EMPLOYING REVERSE POLISH NOTATION IN ENCRYPTION

Dr.S.S. Dhenakaran

Assistant Professor, Department of Computer Science and Engineering
Alagappa University, Karaikudi, Tamilnadu, India.
ssdarvind@yahoo.com

ABSTRACT

Cryptosystem is one of the effective principles helpful to internet aspirants to send message safely to the respondents. This principle ensures reliability for the message to be sent over internet. The basic requisite of the method is transforming the original message into some other stream to hide the syntax and semantics of the message before transmitting over internet. This paper is proposed to carry the job of perplexing the input message before applying the encryption process. The use of postfix makes the input content muddled for complication in understanding the ciphertext. The simulated Polish Notation principle is applied to mangle the characters of the message and multiple symmetric keys already created is used for encryption and decryption.

KEYWORDS

polish notation, mangled text, encryprion, decryption, ciphetext, multiple symmetric keys

1. INTRODUCTION

Cryptography is the art or science of keeping message secret. Cryptography deals with the aspects of secure messaging, authentication, digital signatures, electronic money, and other applications In cryptographic terminology, the message is called plaintext. Encoding the contents of the message in such a way that hides its contents from outsiders is called encryption. The encrypted message is called the ciphertext. The process of retrieving the plaintext from the ciphertext is called decryption. Encryption and decryption usually make use of a key, and the coding method is such that decryption can be performed only by knowing proper key. Since phishing, Botnet computers exist in internet, Industries and Organizations require highly reliable security systems to conduct business to its business parties and customers. To safeguard the vital information and confidential facts, they require systems protecting the industries and organization transacting information which nobody knows utilizing the communication lines. Many models are presently available to fulfill the above requisites [4]. Among them the cryptosystem is one of the mathematical models helping the industrial people to write the secret code for their information and to safely transfer the information on the computer and communication systems. The cryptosystems convert the original information into unintelligible information by dismantling the syntax and semantics of the information to preserve security on the reliable facts. The heart of the work is preparing the unordered sequence for the input message to be fed to the cryptosystem. The work in this paper introduces the use of mathematical simulated polish notation to strengthen the encryption process with the multiple symmetric keys for encryption.

DOI : 10.5121/acij.2011.2208

2. MODIFIED NEWTON-RAPHSON METHOD

Consider an equation f(x) = 0, where f is a real valued function defined on real line. Consider the usual metric d(x,y) = l x-y l on the real line. Write this equation in the form

$$x = x - f\,'(x) * f(x).$$

A solution of the equation f(x) = 0 (or f'(x) = 0) is a solution [3] of x = x – f'(x) * f(x). A solution of this equation is a fixed point of

$$g(x) = x - f'(x) * f(x).$$

The Banach fixed point theorem suggests a fixed point iteration method

$$x_{n+1} = x_n - f\,'\,(x_n) * f\,(x_n)$$

for a fixed point of g(x) or a solution of f(x) = 0 (or f'(x)=0) . The convergence of this iteration method is assured when f(x) satisfies a nice condition so that g(x) becomes a contraction. For example, when l f(x) f'(x) - f(y) f'(y) l <= α l x-y l, for some x,y in the domain of f for some α ,0< α < 1. A specific example may be f : [0,1/4] → [0,1/4] defined by f(x) = x^2 / 2 satisfies l f(x) f'(x) - f(y) f'(y) l <= 3/16 l x-y l .

Extend the principle to a system of m equations

$$f1(x_1,x_2,x_3,\ldots\ldots x_n) = 0$$
$$f2(x_1,x_2,x_3,\ldots\ldots x_n) = 0$$
$$f\,3(x_1,x_2,x_3,\ldots\ldots x_n) = 0$$
$$\text{-- -- -- -- -- -- --}$$
$$fm(x_1,x_2,x_3,\ldots\ldots x_n) = 0$$

The matrix form of these equations can be written as

$$X = X \text{ --- } J * F_x$$

where

$$X = \begin{bmatrix} x_1 \\ x_2 \\ \cdots\cdots \\ \cdots \\ x_n \end{bmatrix} \quad J = \begin{bmatrix} \frac{\partial f_1}{\partial x_1} \cdots \frac{\partial f_m}{\partial x_1} \\ \cdots\cdots \\ \frac{\partial f_1}{\partial x_n} \cdots \frac{\partial f_m}{\partial x_n} \end{bmatrix} \text{ and } F_x = \begin{bmatrix} f_1(x_1 \ldots x_n) \\ f_2(x_1 \ldots x_n) \\ \cdots\cdots \\ f_m(x_1 \ldots x_n) \end{bmatrix}$$

The solution of the equations is a fixed point of the mapping g : R^n → R^n defined by

$$g(X) = X_x \text{ --- } J_x * F_x$$

Let us consider the usual Euclidean metric d on R^n defined by

$$d(X, Y) = \left(\sum_{i=1}^{n} |\, x_i - y_i \,| \right)^{1/2}$$

The Banach fixed point theorem suggests the following iteration method

$$\begin{bmatrix} x_1^{(k+1)} \\ x_2^{(k+1)} \\ \cdots \\ \cdots \\ x_n^{(k+1)} \end{bmatrix} = \begin{bmatrix} x_1^{(k)} \\ x_2^{(k)} \\ \cdots \\ \cdots \\ x_n^{(k)} \end{bmatrix} - \begin{bmatrix} \frac{\partial f_1}{\partial x_1} \cdots \frac{\partial f_m}{\partial x_1} \\ \cdots \\ \frac{\partial f_1}{\partial x_n} \cdots \frac{\partial f_m}{\partial x_n} \end{bmatrix} * \begin{bmatrix} f_1(x_1^{(k)} \ldots x_n^{(k)}) \\ f_2(x_1^{(k)} \ldots x_n^{(k)}) \\ \cdots \\ f_m(x_1^{(k)} \ldots x_n^{(k)}) \end{bmatrix}$$

The convergence of this method is assured when $f_1, f_2, \ldots f_m$ satisfy the following conditions so that g becomes a contraction.

$$\| J_x * F_{x} - J_y * F_y \| <= \alpha * \| X - Y \|$$

for all vectors $[x_1, x_2, \ldots . x_n]$, $[y_1, y_2, \ldots . y_n]$ in the domain for some alpha with $0 < \alpha < 1$, and the Euclidean vector norm $\| \quad \|$..

3. MULTIPLE SYMMETRIC KEYS

The multiple symmetric keys are used in the proposed work. For, two real valued functional equations are constructed with the contents of user's personal information and digital signature. The backbone of these equations is the identification of patterns in the prime inputs. Here the pattern is assumed as the characteristics of character. The patterns are assumed as variables and the number of elements in each pattern is taken as the coefficient of a variable. Hence the sum of the number of patterns is equated with the number of characters in the personal information and digital signature which leads to frame two real valued functional equations. The functional equations are then solved using Modified Newton-Raphson method. The solutions of these equations are floating point numbers which are presumed as multiple symmetric keys [6]. The design of the proposed work employs four keys in encryption and decryption processes. Let the two real valued functional equations be

$$a_{11}x_1 + a_{12} x_2 + a_{13} x_3 + \ldots . + a_{1n}x_n = b_1$$
$$a_{21}x_1 + a_{22} x_2 + a_{23} x_3 + \ldots . + a_{2n}x_n = b_2$$

where $a_{11}, a_{12}, a_{13} \ldots \ldots . a_{1n}$

$a_{21}, a_{22}, a_{23} \ldots \ldots a_{2n}$ and

b_1, b_2 are known constants.

Let the equations be redefined as

$$f1(x_1, x_2, x_3, \ldots \ldots x_n) = 0$$
$$f2(x_1, x_2, x_3, \ldots \ldots x_n) = 0$$

Using Modified Newton-Raphson method, the real valued equations are solved and the solutions are taken as the multiple symmetric keys.. Further the proposed method focuses on four patterns and hence it generates four symmetric keys [1]. Since the equations are real valued, the keys are floating point numbers. The total length of the keys altogether is 128 bits long. These keys are combined with 16 bit data while performing encryption and decryption process [2]. The mathematical and geometrical representation of Modified Newton Raphson method is given below. Let the equations constructed be

$$a_{11} \; x_1 + a_{12} x_2 + \ldots a_{1n} x_n = b_1$$
$$a_{21} \; x_1 + a_{22} x_2 + \ldots a_{2n} x_n = b_2$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$
$$a_{m1}\ x_1 + a_{m2}\,x_2 + \ldots\ a_{mn}\,x_n = b_m$$

where $a_{11},a_{12},\ldots\ldots a_{1n\ldots\ldots}\ a_{m1},a_{m2},\ldots\ldots a_{mn}$ and $b_1,b_2\ldots.b_m$ are known constants. The value of the variables $x_1,x_2,x_3\ldots.x_n$ are to be found. Let the m equations in n variables be represented by the following real valued functions.

$$f_1\ (x_1,x_2,x_3\ldots\ldots x_n) = 0$$
$$f_2\ (x_1,x_2,x_3\ldots\ldots x_n) = 0$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$f_m\ (x_1,x_2,x_3\ldots\ldots x_n) = 0$$

Suppose that $x_1^{(k)}$, $x_2^{(k)}\ldots\ldots.x_n^{(k)}$ are given approximate solutions of this system and $x_1^{(k)}+h_1$, $x_2^{(k)}+h_2,\ldots\ldots.x_{nn}^{(k)}+h_n$ are exact solution of the system. By Taylor's theorem, we have

$$\begin{bmatrix} 0 \\ 0 \\ \cdots\cdots \\ \cdots\cdots \\ 0 \\ \\ \end{bmatrix} = \begin{bmatrix} f_1\,(x_1^k+h_1,..x_n^k+h_n) \\ f_2\,(x_1^k+h_1,..x_n^k+h_n) \\ \cdots\cdots \\ \cdots\cdots\quad - \\ f_m\,(x_1^k+h_1,..x_n^k+h_n) \\ \\ \end{bmatrix} \approx \begin{bmatrix} f_1\,(x_1^k,..x_n^k) \\ f_2\,(x_1^k,..x_n^k) \\ ------- \\ \cdots\cdots \\ f_m\,(x_1^k,..x_n^k) \\ \\ \end{bmatrix} + \begin{bmatrix} \frac{\partial f_1}{\partial x_1} \ldots \frac{\partial f_m}{\partial x_1} \\ \cdots\cdots\cdots \\ \frac{\partial f_1}{\partial x_n} \ldots \frac{\partial f_m}{\partial x_n} \end{bmatrix} * \begin{bmatrix} h_1 \\ h_2 \\ \\ \\ h_m \\ \\ \end{bmatrix}$$

when m x n matrix is at [x1(k), x2((k) ……xn(k)]. When n = m , we have

$$\begin{bmatrix} x_1^{(k)}+h1 \\ x_2^{(k)}+h2 \\ \cdots\cdots \\ \cdots\cdots \\ x_n^{(k)}+hn \\ \\ \end{bmatrix} \approx \begin{bmatrix} x_1^{(k)} \\ x_2^{(k)} \\ \cdots\cdots \\ \cdots\cdots \\ x_n^{(k)} \\ \\ \end{bmatrix} - \begin{bmatrix} \frac{\partial f_1}{\partial x_1} \ldots \frac{\partial f_1}{\partial x_n} \\ \\ \frac{\partial f_m}{\partial x_n} \ldots \frac{\partial f_m}{\partial x_n} \end{bmatrix}^{-1} * \begin{bmatrix} f_1\,(x_1^k,..x_n^k) \\ f_2\,(x_1^k,..x_n^k) \\ ------- \\ \cdots\cdots \\ f\ _m\,(x_1^k,..x_n^k) \\ \\ \end{bmatrix}$$

This gives the following classical Newton's method when n = m.

$$\begin{bmatrix} x_1^{(k+1)} \\ x_2^{(k+2)} \\ \cdots\cdots \\ \cdots\cdots \\ x_n^{(k+n)} \\ \\ \end{bmatrix} \approx \begin{bmatrix} x_1^{(k)} \\ x_2^{(k)} \\ \cdots\cdots \\ \cdots\cdots \\ x_n^{(k)} \\ \\ \end{bmatrix} - \begin{bmatrix} \frac{\partial f_1}{\partial x_1} \ldots \frac{\partial f_1}{\partial x_n} \\ \\ \frac{\partial f_m}{\partial x_1} \ldots \frac{\partial f_m}{\partial x_n} \end{bmatrix}^{-1} .* \begin{bmatrix} f_1\,(x_1^k,..x_n^k) \\ f_2\,(x_1^k,..x_n^k) \\ ------- \\ \cdots\cdots \\ f_m\,(x_1^k,..x_n^k) \\ \\ \end{bmatrix}$$

Thus

$$\begin{bmatrix} x_1^{(k+1)} \\ x_2^{(k+2)} \\ \ldots\ldots\ldots \\ \ldots\ldots \\ x_n^{(k+n)} \end{bmatrix} \approx \begin{bmatrix} x_1^{(k)} \\ x_2^{(k)} \\ \ldots\ldots \\ \ldots\ldots\ldots \\ x_n^{(k)} \end{bmatrix} - \begin{bmatrix} \frac{\partial f_1}{\partial x_1} \ldots \frac{\partial f_1}{\partial x_n} \\ \\ \frac{\partial f_m}{\partial x_1} \ldots \frac{\partial f_m}{\partial x_n} \end{bmatrix}^{-1} * \begin{bmatrix} f_1(x_1^k,..x_n^k) \\ f_2(x_1^k,..x_n^k) \\ \text{-------} \\ \ldots\ldots \\ f_m(x_1^k,..x_n^k) \end{bmatrix}$$

is a Modified Newton-Rapshon method. Newton-Raphson method for n=m=1 has a geometric interpretation through tangents. Similarly, the geometrical interpretation of the Modified Newton-Raphson method for n=m=1 is given below.

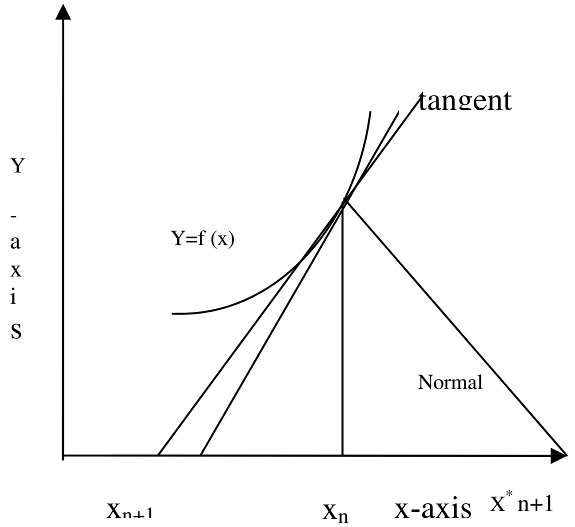

Figure 1. Modified Newton-Raphson Method

The method provides x^*_{n+1} as the next iterative point which is manipulated to get x_{n+1} for convergence such that $\mathbf{x_n - x_{n+1} = x^*_{n+1} - x_n}$. The convergence is verified by Banach Fixed Point Theorem [3]. The following principle caters the needs of achieving cryptography requirements [7].

4. POLISH NOTATION

Normally, polish notation is used to represent arithmetic expression. The polish notation extended to data structures is to rearrange the symbols of arithmetic expressions in order to represent the newer form of arithmetic expression. To do this process, a few mathematical principles are provided which are prefix, postfix and infix notations. These notations are shortly defined in the next few lines. When the operator symbol is placed before the operands in an expression, the representation is prefix form of the expression. When the operator symbol is placed between operands in an expression, the representation is infix form of the expression.

Similarly, when the operator symbol is placed after the operands in an expression, the representation is postfix form or polish notation of the expression. Out of these notations, postfix is the familiar mathematical principle adopted by computer algorithms to compute arithmetic expressions. The mathematical expression is evaluated with the help of stack. The principle of postfix notation is extended in the proposed work to obscure the plaintext.
Let the given expression be X+Y.
The Prefix form of the expression is +XY
The Postfix form of the expression is XY+
The Infix form of the expression is X+Y

5. SIMULATED POLISH NOTATION

To make use of simulated polish notation, a plaintext is used in place of arithmetic expression as in the case of polish notation. The simulated polish notation reserves a few characters for operands, operators, left and right parentheses. Priority is assigned to the characters to play the role of symbols in polish notation. The proposed work distorts the characters of the plaintext. The assumption of operands, operators and parentheses are shown below. The characters reserved for operands,

b	d	f	h	j	l	n	p	r	t	v	x	z
B	D	F	H	J	L	N	P	R	T	V	X	Z
2	4	6	8									

The characters reserved for operators,

y	w	u	s	q	o	m	k	I	g	e	c	a
Y	W	U	S	Q	O	M	K	I	G	E	C	A
3	5	7	;	.	,	blank						

with the higher priority to y or Y and least priority to blank.

Left parenthesis ű, Right parenthesis

Extending the reversed polish notation principle, the characters of the input message are scrambled. The necessary algorithm for scrambling plaintext with previous assumption is given below [5].

6. POLISH ALGORITHM TO MANGLE PLAINTEXT

Let Q be the given plaintext and P be the mangled expression to be found.
POLISH(Q,P)

```
1. Push ű onto stack and add Ă̄ to the end of Q.
2. Scan Q from left to right and repeat steps 3 to 6 for each element of Q until the stack is
   empty.
3. If an operand is encountered, add it to P.
4. If a left parenthesis (ű) is encountered, push it onto stack.
5. If an operator ⊗ is encountered, then
        a)  Repeatedly pop from stack and add to P each operator which has the
            same precedence as or higher precedence than ⊗
        b) Add ⊗ the operator to stack.
```

```
    EndIf
6. If a right parentheses (A̿ ) is encountered, then
        a) Repeatedly pop from stack and add it to P each operator until a left parenthesis
           is encountered.
        b) Remove the left parenthesis
      EndIf
    End of Step 2
7.Exit
```

The following algorithm regenerates the plaintext from the mangled information which is used in the decryption process.

7. ALGORITHM REGENERATING PLIANTEXT

Let Q be the given Postfix expression and P be the plaintext (infix) expression to be found.

```
INFIX (Q,P)
1. Add a A̿ at the end of Q.
2. Scan Q from left to right and repeat steps 3 to 4 for each element of Q until Q is A̿ .
3. If an operand is encountered, add it to DATALIST
4. If an operator is encountered, add it to SYMBOLLIST.
5. Scan DATALIST from left to right and perform steps 6 to 7 until the DATALIST is
   empty.
6. Push the data on to stack
7. Scan SYMBOLLIST from left to right and perform steps 8 to step 9.
8. Push the symbol onto stack.
9. Go to step 5.
   End of step 5
10. Display the contents of stack
11. Exit
```

7.1 Multiple Symmetric Keys

Key1 :	0.10000233430123
Key2 :	0.19786574564624
Key3 :	0.13465632430123
Key4 :	0.15891672189911

Input : American Online Services
Polish Output : Aren acimnln eiOrveceiSs

7.2 Encrypted Data

```
270006296376766366
530012314596584456
130003044294281134
530012314596584456
180004215176696955
500011708824158208
712316620137658581
```

```
201984490554915815
395731563139836150
121190678499982049
554024030066095621
484762713999928197
197865790366011097
363572009111667081
870609210209220952
201984490554915815
356158310068829290
824096751018929082
364726863557715558
216704615888139059
364726863557715558
191634871165544038
662152977720541184
539181645636934042
```

7.3 Decrypted Data: American Online Services

8. CONCLUSION

It is concluded that reverse polish notation or polish notation is used to shuffle the contents of text file. The shuffling is done by simulated polish notation whose throughput established muddling characters in the text file. The shuffling can be enhanced by altering the characters fixed for operands and operators. The effect of polish notation is tested in cryptosystem.

REFERENCES

[1] S.S.Dhenakaran,(2007), "A New Approach to Multiple Symmetric Keys" IJCSNS, Vol 7, No. 6, pp. 254-259, June 2007.

[2] S.S.Dhenakaran, (2007), "Cryptosystem using Multiple Symmetric Keys" workshop, organized by National Technical Research Organization at PSG Tech, Coimbatore, Tamil Nadu, during 22-23, June 2007.

[3] S.S.Dhenakaran, (2008), "Crypto System using Banach Fixed Point Theorem" in International Journal of Discrete Mathematical Sciences and Cryptography Vol.11, No. 5, pages 579-587 , Oct. 2008.

[4] Abdel-Karim AI Tamimi, (2006), "Performance Analysis of Data Encryption Algorithms", Lecture Notes CSE, 567 M: Computer Systems Analysis, Washington University in St. Louis, 2006.

[5] Bruce Schneier, (1996), "Applied Cryptography Second Edition: protocols, Algorithms and Source Code in C", John Wiley & Sons, New York, 1996.

[6] Damgard.I.B and Knudsen.L.R, (1998), "Two-Key triple encryption", The Journal of Cryptography , Vol. 11, No.3, Springer, Newyork, pp. 209-218, 1998.

[7] Syverson. P and Meadows.C, (2003), "A logical language for specifying Cryptographic protocol requirements", In Proc. 14th IEEE Symposium on Security & privacy, pp. 165-177, 2003.