UNIVERSITI PUTRA MALAYSIA

ENCRYPTING TEXT DATA USING ELLIPTIC CURVE CRYPTOGRAPHY

ABAS ABDULLAHI ALI

FSKTM 2018 31

ENCRYPTING TEXT DATA USING ELLIPTIC CURVE CRYPTOGRAPHY

By

ABAS ABDULLAHI ALI

Project Paper Submitted to the School of Graduate Studies, University Putra Malaysia, in Fulfillment of the Requirements for the Master of Information Security, in the Faculty of Computer Science and Information Technology

January 2018

COPYRIGHT

DEDICATIONS

I dedicate this work to my beloved mother, Zainab Haji Hassan Wardhere, for her lifetime support, care and love.

Abstract of the Project Paper Presented to the Senate of University Putra Malaysia in Fulfilment of the Requirement for the Master of Information Security

ENCRYPTING TEXT DATA USING ELLIPTIC CURVE CRYPTOGRAPHY

By

ABAS ABDULLAHI ALI

JANUARY 2018

Chairman: Sharifah Md. Yasin, Ph.D.

Faculty: Computer Science and Information Technology

Elliptic curve cryptography has been a hot topic since its birth in 1985. Elliptic curve cryptography has been proven to be secure and requires small key sizes in comparison to the well-known and most used cryptographic algorithms. In this study, a new approach is proposed to enhance the performance of the encryption which means eliminating classic mapping techniques. In this new procedure, the text is converted into its equivalent ASCII values which will serve as a raw data for the Elliptic curve cryptography. This technique boosts the system performance by wiping out the lookup table compared to the current mapping techniques that tend to share the lookup table between the recipient and the sender. Encrypting and decrypting any text that has an equivalent ASCII code is the core principle of this algorithm.

Abstrak Tesis Yang Dikemukakan Kepada Senat Universiti Putra Malaysia Sebagai Memenuhi Keperluan Untuk Ijazah Sarjana Keselamatan Maklumat

MENYULITKAN DATA TEKS MENGGUNAKAN KRIPTOGRAFI LENGKUNG ELIPTIK

Oleh

ABAS ABDULLAHI ALI

JANUARY 2018

Pengerusi: Sharifah Md. Yasin, PhD

Fakulti: Sains Komputer Dan Teknologi Maklumat

Kriptografi lengkung eliptik telah menjadi topik hangat sejak kelahirannya pada tahun 1985. Kriptografi lengkung eliptik telah terbukti selamat dan memerlukan saiz kunci kecil berbanding dengan algoritma kriptografi yang terkenal dan yang paling banyak digunakan. Dalam kajian ini, satu pendekatan baru telah dicadangkan untuk meningkatkan prestasi enkripsi yang bermaksud menghapuskan teknik pemetaan klasik. Dalam prosedur baru ini, teks ditukarkan ke nilai ASCII yang setara yang akan berfungsi sebagai data mentah untuk kriptografi lengkung Elliptic. Teknik ini meningkatkan prestasi sistem dengan memadam jadual carian berbanding dengan teknik pemetaan sediada yang cenderung untuk berkongsi jadual carian antara penerima dan penghantar. Menyulitkan dan menyahsulit sebarang teks yang mempunyai kod ASCII yang setara adalah prinsip teras algoritma ini.

ACKNOWLEDGMENTS

The completion of this work could not have been possible without the help of the Great Almighty, Allah Subhanahu Wa Tala, and the assistance and help of countless people. Their contributions are gratefully acknowledged and sincerely appreciated. I would like to express my deep appreciation to my mother, Zainab Haji Hassan Wardhere, and my father, Abdullahi Ali Haile, for their endless support during this work and my entire life journey. I would like to thank, Dr. Sharifah Md. Yasin for her endless support, spirit and understanding during this study. To all my siblings, friends and others who in one way or another shared their support.

This Project Paper was submitted to the Senate of University Putra Malaysia and has been accepted as Partial Fulfilment of the Requirement for the Master of Information Security.

Sharifah Md. Yasin, PhD
Senior Lecturer
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Chairman)
Date:

Hajah Zaiton Muda, M.Sc.
Senior Lecturer
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
Internal Examiner
Date:

Declaration by Graduate Student

I hereby confirm that:

- this thesis is my original work;
- quotations, illustrations and citations have been duly referenced;
- this thesis has not been submitted previously or concurrently for any other degree at any other institutions;
- intellectual property from the thesis and copyright of thesis are fully-owned by Universiti Putra Malaysia, as according to the Universiti Putra Malaysia (Research) Rules 2012;
- written permission must be obtained from supervisor and the office of Deputy Vice-Chancellor (Research and Innovation) before thesis is published (in the form of written, printed or in electronic form) including books, journals, modules, proceedings, popular writings, seminar papers, manuscripts, posters, reports, lecture notes, learning modules or any other materials as stated in the Universiti Putra Malaysia (Research) Rules 2012;
- there is no plagiarism or data falsification/fabrication in the thesis, and scholarly integrity is upheld as according to the Universiti Putra Malaysia (Graduate Studies) Rules 2003 (Revision 2012-2013) and the Universiti Putra Malaysia (Research) Rules 2012. The thesis has undergone plagiarism detection software.

Signature: ________________________ Date: ________________________

Name and Matric No.: ____

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

1.1 Cryptography

Cryptography is the art of masking data so that only the intended recipients can remove the mask and recover the actual data. That data can be a text, image, video, or a message that contains image, video, and text. The method of masking is converting the actual form of the data into a new form, that cannot be readable unless you have the key to recover the message. The two main goals of cryptography are authenticity and secrecy. Authenticity and secrecy are very distinct, the first goal, ensures that the message can only be enciphered by the holder of the key. It ensures the message is not spoofed, altered, or reproduced during the transmission. The second goal, ensures that the message can only be deciphered by the intended recipient. If the message is being captured during the transmission by unintended recipient, the eavesdropper cannot recover the message, because of the unavailability of the key. The science that deals with underlying cryptographic schemas is called cryptology. The science for cracking or breaking cryptographic methods is called cryptanalysis. Shannon (1949) has introduced practical and theoretical cryptographic security.Practical cryptographic security is that the cryptographic systems cannot broken using the available computational resources. While, Theoretical cryptographic security is that the cryptographic system is impossible to break regardless of the computational resources. The most cryptographic standards are asymmetric, symmetric, hash function and digital signature.

1.1.1 Symmetric Cryptography

Shared key or secret key are the popular names for symmetric cryptography. Since, the sender and the receiver of the message share a single secret key to encipher and decipher a message. One important aspect in symmetric cryptography is to share the secret key through save communication line. The two communicating parties should be very careful, because if the key is known by another party, i.e. attackers, they can reproduce encrypted messages and decrypt messages. This type of cryptography is liked by most since it uses less resources, and it is fast to encipher and decipher messages. The well-known algorithms that follow this standard are: Advanced Encryption Standard (AES), Data Encryption Standard(DES), Triple DES, and Blowfish. The key lengths used by symmetric cryptography vary from 56, 64, 128, 256 and 448-bit size keys. Most of these standards use 64-bit block size except for AES which uses 128-bit block size.

1.1.2 Asymmetric Cryptography

Public key cryptography is the interchangeable name for Asymmetric cryptography. Before sending a message, each of the two parties, the sender and the receiver, create public and private key. The sender shares his/her public key with the receiver to decrypt the message received. The sender uses the private key to encrypt the message. In this technique, no one can use the public key for encryption and decryption of the same message and vice versa. Many people like this kind of encryption as it provides more privacy, because your messages can only be read by people who has your public key.

This kind of standard is implemented by many algorithms such as Elliptic Curve Cryptography (ECC), Rivest, Shamir and Adelman (RSA), and Diffie-Hellman.

1.1.3 Hash Function

The hash function is a one-way encryption, the hash function is a well-defined procedure or mathematical formula that represents a small size of bits which is generated from a large sized file, the result of this function can be called hash code or hashes. The generating of hash code is faster than other methods which make it more desired for authentication and integrity. Cryptographic hash functions are much used for digital signature and cheap constructions are highly desirable. The use of cryptographic hash functions for message authentication has become a standard approach in many applications, particularly internet security protocols. The authentication and the integrity considered as main issues in information security, the hash code can be attached to the original file then at any time the users are able to check the authentication and integrity after sending the secure data by applying the hash function to the message again and compare the result to the sender hash code, if its similar that is mean the message came from the original sender without altering because if there is any changed has been made to the data will changed the hash code at the receiver side.

1.1.4 Digital signature

Digital signature is used to ensure the authenticity of a message, key, and any kind of data. Outside of our technology world, digital signature can be a signature of a person, a stamp of an organization. Practically, digital signature can be created by encrypting a message with your private key and sending it to another party, which will use your public key to verify whether the message came from you or not. In another way, it can be used by Universiti Putra Malaysia(UPM), by encrypting a message with their private key and save it in the student certificate, the ministry of high education will use the public key of UPM to check if the certificate is produced by UPM or not.

1.2 Elliptic Curve Cryptography(ECC)

Elliptic curve cryptography is commonly used to authenticate public-key protocols most especially when trying to implement digital signature and key-agreement. In 1985, Neal Koblitz and Victor Miller freely developed Elliptic curve cryptography, which is public key cryptography8. The use of elliptic curve cryptography has greater benefits because it can be understood easily; it also offers small key size and proficient implementations which are similar to security level used in other schemes such as RSA. Moreover, ECC has been a late research region in the field of cryptography. It gives more elevated amount of security with lesser key size contrasted with other cryptographic methods9. As of late, ECC has pulled in the consideration of developers and analysts because of its vigorous scientific structure and most astounding security contrasted with other existing calculations like RSA. Elliptic curve cryptography offers break even with security for little piece estimate than RSA where bigger key size is required, which diminishes the preparing multifaceted nature[10].

1.2.1 ECC scheme

The conception of data security prompts to the development of Cryptography. As it were, Cryptography is the exploration of keeping data secure. Cryptography is the mechanism of changing a plain message to make it secure and resistant from attackers. In 1985, Neal Koblitz and Victor Miller freely developed Elliptic curve cryptography, which is based on public key cryptography. Typically, prime field elliptic curve cryptography relies on the elliptic curve equation, which is known as Weierstrass equation:

$$y^2 = x^3 + ax + b \tag{1.1}$$

where a and b are the constant with

$$4a^3 + 27b^2 \neq 0 \tag{1.2}$$

Coordinate points of elliptic curve make it viable to do cryptographic operation over finite field. Mathematically, elliptic curve point equations are: point doubling, point addition, point multiplication, and point at inverse. In this scheme, we will focus on point multiplication of ECC. ECC is a public key cryptography, which require a public key and a private key. Consider that Aziah and Abu Bakar are contacting each other. They found a base point which is G and a common elliptic curve equation. Consider Aziah has a private key nA and Abu Bakar has also a private key which is nB. Aziahs public key will be: Pa = nAG.

while Abu Bakars public key will be Pb = nBG. If Aziah want to send a message Pm to Abu Bakar, Aziah uses Abu Bakars public key to encrypt the message. The cipher text is going to look like Pc = {kG, Pm + kPb}. where "k" is an arbitrary whole number. The arbitrary "k" ensures that notwithstanding for a same message the figure content produced is diverse every time. This gives trouble for somebody who is illicitly attempting to decode the message. Abu Bakar decrypts the message by subtracting the facilitate of "kG" increased by nB from 'Pm + kPb'. Here duplicated does not mean straightforward multiplication that we do in algebra, rather it is different expansion of focuses utilizing the point expansion technique expressed above in point multiplication. As the multiplier nB is the mystery key of Abu Bakar, no one but Abu Bakar can decipher the message sent by Aziah.

1.3 Research Problem

It is well-known that classic ECC mapping techniques of the characters to affine points is costly because they require the two communicating parties which are sender and recipient to share a lookout table[5]. According to [2], it may require a set of predefined constants to be known by all the devices taking part in the communication. In which, if it is compromised will give the attacker to manipulate the entire secure communication line to his/her interest. it is easy to decipher using letter frequency attack, because the simple mappings preserve letter frequencies of the plaintext message[4]. Some researchers use a technique of mapping the message to some distinct point on the elliptic curve by modifying the message using a mapping algorithm[6]. The mapping table can be known by capturing the packets of the encrypted message.

1.4 Research Objective

Our aim is to use a deterministic approach that guarantees the security of the message by implementing a prime ECC algorithm. It can be used to encipher and decipher any type of message with defined ASCII values. Omitting the costly operation of mapping and the need to share the common lookup table between the two parties in the communication. It will provide faster computational time using smaller key size due to the significantly small parameters in ECC. Moreover, this method will guarantee the confidentiality of the message. All these characteristics will ensure that our scheme is immune to attacks. Unlike the previous techniques of ECC, in this research the combination of plaintext will utilize the comparison of ASCII codes. The input of the ECC is the result of the pairing. This algorithm enhances the efficiency, since it doesnt require a table of mappings to be shared by encipher and decipher and it has the ability to encipher any text but it should have an ASCII code[5].

1.5 Research Scope

In this project, text data will be encrypted and decrypted using Elliptic curve cryptography. Text data is selected for this research because of its importance for communication and its wilder usage in our day to day routine. Moreover, Python programming language is used for the implementation of the algorithm. Python is very powerful, easy, and secure programming language. In addition, it uses less computing resources which is very important for our project.

1.6 Research Motivation

ECC is an excellent choice for low complexity devices and networks that require public key cryptosystem[12]. ECC is well-suited for applications that need long-term security requirements. ECC has smaller key size which yield to faster computation[9]. ECC has a benefit over systems based on the multiplicative group of a finite field is the absence of a sub exponential-time algorithm[6]. ECC is suitable for large size data as they have designed to encrypt in terms of blocks consisting of multiple characters[5]. ECCs arithmetic is computationally less complex than other cryptographic algorithms[3].

BIBLIOGRAPHY

King, B. (2009). Mapping an Arbritrary Message to an Elliptic Curve When Defined over GF (2^ n). IJ Network Security, 8(2), 169-176.

Bh, P., Chandravathi, D., & Roja, P. P. (2010). Encoding and decoding of a message in the implementation of Elliptic Curve cryptography using Koblitz's method. International Journal on Computer Science and Engineering, 2(05), 1904-1907.

Kolhekar, M., & Jadhav, A. (2011). Implementation of elliptic curve cryptography on text and image. International Journal of Enterprise Computing and Business Systems, 1(2).

Amounas, F., & El Kinani, E. H. (2012). Fast mapping method based on matrix approach for elliptic curve cryptography. International Journal of Information & Network Security (IJINS), 1(2), 54-59.

Singh, L. D., & Singh, K. M. (2015). Implementation of Text Encryption using Elliptic Curve Cryptography. Procedia Computer Science, 54, 73-82.

Sengupta, A., & Ray, U. K. (2016). Message mapping and reverse mapping in elliptic curve cryptosystem. Security and Communication Networks, 9(18), 5363-5375.

Koblitz, N. (1994). A course in number theory and cryptography (Vol. 114). Springer Science & Business Media.

Benssalah, M., Djeddou, M., & Drouiche, K. (2012). RFID authentication protocols based on ECC encryption schemes. In RFID-Technologies and

Applications (RFID-TA), 2012 IEEE International Conference on (pp. 97-100). IEEE.

Amounas, F. (2013). Secure encryption scheme of amazigh alphabet based ECC using finite state machine. In Security Days (JNS3), 2013 National (pp. 1-4). IEEE.

shi Chen, W., & Liu, C. (2011). The Applied Research of ECC Encryption Algorithm in VPN Technology. In Internet Technology and Applications (iTAP), 2011 International Conference on (pp. 1-4). IEEE.

Xu, D., & Chen, W. (2010). 3G communication encryption algorithm based on ECC-ElGamal. In Signal Processing Systems (ICSPS), 2010 2nd International Conference on (Vol. 3, pp. V3-291). IEEE.

Habib, M., Mehmood, T., Ullah, F., & Ibrahim, M. (2009). Performance of wimax security algorithm (the comparative study of rsa encryption algorithm with ecc encryption algorithm). In Computer Technology and Development, 2009. ICCTD'09. International Conference on (Vol. 2, pp. 108-112). IEEE.

Gupta, K., Silakari, S., Gupta, R., & Khan, S. A. (2009). An ethical way of image encryption using ECC. In Computational Intelligence, Communication Systems and Networks, 2009. CICSYN'09. First International Conference on (pp. 342-345). IEEE.

Gupta, K., & Silakari, S. (2010). Performance analysis for image encryption using ECC. In Computational Intelligence and Communication Networks (CICN), 2010 International Conference on (pp. 79-82). IEEE.

Soram, R. (2009). Mobile sms banking security using elliptic curve cryptosystem. International Journal of Computer Science and Network Security, 9(6), 30-38.

Jagdale, B. N., Bedi, R. K., & Desai, S. (2010). Securing MMS with high performance elliptic curve cryptography. International Journal of Computer Applications, 7, 17-20.

Liu, S., King, B., & Wang, W. (2007). Hardware organization to achieve high-speed elliptic curve cryptography for mobile devices. Mobile Networks and Applications, 12(4), 271-279.

Edoh, K. D. (2004). Elliptic curve cryptography: Java implementation. In Proceedings of the 1st Annual Conference on Information Security curriculum development (pp. 88-93). ACM.

Cilardo, A., Coppolino, L., Mazzocca, N., & Romano, L. (2006). Elliptic curve cryptography engineering. Proceedings of the IEEE, 94(2), 395-406.