A New Approach to Multiple Symmetric Keys

Dhenakaran S.S [1], Naganathan E.R [2]
ssdarvind@yahoo.com
[1]Department of Computer Science and Engineering
Alagappa University, Karaikudi – 630 003.
Tamil Nadu, India.

[2]Department of Computer Science and Engineering
Alagappa University, Karaikudi – 630 003.
Tamil Nadu, India.

Summary

Cryptosystem provides a cornerstone for secure information. Cryptosystems list many mechanisms on which security techniques and technologies are built. This paper demonstrates the generation of multiple symmetric keys to secure information. Preliminary studies of Newton-Raphson method, RSA algorithm, Modified Newton-Raphson method and proposed model using multiple symmetric keys are presented.

1.INTRODUCTION

It is well known that the cryptosystems convert readable data into gibberish to provide security for vital information. A cryptosystem takes a plaintext as input and produces encrypted text known as ciphertext. The strength of the algorithm that works behinds the Cryptosystem makes the ciphertext difficult to understand and a challenging job for intruders and attackers. In addition to keeping secrets, a cryptosystem can add security to the process of authenticating people's identity to get back the information from senders.

Symmetric key or Asymmetric keys are used to lock and unlock data. It is known that the symmetric encryption is a form of cryptosystem in which encryption are performed using the same key. It is also known as conventional encryption. Preneel[5] has carried out the study of the developments in conventional cryptosystem. The symmetric encryption transforms plaintext into ciphertext using a secret key and an encryption algorithm. Using the same key and a decryption algorithm, the plaintext is recovered from the ciphertext. The symmetric ciphers use substitution or transposition techniques. Laud[6] has made comments about the symmetric system for hopefulness and Magliveras[4] focused the importance of algebraic properties of the cryptosystem. The Substitution techniques map plaintext elements into ciphertext elements.

Transposition techniques transpose the positions of plaintext elements. Similarly asymmetric encryption transforms the plaintext to ciphertext and vice-versa using different keys. The New Mathematical algorithm [1] for finding the roots of the real valued function and modified algorithm have applied to many applications to find solutions.

Impagliazzo[2] has carried out the study of the requirements for secure use of conventional encryption.

1. It requires a strong encryption algorithm. At a minimum, the algorithm to be such that an opponent who knows the algorithm and has access to one or more ciphertext would be unable to decipher the ciphertext or figure out the keys. This requirement is usually stated in a stronger form.
2. Sender and receiver must have obtained copies of the secret key in a secure fashion and must keep the key secure.

Realizing the importance of securing the information, at most care is taken to design the proposed mathematical algorithm and finding the multiple symmetrickeys. The cryptanalytic attack

on the nature of algorithm and Brute-force attack on key finding would be difficult in this method. The rest of the paper is focused as follows. Section 2 presents the basics of solving real valued functions. The RSA encryption is provided in Section 3. Section 4 presents the Modified Newton-Raphson method to solve mxn system of equations and section 5 demonstrates proposed system with multiple symmetric keys for encryption. Conclusion part is represented in section 6 of the paper.

2. NEWTON-RAPHSON METHOD

The Newton-Raphson method is used to improve the result obtained from initialization. Let x_0 be the initial approximate root of the real valued function f(x) = 0. Let $x_1 = x_0 + h$ be the next approximate of the function f(x) = 0. Expanding $f(x_0 + h)$ by Taylor's series, we obtain

$$f(x_0) + h\, f'(x_0) + h^2 / 2!\ f''(x_0) + \ldots\ldots\ldots = 0.$$

Neglecting the second and higher order derivatives , we have

$$f(x_0) + h\, f'(x_0) = 0.$$

This gives the value of h as

$$h = - f(x_0) / f'(x_0)$$

A better approximation than the value of x_0 is given by x_1. That is,

$$x_1 = x_0 - f(x_0) / f'(x_0).$$

Successive approximation for the variables $x_2, x_3, x_4 \ldots\ldots x_{n+1}$ are given by

$$x_{n+1} = x_n - f(x_n) / f'(x_n). \quad \ldots\ldots\ldots\ldots\ldots\ldots (1)$$

Equation (1) is known as Newton-Raphson formula. It is simply called Newton method of finding the root of the equation. Newton's formula converges provided the initial approximation x_0 is chosen sufficiently close to the root. Thus a proper choice of initial value is very important for the success of the Newton's method. Geometrically, the method provides the following steps to reach the solution.

Procedure for finding value of x

1. Draw the curve of the function f(x) = 0 on the XOY plane.
2. Draw a normal at x_0 to the curve. Let the normal meets the curve at $(x_0, f(x_0))$.
3. Draw a tangent at $(x_0, f(x_0))$ on the curve and let the tangent meets the x-axis at x_1 which is the next approximated root of the function f(x)=0.
4. This process is repeated for newer approximations to find the exact root of the function f(x) = 0.

The geometrical representation of the method is shown below.

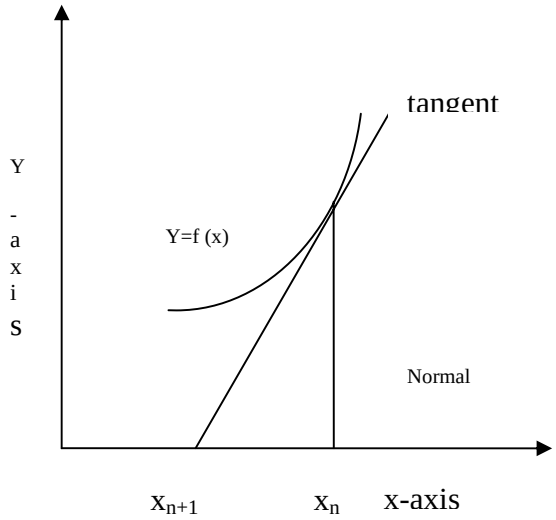

fig 1 Newton-Raphson Method

The closer approximation to the root is given by

$x_1 = x_0 - f(x_0) / f'(x_0)$
$x_2 = x_1 - f(x_1) / f'(x_1)$
$x_3 = x_2 - f(x_2) / f'(x_2)$
…….
…….
$x_n = x_{n-1} - f(x_{n-1}) / f'(x_{n-1})$
$x_{n+1} = x_n - f(x_n) / f'(x_n)$

3. RSA ALGORITHM

RSA is an Internet encryption and authentication cryptography system developed in 1977 by three Mathematicians Ron Rivest, Adi Shamir and Len Adleman and hence the acronym RSA. The RSA cryptosystem is based on modular exponentiation modulo of the product of 2 large primes. Each individual has an encrypting key consisting of a modulus n = pq; where n is called

the modulus , p & q are large primes and an exponent e that is relatively prime to (p-1)(q-1). The selection of large primes lead the difficulty to break the ciphertext.

RSA ENCRYPTION

In the RSA encryption method, messages are translated into sequence of integers. This can be done by translating each letter into an integer. These integers are grouped together to form large integers, each representing a block of letters. The encryption proceeds by transforming the integer M, representing the plaintext to an integer C, representing the ciphertext (the encrypted message) using the function

$C = M^e \mod n$

RSA DECRYPTION

The plaintext message can be recovered when the decryption key d, an inverse of e modulus (p-1)(q-1) is known. The original plaintext P is obtained using the function

$P = C^d \mod n$

4. MODIFIED NEWTON-RAPHSON ALGORITHM

This mathematical method is a novice technique for finding solutions to a set of linear equations. The algorithm finds solution to the set of m linear equations in n unknown variables with unique solution. The algorithm is derived from the Newton-Raphson method of finding approximate value to the root of an equation.

Let the m equations be in the form

$a_{11}\ x_1 + a_{12}\ x_2 + \ldots\ a_{1n}\ x_n = b_1$
$a_{21}\ x_1 + a_{22}\ x_2 + \ldots\ a_{2n}\ x_n = b_2$
……...
$a_{m1}\ x_1 + a_{m2}\ x_2 + \ldots a_{mn}\ x_n = b_m$

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

$f_1\ (x_1,x_2,x_3\ldots\ldots.x_n,b_1) = 0$
$f_2\ (x_1,x_2,x_3\ldots\ldots.x_n,b_2) = 0$
…….
$f_m\ (x_1,x_2,x_3\ldots\ldots.x_n,b_m) = 0$

Let x_0 be the initial approximation to the root of the functions $f_1(x),f_2(x)\ldots\ldots..f_m(x)$ and next approximation be $x_1 = x_0 + h$.to the functions $f_1(x),f_2(x)\ldots\ldots..f_m(x)$. That is,

$f_1\ (x_0 + h) = 0$
$f_2\ (x_0 + h) = 0$
…….
$f_m\ (x_0 + h) = 0$

Using Taylor's theorem we get,

$f_1\ (x_0) + h\ f_1'(x_0) + h^2\ f_1''(x_0) + \ldots = 0$
$f_2\ (x_0) + h\ f_2'(x_0) + h^2\ f_2''(x_0) + \ldots = 0$
……

$f_m\ (x_0) + h\ f_m'(x_0) + h^2\ f_m''(x_0) + \ldots = 0$

Since h is small, neglecting the higher powers of h, we get

$f_1(x_0) + h\ f_1'(x_0) = 0$ implies $h = - f_1(x_0)/ f_1'(x_0)$
$f_2(x_0) + h\ f_2'(x_0) = 0$ implies $h = - f_2(x_0)/ f_2'(x_0)$
…….
$f_m(x_0) + h\ f_m'(x_0) = 0$ implies $h = - f_m(x_0)/ f_m'(x_0)$

From the value h , the next approximation is obtained as

$x_1 = x_0 - f_1(x_0) / f_1'(x_0)$
$x_2 = x_1 - f_1(x_1) / f_1'(x_1)$
$x_3 = x_2 - f_1(x_2) / f_1'(x_2)$
…….
$X_n = x_{n-1} - f_1(x_{n-1}) / f_1'(x_{n-1})$

Generalizing for m real valued functions we get,

$x_i = x_{i-1} - f_j(x_{i-1}) / f_j'(x_{i-1})$

where i=1 ,2,3…….n and
j = 1,2,3…….m

The Newton-Raphson method provides a formula to find new value of x as

$X_{n+1} = x_n - f(x_n) / f'(x_n)$

Since the modified Newton-Raphson method considers normal line instead of tangent line a closer approximation to the root of the equation is obtained by modifying Newton formula as shown below.

$X_{n+1} = x_n - f(x_n) * f'(x_n)$

The geometrical representation of this method is shown in the following diagram.

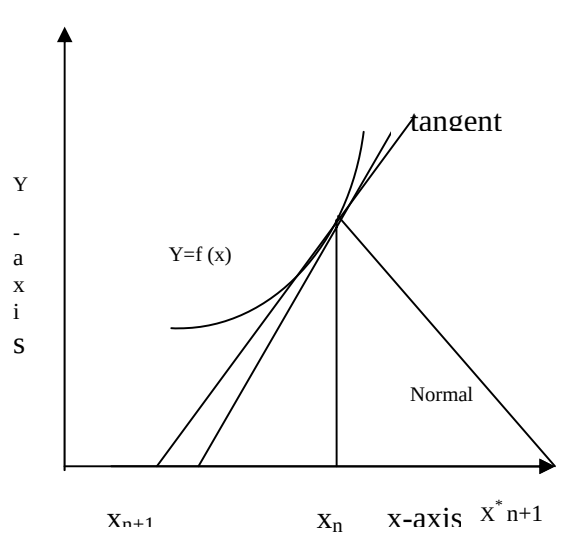

fig 2 Modified Newton-Raphson method

Procedure for finding next value of x

1. Let x_n be an initial value of x
2. Draw a normal to the x-axis at the point x_n.
3. Let the normal meets the curve at the point $y_n = f(x_n)$.
4. Draw a tangent to the curve at the point (x_n, y_n) and draw a normal to the tangent and let the normal to the tangent meets the x-axis at x^*_{n+1}.
5. Take x_{n+1} to the left of x_n as the next approximation by assuming the distance between x_n to x_{n+1} is equal to x_n to x^*_{n+1}.
6. This process of finding new value of x is repeated till it satisfies the given equations.

The matrix form for finding the new value of x to the set of m linear equations in n unknown variables are given below.

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

$$x_n^{(k+1)} \quad x_n^{(k)} \quad \frac{\partial f_1 \ldots \partial f_m}{\partial x_n \quad \partial x_n} \quad f_m(x_1^k..x_n^k)$$

Assuming that the system of linear equation obtained solution at the k^{th} approximation, we have the real valued functions as shown below.

$f_1(x_1^k, x_2^k x_3^k \ldots .x_n^k, b_1) = 0$
$f_2(x_1^k, x_2^k x_3^k \ldots .x_n^k, b_2) = 0$
$f_3(x_1^k, x_2^k x_3^k \ldots .x_n^k, b_3) = 0$
……..
……..
$f_m(x_1^k, x_2^k x_3^k \ldots .x_n^k, b_m) = 0$

5. PROPOSED NAMSK ALGORITHM

The proposed **N**ew **A**pproach to **M**ultiple **S**ymmetric **K**eys algorithm [**NAMSK**] has used the modified Newton-Raphson method and RSA algorithm. The modified Newton's method is used to generate multiple symmetric keys from the alphanumeric primary key and digital signature. These two prime elements are most essential to generate the multiple keys. The length of the primary key and digital signature would be helpful to generate higher digits symmetric keys.

From the primary key and digital signature the algorithm first generates different patterns based on the characteristics of the characters. These patterns are further used to find two linear equations in n unknown variables. The coefficients of the unknowns are calculated from the two prime elements. Let the two linear equations be represented as

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

where $a_{11}, a_{12}, a_{13} \ldots a_{1n}$
$a_{21}, a_{22}, a_{23} \ldots a_{2n}$ and
b_1, b_2 are known constants.

Let these two equations be represented as the real valued functions as

$f_1(x_1^k, x_2^k x_3^k \ldots .x_n^k, b_1) = 0$
$f_2(x_1^k, x_2^k x_3^k \ldots .x_n^k, b_2) = 0$

Using the Modified Newton-Raphson method, the above real valued functions are solved and

the solution of the variables are taken as the multiple keys of the proposed algorithm.

Next the RSA algorithm is used with two prime numbers to convert the plaintext to ciphertext1. The output of the RSA ciphertext1, is further used as input to another part of the proposed encryption algorithm with the multiple keys to generate ciphertext2 which is the desired ciphertext of the new cryptosystem.

NAMSK ENCRYPTION

In the NAMSK encryption method, plaintext are translated into sequence of integers. This can be done by translating each letter into an integer using the RSA algorithm with the prime numbers. The RSA part of encryption transforms the integer M, representing the plaintext to an integer C representing the ciphertext1. Further the integers C of the ciphertext1 are grouped together to form large integers C_{New} using the multiple keys of the proposed algorithm. Damgard[2] triple encryption process with two-key system are analysed for better system. The group of large integers are forming the ciphertext2 which is the desired ciphertext of the proposed system.

$C_{New} = M_i^{\ e} \bmod n * 1 / k(xi)$
$C_{New} = C^1_{New}\ C^2_{New}\ C^3_{New}\ldots\ldots C^n_{New,}$ a group of encrypted values

Where i = 1,2,……..n .

$K(x_i)$ are multiple symmetric keys generated.

$C^1_{New}\ C^2New\ C^3_{New}\ldots\ldots C^n_{New}$ are converted integer values which got by left rotation as many times as possible to meet the required value.

NAMSK DECRYPTION

The plaintext message can be recovered when the decryption key d, an inverse of e modulus (p-1)(q-1) is known and used from the RSA algorithm. The original plaintext P is obtained using the function with the multiple keys

$$P = (C^i_{New} * k(x_i))^d \bmod n$$

Where i=1,2,3…… n.

$P = P_1, P_2, P_{3.....} P_n$ a group of decrypted text values which got by right rotation as many times as possible to get the requisite values.

NAMSK ALGORITHM

1. Input : Read an alphanumeric key of any size not exceeding 1000 characters. Also read a digital signature as another key.
2. Initialize an algorithm to find numerical solution of these two input keys by forming multi varied linear equations.
3. Let the multivariate key be x1,x2,….xn.
4. Read two random numbers P and Q as in RSA method.
5. Find the value of phi,e,d as in RSA method.
   // Encryption process
6. while (Text message != EOF)
   do

   $C_{New} = M_i^{\ e} \bmod n * 1 / k(xi)$

   Rotate the value of C_{New} to the left as many times to get the desired output.

   Display C_{New} // encrypted value

   done
   // Decryption process
7. while (encrpyted message != EOF)
   do

   Rotate the value of C_{New} to the right as many times to get the desired output.

   $P = (C^i_{New} * k(x_i))^d \bmod n$

   Display P // Plaintext

   done
8. Exit

6. CONCLUSION

The paper has demonstrated the newer method of encryption and decryption using a Mathematical Technique. This technique is useful for the refinement of the cipherhtext to increase the complexity to produce the better ciphertext. The refinement process may be continued to give next better ciphertext. As the method is depending on multiple symmetric keys which has found by a newer mathematical

algorithm and to the best of our knowledge it would be difficult to attackers for cryptanalysis.

REFERENCES

[1] S.S.Dhenakaran and Dr.C.Ganesamoorthy, A New Mathematical Model to solve Linear Equations , Modified Newton-Raphson method, National Conference , Central Electro Chemical Research Institute, India.

[2] R.Impagliazzo and B.M.Kapron, Logics for reasoning about Cryptographic Constructions. In Proc. 44 th IEEE Symposium on foundations of Computer Science, pages 372-381, 2003.

[3]I.B.Damgard and L.R.Knudsen, Two-Key triple encryption. The Journal of Cryptography, 1997.

[4]S.S.Magliveras and N.D.Memon. Algebraic properties of Cryptosystem PGM. Journal of Cryptology 5(3) : 167-184,1992.

[5]B.Preneel, V.Rijmen and A.Bosselaers, Recent developments in the design of convetional cryptographic algorithms. This volume, pages 106-131.

[6]P.Laud . Symmetric encryption in automatic analyses for confidentiality against active adversaries. In Proc. 25th IEEE Symposium on Security & privacy , pages 71-85,2004.

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

APPENDIX

S.S.Dhenakaran Senior Lecturer working in the Department of Computer Science and Engineering Alagappa University,Karaikudi, India. He has completed his M.Sc in Mathematics in Madurai Kamaraj University, Tamil Nadu, India in the year 1984, PGDOR from Anna University, Chennai, Tamil Nadu, India during 1986, MCA degree from Bharathidasan University, Tamil Nadu, India during 2003 and M.Phil Computer Science from Bharathidasan University, Tamil Nadu, India during 2005.He has 19 years of teaching experience in the field of computing. He has presented two papers in National Conferences. His area of interest is Cryptography and Computer Graphics and Optimization techniques.

Dr.E.R.Naganathan Reader and Head, Department of Computer Science and Engineering, Alagappa University, Karaikudi, India. He has completed his M.Sc Applied Maths from Thiagarajar College of Engineering, Madurai, India in the year 1985. He has received his Ph.D in Computer Applications from Alagappa University, Karaikudi, Tamil Nadu, India in the year 2000. He has 20 years of teaching experience in the field of computer science. Also he has visited Jordon as Assistant Professor for two years in the Department of Computer Science, Jerash University. Moreover he has worked as Professor in Sona Engineering College, Salem India for one year. He has presented many papers in National and International journals. His area of interest is Optimization techniques, Cryptography and NetworkSecurity.