的模逆元，如此可以得到

$$\Delta^{-1} AA^* \equiv \Delta^{-1}\Delta E \pmod{m} \implies \Delta^{-1} AA^* \equiv E \pmod{m}$$
$$\implies A\,\Delta^{-1}A^* \equiv E \pmod{m}$$

比照模逆矩阵定义式，可以推出

$$\implies A^{-1} \equiv \Delta^{-1}A^* \pmod{m}$$

如此，充分说明只要矩阵行列式与 m 互素，矩阵 A 的模逆矩阵就存在且可求。

其次，必要性：

设Δ与 m 的最大公约数为 d，即

$$\gcd(\Delta, m) = d$$

根据贝祖定理，只有Δ、m 与 d 的倍数 kd 三者满足以与 m 分别为系数的贝祖方程

$$\Delta x + my = kd$$

此时上述方程才存在整数解。

将上式对模 m 取余，可得

$$\Delta x \equiv kd \pmod{m}$$

也就是说，任意整数 x 在模 m 下乘以矩阵行列式都只能等于最大公约数 d 的倍数，不可能等于 1，此时矩阵行列式不存在模逆元。

将此结果代入矩阵同余方程

$$AA^* = \Delta E$$

可以推出

$$\implies xAA^* \equiv x\Delta E \equiv kdE \pmod{m}$$

此时如果 k 与 m 互素，则 k 存在模 m 的逆元，于是

$$xk^{-1}AA^* \equiv dE \pmod{m}$$

因题设，可得

$$\exists\, k_1 \in \mathbb{Z},\ k_2 \in \mathbb{Z},\ \text{使得}\ \Delta = k_1 d\ ,\quad m = k_2 d$$

又因为 d 与模 m 不互素，所以上式右端因子 d 不存在模 m 的逆元，所以此时上述同余式两端在模 m 下不可能再化简。所以不存在该矩阵和其模伴随矩阵与任意整数 x 之积同余于模 m 单位矩阵 E。

如果 k 与 m 不互素，则 k 不存在模 m 的逆元，于是任意矩阵 A 与其模伴随矩阵和任意整数 x 三者在模 m 下相乘结果都只同余于最大公约数的倍数与模单位矩阵之积。

最后再看矩阵行列式等于零或模m同余于零时的情形，此时

$$\gcd(\Delta, m) = m$$

显然此时Δ不存在模逆元，故此时亦不存在模逆矩阵。

总之，当且仅当

$$\gcd(\Delta, m) = 1$$

模逆矩阵存在，即模逆矩阵存在的充分必要条件是Δ与 m 互素，证毕。

4 希尔算法评估

因为希尔算法解密矩阵可以根据加密矩阵直接求出，故不可作为公钥机制加密。但是希尔算法对加密模 m 没有任何要求，即便是在模 2 下希尔加密如果采用高阶矩阵加密数据仍然非常安全。这样将这一算法可以方便的推广到加密模小的应用场景。

希尔加密算法的缺点在于易被已知明文和密文攻击者击破，因为找到可逆的明文矩阵 P，攻击方求出 P 的模逆矩阵，就破获了希尔加密的加密矩阵。

希尔算法的密钥空间

希尔密钥空间需要求出同余方程

$$(7)\ \forall\ a \in \mathbb{Z}_m \wedge \gcd(a, m) = 1\ ,\ \Delta \equiv a \pmod{m}$$

的解集个数。

高阶矩阵希尔密钥空间计算相当复杂，二阶矩阵的密钥空间为

$$|G\mathbb{M}_2(\mathbb{Z}_m)| = m^4 \prod_{i=1}^{s} \left(1 - p_i^{-1}\right)\left(1 - p_i^{-2}\right)$$

此证明的详细过程可参见参考文献。

5 应用前景展望

随着算力的提高，希尔加密算法模 m 就可以取到几十位，甚至到 200 位以上，希尔加密应用前景亦更加广泛。

5.1 加密数据类型拓展

希尔加密数据类型可以不断拓展，将不再局限于文字或字符类数据，可以是图片、图形图像、音频、甚至视频数据等等数据类型。

5.2 与数字传输技术融合发展

希尔加密可直接对网络传输数据加密，此时对传输中的信息数据流进行加密，按加密矩阵阶数 n 进行数据分组后加密生成密文数据包，双方约定好密码实现自动加密，经云端到达终端后自动重组、解密成为明文数据。

参考文献

[1] 杨根学. 希尔密码的破译[J]. 娄底师专学报, 2000 (4): 54-57.

[2] 佚名. 密码学的数学基础[P]. 哔哩哔哩视频分享平台, 2022 (4): 1-5.

[3] 戴经国等. 关于Hill密码密钥空间大小的计算[J]. 科学技术与工程, 2007 (1): 7.