



Implementation of ACBS Crypto System in Android

¹Er Gurjinder Kaur, ²Simarjit Singh

¹Research Scholar, Department of Computer (DIPS Dhilwan) India

²Asst. Prof. Departmentt of Computer (DIPS Dhilwan) 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 centre 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. 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. 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:

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. A number of symmetric key encryption algorithms like DES, TRIPLE DES, AES, BLOWFISH have been developed to provide greater security affects

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.

B) 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.

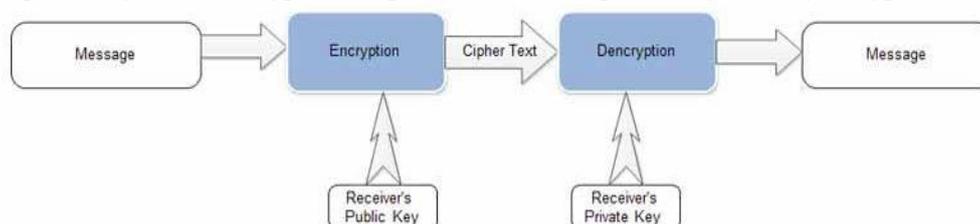


Figure 1.1: Asymmetric Key Encryption/Decryption

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.

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

The equation of the sphere: - Let (x_1, y_1, z_1) 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:

$$(x - x_1)^2 + (y - y_1)^2 + (z - z_1)^2 = (R)^2$$

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. 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 (x_1, y_1, z_1) be the centre so by distance method: -

$$(a - x_1)^2 + (b - y_1)^2 + (c - z_1)^2 = (r)^2$$

So we can obtain a number of points on the sphere, and select a point as a private key. This concept is presented in figure [1.2].

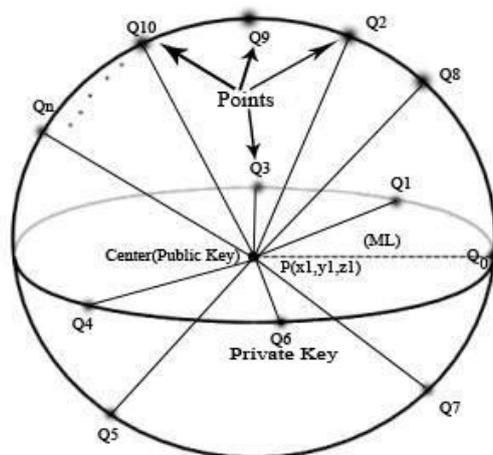


Figure 1.2: Spherical representation of new approach

We can choose one point on the sphere as our private key, and $P(x_1, y_1, z_1)$ is the center which is selected as public key. ML is the message length, it should be fixed and fixed value is 64-bits. $Q_0, Q_1, Q_2, Q_3, \dots, Q_n$ are the points on the sphere.

IV. NEW ASYMMETRIC KEY ALGORITHM

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 .

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 F_1 from Prk.
- 3) Generate an upper triangular 3X3 matrix B , with diagonal as (F_1) .
- 4) Do permutation of C .
- 5) Calculate $S_1 = C * B$ (1X3 matrix).

V. IMPLEMENTATION

We use Eclipse Tool for implementation of ACBS crypto system. We develop an Android Application.

Encryption Process:- The encryption algorithm runs as the background activity to perform the operation of encryption. When the message is entered, this application will produce the cipher text by using the encryption algorithm.

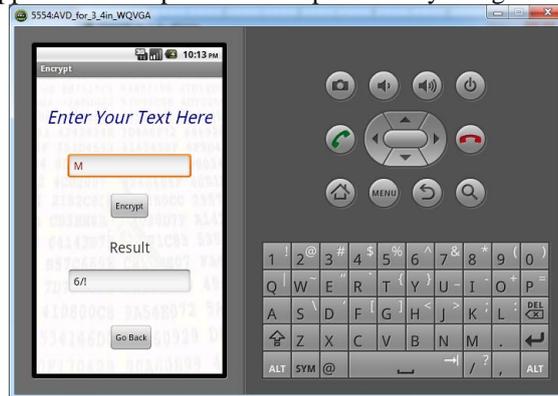


Figure 1.3: Encryption Process

Decryption Process:-

This application on the receiver side will perform the decryption process to get the original message. Figure [1.4] describes the working of decryption process.

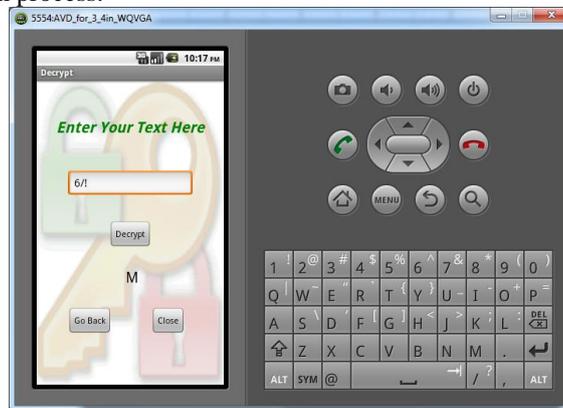


Figure 1.4: Decryption Process

VI. SECURITY ANALYSIS OF ACBS

We are using the distance method to generate the points on the sphere. From the attacker point of view by knowing the public key he cannot find the private key because he does not know the exact the value of the R which may be from the range of 64 to 2^{64} in the case when the message length is 64. If the message length is 64 bits then the numbers of generated points are 18446744073709551616. Now consider when the message length is 128 bits.

Crypt Analysis attack:- If the attacker knows the 2^8 part of the radius then there is 2^{56} is not known in the case when message length is 64 bits and 2^{120} is not known if the message length is 128 bits. In Figure 1.5 an attack is performed by using (15, 22, 81) as private key.

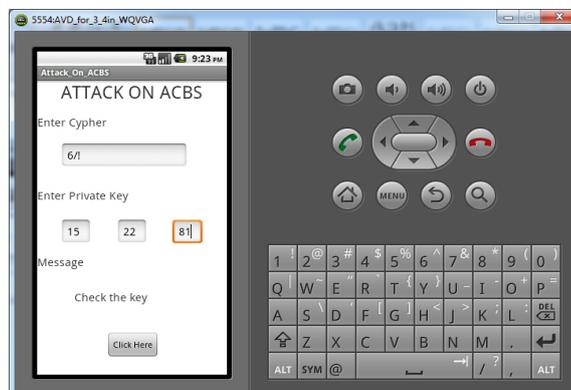


Figure 1.5: Performing Attack with Point (15, 22, 81)

Brute-Force attack:- In the case of Brute-Force attack, Average time required to search the 56 bit key for decryption is **1142 years**. According to the theory of the Brute-Force attack and Crypt Analysis ACBS Crypto System is highly secure. This is not easy for an attacker to break the security of our ACBS: Crypto System.

VII. CONCLUSION

Given new algorithm is performing very efficient in order to provide security to the information against attacks. If we measure the security then Key Generation given in this approach proven to be has a high degree of security. Hence this cryptosystem is applicable for use in various applications including Android, E-Commerce etc

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.

REFERENCES

- [1] 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.
- [2] Guido Bertoni, "ECC Hardware Coprocessors for 8-bit Systems and Power Consumption Considerations", 0-7695-2497-4/06 © 2006 IEEE.
- [3] Kamini H. Solanki, Chandni R. Patel, "New Symmetric Key Cryptographic algorithm for Enhancing Security of Data". International Journal Of Research In Computer Engineering And Electronics. VOL: 1 ISSUE :3 (DEC 2012).
- [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] Ravi Shankar Dhakar, "Modified RSA Encryption Algorithm (MREA)", DOI 10.1109/ACCT.2012.74, © 2012 IEEE.
- [6] 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.
- [7] 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", (ICVCI) 2011 Proceedings published by International Journal of Computer Applications® (IJCA).
- [8] ZHANG Yun-peng, "Asymmetric Cryptography Algorithm with Chinese Remainder Theorem", 978-1-61284-486-2/11,©2011 IEEE.
- [9] S. Maria Celestin Vigila, "Implementation of Text based Cryptosystem using Elliptic Curve Cryptography", 978-1-4244-4787-9/09 ©2009 IEEE.