Volume 4, Issue 3, March 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

ACBS: Asymmetric Cryptography Based on SPHERE

Gurjinder Kaur
Depatment Of Computer Science
Lovely Professional University
India

Simarjit Singh (Asst. Prof.)
Depatment Of Computer Science
DIPS College Dhilwan
India

Anu Garg (Asst. Prof).
Depatment Of Computer Science
Lovely Professional University
India

Abstract— Cryptography is the scheme that is used to encrypt a simple text. It hides the meaning of the message. It pays an important role in security over a network. In this proposal we present a cryptography system that is based on the Sphere (a shape in mathematics). Sphere is locus of point in space which moves in such a way that its distance from fixed point always remain constant, where fixed point is the center of the sphere and constant distance is the radius of sphere. We used the sphere concept for implementing the asymmetric cryptography. In this system public key and private key are generated by using the property of Sphere. Here we choose a point which lie on the sphere as my private key and take the center of sphere (fixed point) as my public key. This key management provides more security against attacks.

Keywords— Cryptography, Encryption, Decryption, Symmetric cryptography, Asymmetric cryptography, Sphere.

I. INTRODUCTION

The term Network Security and Cryptography is very broad itself. The term Network means more than one systems are connected to each other. In the early 1960s, a single computer had to be physically shared. It makes difficult to sharing of data and other information. For solution of this problem the researchers were developed a way to "connect" the computers, so they could share their resources more efficiently. Hence, the computer network was born. In 1977, early PC-based Local Area Networks, or LANs (Local Area Networks) were spreading which include academics. LAN variants also developed, including Metropolitan Area Networks (MANs) to cover large areas such as a college campus, and Wide Area Networks (WANs) for university-to-university communication. From the very first day of the network it is thinking of the wired technology but now it is 20th century, which adopted the Wireless Networking technology. Before the 90s, networks were not common to all and the general people were not the heavy internet users. During these times, security was not a serious issue in networking. In the 80s, use of the network began to grow very quickly. So the need for security was also growing because the universities, government and military installations are connecting. Cryptography is the scheme that is used to encrypt a simple text. It hides the meaning of the message. It basically derived from the Greek word kryptos , which means hidden. It pays an important role in security over a network. Cryptography algorithms are the mathematical functions that are used for encryption and decryption. Different cryptographic algorithms have different degree of security. The degree of security depends upon the fact that how much an algorithm is hard? How much time to be needed to break the algorithm? If more time is required to break an algorithm than the time to decryption of message then the applied algorithm is probably safe or secure. We use the term probably because there is always a backdoor in every system. Cryptography is of two types: one is symmetric cryptography and other is asymmetric cryptography.

A) Symmetric Cryptography

Symmetric cryptography is the cryptosystem in which a single key or the same key is used to encrypt and decrypt the message. So the symmetric cryptography is also known as shared key or single key cryptography. There are basically two techniques substitution and the transposition techniques, in symmetric cryptography. In substitution technique mapping is done from plain text into cipher text. In transposition technique, transpose the position of plain text elements taken with systematically. A number of symmetric key encryption algorithms like DES, TRIPLE DES, AES, BLOWFISH have been developed to provide greater security affects. Figure 1.1 shows the encryption and decryption of a plain text or message. The input to the encryption process is plain text and that of decryption process is cipher text. First the plaintext is passed through the encryption algorithm which encrypts the plaintext using a key and then the produced cipher text is transmitted At the end of decryption, the input cipher text is passed through the decryption algorithm which decrypts the cipher text using the same key as that of encryption. Finally we get the original plaintext message.

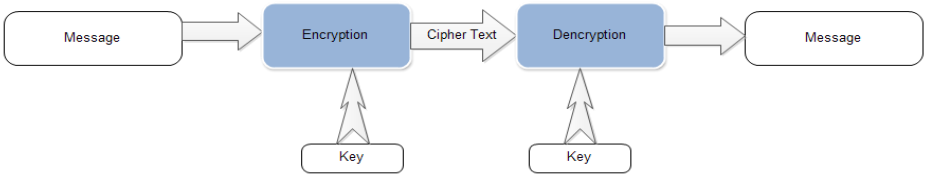

Figure 1.1: symmetric key encryption/decryption

The drawback of this system is that every time the shared key kept secure. If the attacker gets the key which is shared by the both parties he will able to access the information for every transmission between the parties. So, asymmetric cryptography will overcome this limitation of symmetric cryptography.

A) Asymmetric Cryptography

Asymmetric key cryptography is also known as public key cryptography. It uses two different keys: - one public key and the other is private key. It is computationally hard to find the private key from the public key. Anyone can encrypt a message with the public key but not decrypt it. The person who has the private key can only decrypt the message. The sender encrypt the data using the receiver's public key and the receiver decrypt the data with its own key known as private key. There are a number of Asymmetric key encryption algorithms like RSA, ECC. Following [1.2] is the figure of asymmetric encryption and decryption:-

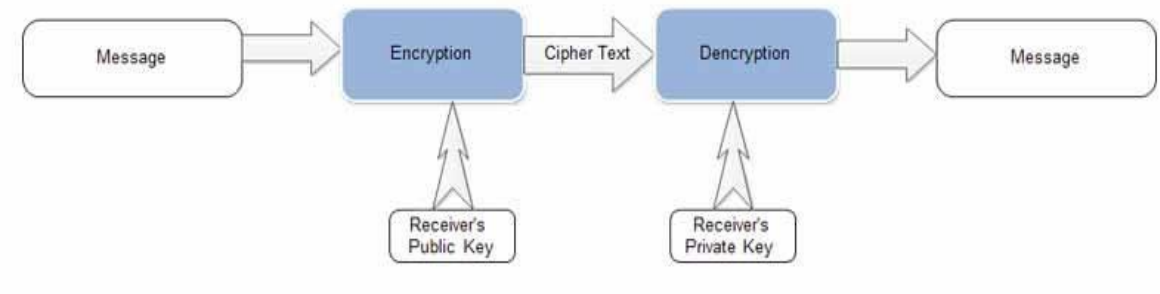

Figure 1.2: Asymmetric key encryption/decryption

This is how sender A can send a message to the receiver B using public-key cryptography:
(a) A and B both will agree on a public-key cryptosystem.
(b) B sends A his public key.
(c) A encrypts his message using B's public key and sends it to B.
(d) B decrypts A's message using his private key.

We can describe asymmetric key cryptography as below: -

AC= (K, E, D)…… (1)

Where AC (asymmetric cryptography) is a function of K, E and D.

Here K represents the key generation algorithm, which gives the keys in pair i.e. (PbK, ScK), here PbK is the public key and ScK is the secret key. E represents the encryption algorithm and D represents the decryption algorithm.

II. PROBLEM FORMULATION

The symmetric key cryptography is less secure than the asymmetric key cryptography. There different approaches related to symmetric cryptography, which include the symmetric key algorithms such as DES, AES, and Circle-Symmetric key cryptography, Geometry Based Symmetric Key Cryptography Using Ellipse, etc. After reviewing the symmetric cryptography, we focused on asymmetric cryptography.

These approaches are based on the symmetric cryptography with different mathematical shapes such as Circle, Ellipse etc, which provide the security. But these approaches are not asymmetric. As discussed earlier that asymmetric cryptography provide more security, so we focused on the asymmetric cryptography that is based on the concept of SPHERE (a mathematical shape).

III. NEW APPROACH

As we discuss that asymmetric cryptography can be done by using algorithms like: - RSA, ECC. Here we purpose a new approach named Asymmetric cryptography based on Sphere. Now the question is what is Sphere? How it can use in cryptography. Here is the solution as we will discuss the concept of sphere.

A) SPHERE: -

Football, basketball, table tennis ball are all examples of geometrical figures which we call "spheres" in three dimensional geometry. Following is the figure of Sphere: -

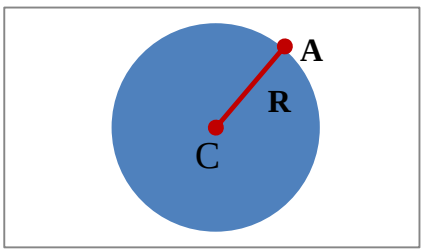

Figure 1.3: Sphere

DEFINITION OF SPHERE: - "A SPHERE IS THE LOCUS OF A POINT WHICH REMAINS AT A CONSTANT DISTANCE FROM A FIXED POINT."

The constant distance is called the radius and the fixed point the centre of the sphere. In figure [1.3] the centre of the sphere is denoted by C and the radius of sphere is denoted by R.

The equation of the sphere: - Let (x1, y1, z1) be the centre and R the radius of a given sphere. Equating the radius r to the distance of any point (x, y, z) on the sphere, we have: -

$(x - x1)^2 + (y - y1)^2 + (z - z1)^2 = (R)^2$……(2)

Choose any point randomly on the circumference of the sphere, which is the Private Key of the receiver and because the center of the sphere is always fixed so take it as a Public key of the receiver and.

To find the public key on the sphere we use the distance method stated that we can find the radius of sphere if we know the centre of sphere and one point which lie on the sphere.

Let (a, b, c) be any point on the sphere and (x1, y1, z1) be the centre so by distance method: -

$(a - x1)^2 + (b- y1)^2 + (c - z1)^2 = (r)^2$…….(3)

So we can obtain a number of points on the sphere, and select a point as a private key.

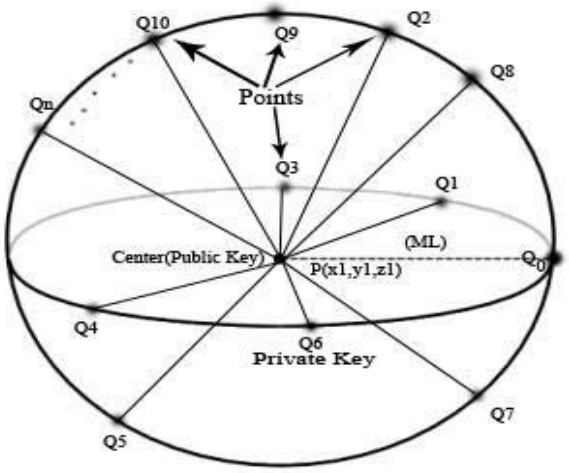

Figure 1.4: Spherical representation of new approach

In the figure 1.4 we can choose one point on the sphere as our private key, and P(x1, y1, z1) is the center which is selected as public key. ML is the message length, it should be fixed and fixed value is 64-bits. Q0, Q1, Q2, Q3, ……., Qn are the points on the sphere.

IV. NEW ASYMMETRIC KEY ALGORITHM

We used following terminology in our new approach ACBS:-

Public Key: - center of Sphere (Pbk), Private Key: - any on the Sphere (Prk), Message Length: - Radius of Sphere, Known parameter: - center of Sphere (Public Key).

Key Generation: - using Distance method of Sphere we generate the pair of Public-Private Key.

Encryption: -

Input: O, a 64- bit value.

Output: - C, a 192- bit value.

1) Let center of Sphere= Pbk (x_1, y_1, z_1).
2) Derive F from Pbk.
3) Generate an upper triangular 3X3 matrix M, with diagonal as F.
4) Calculate S= O*M (1X3 matrix).
5) Do permutations of matrix S.

Output=C.

Decryption: -

Input: -C, a 192 – bit value.

Output: - O, a 64-bit value.

1) Let a point on Sphere= Prk(a_1, b_1, c_1).
2) Derive F1 from Prk.
3) Generate an upper triangular 3X3 matrix B, with diagonal as $(F1)^3$.
4) Do permutation of C.
5) Calculate S1= C*B (1X3 matrix) .

Output= O.

V. CONCLUSION

The conclusion of the study is that from the security point of view the Asymmetric Cryptography technique is more secure than the symmetric cryptography. Because it is difficult to break the system, that uses two different keys. Elliptic

curve cryptosystem provides an efficient alternative to other cryptosystems. In most practical implementations asymmetric key cryptography is used to secure and distribute session keys. If the security of an algorithm is based on keeping the way that algorithm works a secret, it is a restricted algorithm. A large or changing group of users cannot use them, because every time a user leaves the group everyone else must switch to a different algorithm. If someone accidentally reveals the secret, everyone must change their algorithm. Even more damning, restricted algorithms allow no quality control or standardization.

Modern cryptography solves this problem with asymmetric keys, which overcome all the drawback of symmetric cryptography.

ACKNOWLEDGMENT

My warm appreciations go to my parents. I deeply thankful to **Mr. Simarjit Singh (Asst. Prof**), who helped me during my dissertation work. He helped a lot at every step like in decision making, concept development, etc. He motivated me for the development of this new approach. Finally I am thankful to my friends for their valuable support.

I am grateful to my advisor Ms. Anu Garg (Asst. Prof.), Lovely Professional University, Phagwara, Punjab for her excellent guidance, help and support. She provided me the best infrastructure. Her suggestions proved as golden way finders for me. Her guidance proved and golden milestones for me. This dissertation became possible with her supervision and constant help.

REFERENCES

[1] Mohammad jabed Morshed Chowdhury,Tapas Pal, *A New Symmetric Key Encryption Algorithm Based on 2-d Geometry*, ©2009 IEEE.

[2] Rasmi P S, Dr. Varghese Paul, *A Hybrid Crypto System based on a new Circle-Symmetric key Algorithm and RSA with CRT Asymmetric key Algorithm for E-commerce Applications*, International Conference on VLSI, Communication & Instrumentation (ICVCI) 2011 Proceedings published by International Journal of Computer Applications® (IJCA).

[3] Rui Guo, *Pairing Based Elliptic Curve Encryption Scheme with Hybrid Problems in Smart House*, 2013 Fourth International Conference on Intelligent Control and Information Processing (ICICIP) June 9 – 11, 2013, Beijing, China, ©2013 IEEE.

[4] MeltemKURT, Tank YERLiKA Y A, *A New Modified Cryptosystem Based on Menezes Vanstone Elliptic Curve Cryptography Algorithm that Uses Characters' Hexadecimal Values*, ISBN: 978-1-4673-5613-8©2013 IEEE.

[5] Khushdeep Kaur(Research scholar), Er. Seema(Assistant professor), *Hybrid Algorithm with DSA, RSA and MD5 Encryption Algorithm for wireless devices*. International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 ,Vol. 2, Issue 5, September- October 2012.

[6] Prerna Gaur1, Dr. Paramjit Singh, *Geometry Based Symmetric Key Cryptography Using Ellipse*. Volume 2, Issue 7, July 2013 ISSN 2319 – 4847, IJAIEM.

[7] Ankita Agarwal, IMSEC, Ghaziabad (India), *Secret Key Encryption Algorithm Using Genetic Algorithm*. International Journal of Advanced Research in Computer Science and Software Engineering Volume 2, Issue 4, April 2012.

