Applied Mathematical Sciences, Vol. 9, 2015, no. 106, 5293 - 5303
HIKARI Ltd, www.m-hikari.com
http://dx.doi.org/10.12988/ams.2015.56450

A Secure Cryptosystem Using the Decimal Expansion of an Irrational Number

M. K. Viswanath

Department of Mathematics
Rajalakshmi Engineering College, Thandalam
Chennai-602 105, Tamil Nadu, India

M. Ranjith Kumar

Research and Development Centre, Bharathiar University
Coimbatore-641 046, Tamil Nadu, India

Abstract

The main objective of this paper is to develop a simple and robust secure encryption scheme with digital signature. In this paper a cryptosystem with digital signature using the decimal expansion of an irrational number is obtained.

Mathematics Subject Classification: 11T71, 14G50, 68P25, 68R01

Keywords: Hills cipher, digital signature, pseudo inverse of a rectangular matrix and Hypergeometric function

1 Introduction

Network communication is one of the most valuable and priceless assets in the world today. In many cases, the exchanged bits of information need to be secure, and hence security of these bits play a crucial role in network communications [13]. Using cryptographic methods one can ensure the security, confidentiality and integrity of the Network Communication. There are two

types of cryptosystem, namely (i). The symmetric key cryptosystem and (ii). The asymmetric key cryptosystem or the public key cryptosystem. The public key cryptosystems, in vogue today are the RSA, El-Gamal and the Elliptic curve cryptosystem [9, 10]. The robustness of these algorithms lies in the fact that it's not feasible with today's machines to factorize a large number or to solve the discrete logarithm problem. However, this may not be the case in the years to come, on account of the extraordinary progress made in computer technology and especially, the possibility of building the long-awaited quantum computers that will certainly put an end to the use of existing algorithms.

In many environments, it is more important that communications be authenticated rather than be encrypted as a message, since both parties should be convinced of each other's identity. Therefore we must ensure the two necessary properties of communication systems namely: messages are encrypted and messages are authenticated. We demonstrate in this paper how these capabilities are incorporated in the communication system, developed here, using an idea proposed in [16]. The following method provides an implementation of a secure cryptosystem and digital signature. This method is quite robust and can be implemented easily. Readers familiar with irrational numbers, Hills cipher, digital signature and pseudo inverse of a rectangular matrix may directly go to section six for the working of our algorithm.

2 Hill n-Cipher

Hill cipher was first introduced by Lester S. Hill in 1929 in the journal *The American Mathematical Monthly* [4, 8]. Hill cipher is the first polygraphic cipher. A polygraphic cipher is a cipher where the plaintext is divided into blocks of adjacent letters of the same fixed length n, and then each such block is transformed into a different block of n–letters. This polygraphic feature increased the speed and the efficiency of the Hill cipher. Besides, it has some other advantages in data encryption such as its resistance to frequency analysis. The core of Hill cipher is matrix multiplication.

3 Digital Signature

A digital signature is an electronic signature that can be used to authenticate the identity of the sender or the signer of a document, and to ensure the original content of the message or document that has been sent are unchanged [14]. The digital signature provides the following three features:

Authentication

Digital signatures are used to authenticate the source of messages. The ownership of a digital signature key is bound to a specific user and thus a valid signature shows that the message was sent by that user.

Integrity

In many cases, the sender and the receiver of a message need assurance that the message has not been altered during transmission. Digital signatures provide this feature by using cryptographic message digest functions.

Non-Repudiation

Digital signatures ensure that the sender who has signed the information cannot at a later date deny having signed it.

4 Pseudo Inverse of a Rectangular Matrix

Definition 4.1 *Let $A \in \mathbf{R}^{m\times n}$ and $X \in \mathbf{R}^{n\times m}$, then the following equations are used to define the pseudo inverse of a rectangular matrix A [3, 12].*

$$AXA = A \tag{4.1}$$

$$XAX = A \tag{4.2}$$

$$(AX)^T = AX \tag{4.3}$$

$$(XA)^T = XA \tag{4.4}$$

Equations (4.1) *through* (4.4) *are called the Penrose conditions* [11].

Definition 4.2 *A pseudo inverse of a rectangular matrix $A \in \mathbf{R}^{m\times n}$ is a matrix $X = A^{\#} \in \mathbf{R}^{n\times m}$ satisfying equations* (4.1) *through* (4.4). *A pseudo inverse is sometimes called the Moore-Penrose inverse after the pioneering work done by Moore* (1920, 1935) *and Penrose* (1955).

4.1 Construction of Pseudo Inverse

For a given $A \in \mathbf{R}^{m\times n}$, the pseudo inverse $A^{\#} \in \mathbf{R}^{n\times m}$ is unique.

(4.5) If $m = n$ and $rank(A) = m$ then $A^{\#} = A^{-1}$.

(4.6) If $m < n$ and $rank(A) = m$ then $A\,A^T$ is non-singular and $A^{\#} = A^T(AA^T)^{-1}$.

(4.7) If $m > n$ and $rank(A) = n$ then $A^T\,A$ is non-singular and $A^{\#} = (A^TA)^{-1}A^T$.

4.2 Conjecture

(i). If A is a rectangular matrix in $\mathbf{R}^{\text{mxn}}$ formed by the mn consecutive decimal places of any irrational number, with $rank\,(A) = m < n$, then A is always right invertible.

(ii). If A is a rectangular matrix in $\mathbf{R}^{\text{mxn}}$ formed by the mn consecutive decimal places of any irrational number, with $rank\,(A) = n < m$, then A is always left invertible.

5 Irrational Numbers

The decimal representation of a rational number is either finite or periodic. By contrast, the decimal representation of every irrational number is infinite and non-periodic. Also it is a well-known result that, the set of all rational numbers is countable and the set $\mathbf{R}$ of real numbers is uncountable. As $\mathbf{R}$ is the union of the set of all rationals and irrationals, it follows that the set of all irrationals is uncountable. Therefore almost all real numbers are irrational.

5.1 The Euler's Number e

The number e is an important mathematical constant that is used in the base of the natural logarithm. This number was first studied by the Swiss Mathematician Euler in the 1720's, although its existence was more or less implied in the work of John Napier, the inventor of logarithms in the 16^{th} century. Euler was the first to use the letter e for this irrational number in 1727. As a result e is called Euler's number or Napier's constant. The number e is defined as the limit of the convergent sequence $\left\{\left(1+\frac{1}{n}\right)^n\right\}$ or the sum of the infinite series $1+\frac{1}{1!}+\frac{1}{2!}+\frac{1}{3!}+\cdots$ and e is also a transcendental number. Euler gave an approximation of e up to 18 decimal places. Now its value has been calculated to trillion decimal places[15].

6 Hypergeometric Functions

Hypergeometric functions were known to Euler but it was Gauss who studied it systematically for the first time and this had a tremendous influence in many branches of mathematics.

Before we introduce hypergeometric functions we explain the notation called shifted factorial function or Pochammer symbol

$$(a)_k = \begin{cases} a(a+1)\cdots(a+k-1) & if\ \ k = 1,2,3,\cdots \\ 1 & if\ \ k = 0 \end{cases}$$

It can be easily seen that the Pochammer symbol $(a)_k = \frac{\Gamma(a+k)}{\Gamma(a)}$. The hypergeometric function ${}_2F_1\,(a, b; c; x)$ is defined by the series

$${}_2F_1\,(a,b;c;x) = 1+\frac{ab}{c}x+\frac{a(a+1)b(b+1)}{c(c+1)}\frac{x^2}{2!}+\frac{a(a+1)(a+2)b(b+1)(b+2)}{c(c+1)(c+2)}\frac{x^3}{3!}+\cdots$$

$$= \sum_{n=0}^{\infty} \frac{(a)_n (b)_n}{(c)_n}\frac{x^n}{n!}$$

where $|x| \leq 1$ and a, b, c are neither zero nor a negative integer so that the series is neither unity nor terminating. The series converges for $|x| < 1$ and diverges for $|x| > 1$. When $|x| = 1$ the series converges absolutely if $(c - (a + b)) > 0$, $a, b, c \in \mathbf{R}$. The hypergeometric function ${}_2F_1\,(a, b; c; x)$ is symmetric with respect to a, b and there is a beautiful formula of Gauss that shows

$${}_2F_1\,(a,b;c;1) = \frac{\Gamma(c)\Gamma(c-a-b)}{\Gamma(c-a)\Gamma(c-b)}.$$

Srinivasa Ramanujan also worked extensively on hypergeometric functions throughout his life time [4].

7 Construction of the Proposed Cryptosystem

The main idea of the algorithm is to use an irrational number and a sequence generated from its ocean of decimal values, to encrypt the confidential message and to establish user's authentication. The fact that the sequence is random and aperiodic will guarantee a high degree of security and efficiency of the protocol.

To maintain confidentiality as well as authentication, Bob encrypts the confidential message P using the secret key K, to acquire the ciphertext $C = K\,(P)$. And if he wants to send a signed message X to Alice, he first encrypts X using his key S and obtain $Y = S\,(X)$. Bob sends this signed and encrypted message $[Y, C]$ to Alice. On receiving the message $[Y, C]$, Alice decrypts C using the key K^{-1} and obtains $P = K^{-1}(C)$; she then confirms that it was indeed sent by Bob using the key S^{-1}, to acquire $X = S^{-1}(Y)$. Thus both confidentiality and authentication are guaranteed in the above transaction. Bob and Alice ensures the authenticity and integrity of the message pair $[Y, C]$ by using α_0 and an e-lock system.

7.1 Initial Setup

Suppose that Bob wants to send a confidential message with a digital signature to Alice using an irrational number. First he creates an initial setup for secure keys as given below.

1. Fix an irrational number I and make this public.

2. Choose a large prime number p, not exceeding twelve digits based on the availability of decimal places in the expansion of the chosen irrational number and a number n which is the product of two odd primes a and b with a strictly greater than b. These are privately chosen by Bob.

Before proceeding with the encryption/decryption protocols, assume that Bob discussed the entire protocol formally with Alice.

Encryption Protocol

For signature generation and plaintext encryption protocols, Bob does the following: Bob desires to send a secret message to Alice at t hours, $0 \leq t \leq 23$. Here t is considered as completed hours. He chooses an integer α_0 randomly. The keys α_0 and t are security parameters. Bob computes $\beta_{i,t}$, which is the sum of α_0 and the integral part of ${}_2F_1\,(x, y; z; 1)$ with $(\bmod p)$, where $x = n+t$, $y = 10\left(\frac{a+b}{2}\right) + \left(\frac{a-b}{2}\right) + t$ and $z = x + y + i$. To begin with,

$$\beta_{\,i,\,t} = \beta_{1,\,t} \;\equiv\; \alpha_0 \,+\, [{}_2F_1\,(x,\, y\,;\, z\,;\, 1)] \qquad (\bmod p)$$

As α_0 is random and i, t keeps varying, the number $\beta_{i,t}$ is random. The parameter i indicates the number of times Bob and Alice are in contact with each other after fixing α_0.

(a). Signature generation protocol:

To implement the protocol, Bob signs the message P with the signature X. He decides $\beta_{i,t}$ to be the beginning position of the decimal sequence of the irrational number I for the encryption process. The number at ${\beta_{i,t}}^{th}$ place, say β is used to substitute the beginning letter of the signature X by shifting the alphabet by β units $(\bmod N)$, where each alphabet is assigned a numerical value $[a = 0,\ b = 1,\ c = 2,\ \cdots\ ,\ z = 25,\ \cdots\ ,\ N]$. Afterwards the process is continued with the next integer and the corresponding alphabet in the signature. This process is continued till the entire X is encrypted as Y.

(b). Plaintext encryption protocol:

Now Bob has signed the message and he wanted to encrypt the secret message P at the same time t hours, then he does the following:

He computes the sequence of decimals from the position $\beta_{i,t}$ to the next n consecutive decimal places to form a rectangular matrix K. This key matrix K is written in the order of a-rows and b-columns and we use this rectangular matrix for encrypting the secret message P. He arranges the plaintext P in blocks of length b with its numerical equivalent. Finally he encrypts the message using the linear transformation $C \equiv\ K\,P\ \ (\bmod N)$. This encrypted and password protected message pair $[Y, C]$ is sent to Alice for decryption.

The password used here is the product of x and z. The key tuple $(n,\ p,\ \alpha_0)$ is sent to Alice through a secure channel.

Decryption Protocol

Alice finds the factors a, b of n from her private key tuple $(n,\ p,\ \alpha_0)$ and she does the following for the decryption protocol:

(c). Ciphertext decryption protocol:

Alice receives the password protected and encrypted message pair $[Y,\ C]$ at t hours δ minutes (say), and then she knows t is to be taken in completed hours only. She then computes x, y, z and $\beta_{i,\,t}$ for the corresponding parameters i, t and opens the message using the prearranged password $x.z$. She knows, $\beta_{i,\,t}$ is the position of the decimal place to start, in the expansion of the irrational number I. From the position of $\beta_{i,\,t}$, she collects the n consecutive digits from the decimal expansion of I and obtains the rectangular matrix K of order $a \times b$. She then computes the pseudo inverse $K^{\#}$ of K and keep this as her decryption key. She decrypts the ciphertext C easily using the linear transformation $P \equiv K^{\#}C \pmod{N}$, where C is arranged in blocks of a-tuples with its numerical equivalent. Alice can reply to Bob using the decimal expansion of I from the position $\beta_{i+1,\,t} = \beta_{2,\,t}$ in this case. This way they can contact each other continuously without using any key more than once. Bob chooses decimal places in such a way that $K^{\#}$ exists (by our conjecture 4.2, $K^{\#}$ always exists) and the messages are authenticated because of the hidden α_0 in all encryptions.

(d). Signature verification protocol:

Once Alice knows the value $\beta_{i,\,t}$, she can easily verify Bob's identity X by decrypting Y using the ordinary substitution cipher. Thus both confidentiality and authenticity are guaranteed in the above transaction.

8 Implementation of the Protocol

Assume that the system uses a 29-letter alphabet.

a	b	c	d	$\cdots$	w	x	y	z	_	.	!
$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\cdots$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$
0	1	2	3	$\cdots$	22	23	24	25	26	27	28

Consider the case I = Euler's number e, this is made public. Let $n = 15$ and so $a = 5$, $b = 3$ and $p = 2971215073$ (say).

Encryption:

Bob chooses a random integer $\alpha_0 = 5942461138$ and sends the tuple $(n,\, p,\, \alpha_0)$ to Alice through a secure channel. Assume Bob contacts Alice for the 70^{th} time at 2.10 hours, therefore $i = 70$ and $t = 2$. Then,

$$x = n + t = 17, \quad y = 10\left(\frac{a+b}{2}\right) + \left(\frac{a-b}{2}\right) + t = 43, \quad z = x + y + i = 130$$

and ${}_2F_1\,(x,\, y\,;\, z\,;\, 1) = 1779.495\cdots$.

$$\begin{aligned} \beta_{\,i,\,t} &\equiv \alpha_0 + [{}_2F_1\,(x,\, y\,;\, z\,;\, 1)] && (\mathrm{mod}\, p) \\ \beta_{\,70,\,2} &\equiv 5942461138 + [1779.495\cdots] && (mod\, p = 2971215073) \\ &\equiv 32771 && (mod\, p = 2971215073) \end{aligned}$$

Bob find the sequence of decimal places from the position of $\beta_{\,70,\,2} = 32771$ and chooses 15 decimals from this position in the decimal expansion of e. In this case the sequence of decimals is "114643923805213907862 89 $\cdots$" and he generates the 5×3 rectangular matrix

$$K = \begin{pmatrix} 1 & 3 & 0 \\ 1 & 9 & 5 \\ 4 & 2 & 2 \\ 6 & 3 & 1 \\ 4 & 8 & 3 \end{pmatrix}$$

Bob encrypts the secret message, say P="*send fifty crores of euros!*". Then the plaintext is divided into blocks of length three and the corresponding numerical value is given by

$$P = \begin{pmatrix} 18 & 3 & 8 & 24 & 17 & 4 & 14 & 4 & 14 \\ 4 & 26 & 5 & 26 & 14 & 18 & 5 & 20 & 18 \\ 13 & 5 & 19 & 2 & 17 & 26 & 26 & 17 & 28 \end{pmatrix}$$

$$\begin{aligned} C &\equiv K\,P \pmod{N} \\ &\equiv \begin{pmatrix} 1 & 23 & 23 & 15 & 1 & 0 & 0 & 6 & 10 \\ 3 & 1 & 3 & 7 & 25 & 6 & 15 & 8 & 26 \\ 19 & 16 & 22 & 7 & 14 & 17 & 2 & 3 & 3 \\ 17 & 14 & 24 & 21 & 16 & 17 & 9 & 14 & 21 \\ 27 & 3 & 13 & 20 & 28 & 6 & 0 & 24 & 23 \end{pmatrix} \pmod{29} \end{aligned}$$

which gives the ciphertext C, "*bdtr.xbqodxdwynphhvubzoq!agrrgapbjgidoyk_ dvx*". Note that $27 = |P| \neq |C| = 45$.

If he wants to sign the encrypted message P, by X : "*Mr Bob from India*" then he uses 17 consecutive numbers from the beginning position $\beta_{70,\,2} = 32771$, in the decimal expansion of e. In this case "$1146439238052139078628 9\cdots$" is used to encrypt the message X by ordinary substitution cipher method with mod 29. This produces the signature Y: "*nsdfrk!izor!jqmih* " which is the encrypted form of X and $|X| = |Y|$. Now the encrypted and signed message pair $[Y, C]$ protected by the password $x \cdot z = 2210$ is sent to Alice for decryption before 3.00 hours say, at 2.25 hours.

Decryption:

First Alice unlocks the message pair using the prearranged password $x \cdot z = 2210$ and finds the rectangular matrix K of order 5×3 using the position $\beta_{70,\,2} = 32771$ in the decimal expansion of e. From this matrix K, she computes the decryption key

$$K^{\#} \equiv \begin{pmatrix} 25 & 0 & 25 & 25 & 4 \\ 16 & 0 & 17 & 0 & 8 \\ 1 & 15 & 11 & 27 & 17 \end{pmatrix} \qquad (mod\, 29)$$

She divides the ciphertext into blocks of length five and decrypts it with the help of $K^{\#}$.

$$\begin{aligned} P &\equiv K^{\#}C \ \ (mod\ N) \\ &= \begin{pmatrix} 25 & 0 & 25 & 25 & 4 \\ 16 & 0 & 17 & 0 & 8 \\ 1 & 15 & 11 & 27 & 17 \end{pmatrix} \begin{pmatrix} 1 & 23 & 23 & 15 & 1 & 0 & 0 & 6 & 10 \\ 3 & 1 & 3 & 7 & 25 & 6 & 15 & 8 & 26 \\ 19 & 16 & 22 & 7 & 14 & 17 & 2 & 3 & 3 \\ 17 & 14 & 24 & 21 & 16 & 17 & 9 & 14 & 21 \\ 27 & 3 & 13 & 20 & 28 & 6 & 0 & 24 & 23 \end{pmatrix} \\ &\equiv \begin{pmatrix} 18 & 3 & 8 & 24 & 17 & 4 & 14 & 4 & 14 \\ 4 & 26 & 5 & 26 & 14 & 18 & 5 & 20 & 18 \\ 13 & 5 & 19 & 2 & 17 & 26 & 26 & 17 & 28 \end{pmatrix} \quad (mod\, 29) \end{aligned}$$

which gives the original plaintext P: "*send fifty crores of euros!*". By substitution cipher, she can verify Bobs identity X easily by decrypting Y.

9 Conclusion

The cryptosystem developed here is a powerful tool which ensures authentication, non-repudiation and secure communication. We have obtained the method for implementing a secure cryptosystem whose security rests on the difficulty of computing the keys. The security of our method proves to be

adequate, as the keys and the password used are dynamic. Also use of integers appearing in the decimal expansion of e in the encryption will make the decryption difficult by the usual methods of cryptography.

The security of this system is examined in more detail. In particular the keys n, p and α_0 are known only to Bob and Alice, it is not possible for any intruder to break this system. Also since $\beta_{i,t}$ changes each time during an encryption, the key K is dynamic and hence secure against known-plaintext attack. The proposed data encryption scheme given above has advantages of large key space, high level security and is mathematically and computationally simple, unlike the existing cryptosystems.

The proposed system also takes care of data integrity and authentication. Even if an intruder pretends as Alice and sends Bob a message, Bob can send a standard message to the intruder for encryption along with a new α_0 different from the one already used. The ciphertext of the standard message from the intruder will enable Bob to determine the authenticity of the intruder. This system is secure against frequency attack since the length of the plaintext and ciphertext are not equal. Hence the system is secure against all possible known attacks.

References

[1] W.N. Bailey, *Generalized Hypergeometric Series*, Cambridge: University Press, England, 1935.

[2] M. Bellare, R. Canetti and H. Krawczyk, Keying hash functions for message Authentication, *Lecture Notes in Computer Science*, **1109** (1996), 1–15. http://dx.doi.org/10.1007/3-540-68697-5_1

[3] T.L. Boullion and P.L. Odell, *Generalized Inverse Matrices*, Wiley, New York, (1971), 41–62.

[4] M. Eisenberg, *Hill Ciphers and Modular Linear Algebra*, Mimeographed Notes, University of Massachusetts, 1998.

[5] G.H. Hardy, *Hypergeometric series, ch-7 in Ramanujan: Twelve Lectures on subjects suggested by His Life and Work*, 3^{rd} ed., New York: Chelsea, (1999), 101–112.

[6] Howard Anton and Rorres Chris, *Elementary Linear Algebra*, 8th edition, John-Wiley and Sons Inc., New York, (2000), 678–688.

[7] I.A. Ismail, M. Amin and H. Diab, How to repair the Hill cipher, *Journal of Zhejiang University Science A*, **7** (2006), no. 12, 2022–2030. http://dx.doi.org/10.1631/jzus.2006.a2022

[8] S. Lester Hill, Cryptography in an algebraic alphabet, *Amer. Math. Mont.*, **36** (1929), 306–312. http://dx.doi.org/10.2307/2298294

[9] A.J. Menezes , P.C. Van Oorchot and S.A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 2000.

[10] Neal Koblitz, *A course in Number Theory and Cryptography*, Springer, 2^{nd} ed., 1994. http://dx.doi.org/10.1007/978-1-4419-8592-7

[11] R. Penrose, *A generalized Inverse for Matrices*, Communicated by J.A. Todd Received 26 July 1954.

[12] Predrag Stanimirovic and Miomir Stankovic, Determinants of rectangular matrices and Moore-Penrose inverse, *Novi Sad J. Math.*, **27** (1997), no. 1, 53–69.

[13] Rhee and Man Young, *Cryptography and Secure Communications*, McGraw - Hill co., 1994.

[14] R.L. Rivest, A. Shamir and L. Adleman, A method for obtaining digital signatures and public key cryptosystems, *Communications of the ACM*, **21** (1978), no. 2, 120–126. http://dx.doi.org/10.1145/359340.359342

[15] Shigeru Kondo and Alexander J. Yee, *A list of notable large computations of* $\boldsymbol{e}$, Numberworld.org. Last updated: March 7, 2011, Retrieved on 2012-02-24.

[16] M.K. Viswanath, Transcendental Numbers and Cryptography, *Applied Mathematical Sciences*, **8** (2014), no. 174, 8675–8677. http://dx.doi.org/10.12988/ams.2014.410873

[17] M.K. Viswanath and A.R. Deepti, An improvised version of Hill's cipher, *Journal of Discrete Mathematical Sciences and Cryptography*, **11** (2008), no. 2, 231–237. http://dx.doi.org/10.1080/09720529.2008.10698180

[18] M.K. Viswanath and A.R. Deepti, A New Approach to a Secure Cryptosystem using the Microcontroller, *Journal of Information Assurance and Security*, **1** (2006), no. 4, USA.

[19] M.K. Viswanath and M. Ranjithkumar, A Public Key Cryptosystem Using Hill's Cipher, *Journal of Discrete Mathematical Sciences and Cryptography*, **18** (2015), no. 1-2, 129–138. http://dx.doi.org/10.1080/09720529.2014.962856

Received: July 4, 2015; Published: August 12, 2015