Global Journal of Pure and Applied Mathematics.
ISSN 0973-1768 Volume 13, Number 7 (2017), pp. 3105-3112

http://www.ripublication.com

Public Key Cryptosystem Based on Numerical Methods

Inaam Razzaq AL-Siaq

Department of Mathematics, Faculty of Computer Science and Mathematics, Kufa University, Iraq.

Abstract

Nowadays, Public key Cryptosystem offers security features of many products which are need ataraxy electronic communication through an open networked like the internet and wireless com- munication. Diffie Hellman key commutation is a determined method of securely alternate keys through open channel, actually it is one of the first public key cryptosystems. Numerical analysis offers many methods to study of algorithms that use numerical approximation for the problems of mathe- matics. In this work we will introduce a public key cryptosystem using Diffie Hellman key exchange to transfer function and encrypted/ decrypted it using numerical methods to enhance the security electronic communication over a public channel.

Keywords: Diffie Hellman Key Exchange, Bisection Method, Fixed Point Iteration, Newton-Raphson method.

INTRODUCTION

Public key cryptosystems are set of affirmed techniques and standards for maintain communi- cations from eavesdropping, manipulating attacks. For instance, when a any browser such as G*oogle Chrome* is used for home banking, numbers of cryptographic algorithms have been pro- posed to protect data that send to the bank [1]. So, a public key cryptosystem is a technique that is used a pair of keys to encrypt and decrypt a message such that it arrives securely. In brief, a user receives a common and specific key from a testimony authority. Any other employer who would like to send an encoding message can be get the receiver's public key from a public directory. The

employers are use this key to encoding the message, and they will be send it to the receiver. When the receiver gets the message, they decoding it from their special key, that is no person else should have access to do [2].

The process of encoding the messages into unreadable format that can on read by an au- thorized one is called an encryption. While the decryption is operation of converting code into plain text. In other words, decryption is the reverse of encryption. It transforms encoded data connecting send off and files to their original states.

The Diffie Hellman key commutation protocol has evolved by Diffie and Hellman [3] in 1976. In that paper, they also introduced the revolutionary concept of public key cryptography. This system is merely a method for exchanging key; no messages are involved. The following algorithm illustrates this system.

In this paper, we propose an algorithm to encrypt and decrypt messages within public chan- nel using three numerical methods: Bisection Method, Fixed Point Iteration and Newton Raphson Method. If anyone tries to attack the proposed system, he will have the $BP\ M$ file,then with con- verting this file to array form. The problem is recovering the original text using the array in term of recovering system of solutions which is already dependent on function that exchange using Diffie Hellman key exchange algorithm. So, the attacker will face the hard mathematical problem "Discrete Logarithm Problem" [4].

PUBLIC KEY CRYPTOSYSTEM

Public key cryptosystem is a set of cryptographic algorithms that are depend on mathematical problems that acknowledge no active solution such as discrete logarithm. Employer can compute easy to create a public and private key pair and it use for encoding and decoding. The strength inside the computational impracticability for a really created private key to determine from its congruent public key. Therefore the public key can be published without disclose security. Security only depends on protection the special key is special.

In 1976, an public key cryptosystem was published by Diffie and Hellman [3]. This method of key commutation, the method may be use exponentiation in a finite field, thus it can be known as Diffie Hellman key exchange protocol. The first published was practical method for establishment a participate secret key overhead an authenticated.

Diffie Hellman Key Exchange protocol

Diffie and Hellman worked in the early 1970s, to develop the fundamental ideas of dual key, or pub- lic key cryptosystem. They were solving one of the main problems of cryptography. The solution has become known as Diffie Hellman key exchange protocol. This protocol can be summarized in the **Figure** 1.

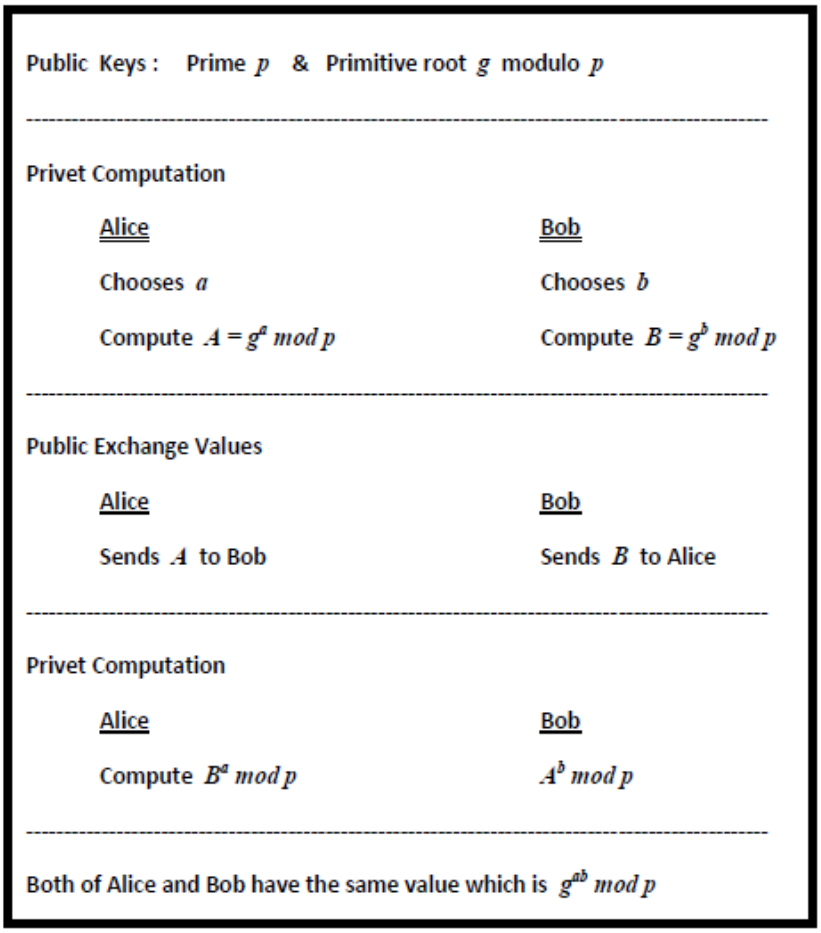

Figure 1: Diffie Hellman Key Exchange

The attacker has the value of p, g, $g^a modp$ and $g^b modp$. The discrete logarithm problem is to compute a or b from $g^a modp$ or $g^b modp$ respectively [5].

NUMERICAL METHODS

The solution of equations of the form f(x)=0 obtains in many applications. If a polynomial is f(x) of degree two or three or four, exact formulae are obtainable. But, if f(x) is a polynomial of order is higher or a transcendental function, the solution is not exist, therefore the numerical methods is very important to find approximate root. [1]

(2-1)Theorem:

Suppose f(x) is continuous function in the interval (a,b) and if f(a) and f(b) are different signs, then f(x)=0 will have at least one real root lies between a and b.[1]

(2-2)Bisection Method:

Presume we have f(x)=0 an equation whose solution is to be searched in the range (a,b). We suppose f(x) is continuous and if f(a) and f(b) are different signs then at least one real root lies between a and b should exist. Let f(a) is positive and f(b) is negative. Then a first approximation x_0 is midpoint of the ends of the range .Now, find the sign of$f(x_0)$. If$f(x_0)$ is negative, then the root lies in interval [a, x_0]. Assume that$f(x_0)$ is positive, then the root in interval [x_0 ,b] and take root as $x_1 = \frac{x_0+b}{2}$,if $f(x_1)$ is negative hence the root in interval[x_0, x_1] then the approximate root

$x_2 = \frac{x_0+x_1}{2}$ .Now if $f(x_2)$ is negative then the root lies between x_0 and x_2 and so on.

However, we stop the process after some steps when the sequence of approximate roots $x_0, x_1, x_2, \ldots$ is convergence. This method is slow convergence but sure.

(2-3)Fixed –Point Iteration Method.

Assume that we want the approximate roots of f(x) =0 …(1)

Now, it can be turn into the form

$$x = \Phi(x) \quad \ldots (2)$$

And then the iterative will be used with the recursive function

$$x_{i+1} = g(x_i), \qquad i = 0,1,2, \ldots$$

Assume x_0 to be the initial guess value to the actual root α of $x = g(x)$. Setting $x=x_0$ in the right hand side of (2), we get the first approximation

$$x_1 = g(x_0)$$

Again setting $x=x_1$ on the R.H.S. of (2) we get successive approximations.

$x_2 = g(x_1)$

$$x_3 = g(x_2)$$

……..

…….....

$x_n = g(x_{n-1})$

The sequence of approximate roots $x_1, x_2, \ldots, x_n$, if it converges to α is taken as the root of the equation f(x)=0.[1]

(2-3-1) The condition for the convergence of the method.

Theorem.

Let f(x) =0 be the given equation whose actual root is α . We will rewrite the equation f(x)=0 to equation as $x=g(x)$. Let *I* be the interval containing the root x=α. If

$|\acute{g}\ (x)| < 1$ for all x in *I*, then the sequence of approximations x_0 ,x_1 ,…,x_n will converge to α , if the initial starting value x_0 is chosen in *I*.[1]

(2-4)Newton-Raphson method

Suppose that $x_0$be an approximate value of a root of f(x)=0

Let x be the exact root nearer to x_0

Then $x = x_0 + h$ such that h is very small, it may be positive or negative.

$\therefore\ f(x) = f(x_0 + h) = 0$ Since x is the exact root of f(x)=0

Now, By Taylor expansion,

$f(x) = f(x_0 + h) = f(x_0) + h\acute{f}(x_0) + \frac{h^2}{2!}\ f''(x_0)$+…=0

i.e., If h is small, neglecting h^2 ,h^3,…etc, we get

$f(x_0) + h\acute{f}\ (x_0) \approx 0$

$\therefore \qquad h \approx -\frac{f(x_0)}{\acute{f}\ (x_0)} \quad if \quad \acute{f}(x_0) \neq 0$

$\therefore \qquad x = x_0 + h = x_0 - \frac{f(x_0)}{\acute{f}(x_0)}$ approximately

Assume the value be x_1

$\therefore \qquad x_1 = x_0 - \frac{f(x_0)}{\acute{f}(x_0)}$

x_1 is a better approximate root than α_0

Now, starting with thisx_1, we get

$x_2 = x_1 - \frac{f(x_1)}{\acute{f}(x_1)}$ Which is still better.

Continuing like this, the process iterate until $|x_{r+1} - x_r|$ is less than the quantity desired.

$$\therefore \qquad x_{r+1} = x_r\ - \frac{f(x_r)}{\acute{f}\ (x_r)} \qquad ,r = 0,1,2, \ldots$$

This is the iterative formula of Newton – Raphson method.[1]

(2-5)Proposed Work

In this section, we will algorithms to Encryption and Decryption message within public channel using the numerical methods.

3.1. Proposed Algorithm

The Algorithms for Encryption and Decryption are as follows:

3.1.1. Algorithm for Encryption

Step 1: Convert the tact message to the decimal for using ASSCII technick

Step 2: Using Diffie Hellman technick to receive the function.

Step 3: Construct system of equation by subtract the ASCII values from the function received and equaled with zero.

Step 4: An array from the solutions of the system of equations.

Step 5: Convert the array to the BMP file.

Step 6: Sending the BMP file in public channel.

3.1.2. Algorithm for Decryption:

Step 1: Read the BMP file

Step 2: create the array using data from BMP file and insulates the actual pixels from Garbage

Example:

If we use the statement "Mathematics is the king of all Science" to Encryption and Decryption by the real root of the function

$f(x)=3.5x^3+xe^x$ and numerical methods.

CONCLUSION

In these paper we find that Newton-Raphson method is the best numerical method where Approximate root finding in the fifth iteration, followed by fixed-point method where the root finding in the eighth iteration, Finally way Bisection method is bad and that the way to find Approximate root in iteration fifteen bearing the error as shown in the following table.

The letters	Newton-Raphson method	The Error	The iteration	Fixed –point method	The Error	The iteration	Bisection method	The Error	he iteration
M	2.421812323945733	zero	5	2.421812323951231	5.505569333763560e-010	50	2.421812323945733	zero	50
a	2.603996247265451	zero	5	2.603996246698666	6.796656748520036e-008	50	2.603996247265451	zero	50

t	2.751402009304901	zero	6	2.751401948643810	8.386478498323413e-006	50	2.751402009304904	4.547473508864641e-013	50
h	2.660773966863740	2.842170943040401e-014	20	2.660773963189985	4.655127554542560e-007	50	2.660773966863741	2.842170943040401e-014	50
e	2.636822831140274	zero	5	2.636822829439560	2.105597189938635e-007	50	2.636822831140274	zero	50
m	2.699500064768203	2.842170943040401e-014	5	2.699500052412652	1.625208568611924e-006	50	2.699500064768203	2.842170943040401e-014	50
a	2.603996247265451	zero	5	2.603996246698666	6.796656748520036e-008	50	2.603996247265451	zero	50
t	2.751402009304901	zero	6	2.751401948643810	8.386478498323413e-006	50	2.751402009304904	4.547473508864641e-013	50
i	2.668635857201623	2.842170943040401e-014	20	2.668635852489564	6.016345821535651e-007	50	2.668635857201623	2.842170943040401e-014	50
c	2.620540551352826	zero	5	2.620540550358875	1.211263906952809e-007	50	2.620540551352826	zero	50
s	2.744143668610717	zero	6	2.744143619981124	6.676583979015049e-006	50	2.744143668610718	5.684341886080802e-014	50
i	2.668635857201623	2.842170943040401e-014	20	2.668635852489564	6.016345821535651e-007	50	2.668635857201623	2.842170943040401e-014	50
s	2.744143668610717	zero	6	2.744143619981124	6.676583979015049e-006	50	2.744143668610718	5.684341886080802e-014	50
t	2.751402009304901	zero	6	2.751401948643810	8.386478498323413e-006	50	2.751402009304904	4.547473508864641e-013	50
h	2.660773966863740	2.842170943040401e-014	20	2.660773963189985	4.655127554542560e-007	50	2.660773966863741	2.842170943040401e-014	50
e	2.636822831140274	zero	5	2.636822829439560	2.105597189938635e-007	50	2.636822831140274	zero	50
k	2.401635833633491	zero	5	2.401635833637873	4.299494094084366e-010	50	2.401635833633491	5.684341886080802e-014	50
i	2.668635857201623	2.842170943040401e-014	20	2.668635852489564	6.016345821535651e-007	50	2.668635857201623	2.842170943040401e-014	50
n	2.707074838821676	2.842170943040401e-014	5	2.707074823207412	2.068867800630869e-006	50	2.707074838821675	2.842170943040401e-014	50
g	2.652851834626772	4.263256414560601e-014	20	2.652851831773039	3.588435362189557e-007	50	2.652851834626772	4.263256414560601e-014	50
o	2.714594848117094	1.421085471520200e-014	6	2.714594828432898	2.627043812708507e-006	50	2.714594848117094	1.421085471520200e-014	50
f	2.644868463735351	zero	5	2.644868461527465	2.754923542624965e-007	50	2.644868463735353	1.705302565824240e-013	50
a	2.603996247265451	zero	5	2.603996246698666	6.796656748520036e-008	50	2.603996247265451	zero	50
l	2.691869668998128	2.842170943040401e-014	5	2.691869659246503	1.273307788096645e-006	50	2.691869668998128	2.842170943040401e-014	50
l	2.691869668998128	2.842170943040401e-014	5	2.691869659246503	1.273307788096645e-006	50	2.691869668998128	2.842170943040401e-014	50
S	2.480001811315051	zero	5	2.480001811320454	5.734079877584009e-010	50	2.744143668610718	5.684341886080802e-014	50
c	2.620540551352826	zero	5	2.620540550358875	1.211263906952809e-007	50	2.620540551352826	zero	50

i	2.668635857201623	2.842170943040401e-014	20	2.668635852489564	6.016345821535651e-007	50	2.668635857201623	2.842170943040401e-014	50
e	2.636822831140274	zero	5	2.636822829439560	2.105597189938635e-007	50	2.636822831140274	zero	50
n	2.707074838821676	2.842170943040401e-014	5	2.707074823207412	2.068867800630869e-006	50	2.707074838821675	2.842170943040401e-014	50
c	2.620540551352826	zero	5	2.620540550358875	1.211263906952809e-007	50	2.620540551352826	zero	50
e	2.636822831140274	zero	5	2.636822829439560	2.105597189938635e-007	50	2.636822831140274	zero	50

REFERENCES

[1] Nagunwa T.;"Examining Usage of Web Browser Security Indicators in e-banking:A Case Study"; International Journal of Advanced Research in Computer Science and Software Engineering; Volume 4,Issue 9,September 2014.

[2] Alfred J.Menezes, Paul C.Van Oorschot and Scott A.Vanstone; "Handbook of Applied Cryptography";1996.

[3] Whitfield D. and Martin E.Hellman;"New Directions in cryptograhy" ;IEEE Transactions on Information Theory;Vol.22,No.6 November 1976.

[4] Song Y.Yan; "Number Theory for Computing"; Second Edition.(2002).

[5] J.Buchmann;" Introduction to cryptography"; 2nd ed.(2004)

[6] Kandasamy , P. Thilagavathy, K.& Gunavathy,k., Numerical Methods, S.Chand and Co.New Delhi 2008.

[7] Saxena , H.C. ,Finite Differences and Numerical Analysis,S.Chand and Co.New Delhi 2008.