IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 20, Issue 6, Ver. I (Nov - Dec 2018), PP 09-11
www.iosrjournals.org

A Study On Diffie Hellman Algorithm And Elliptic Curve Cryptography

[1.]S.Uma Mageshwari, [2.]Dr. R.Santhi
[1]*Research Scholar, R& D Centre, Bharathiar University , Coimbatore.*
[2]*Research Supervisor, Bharathiar University, Coimbatore.*
Corresponding Author: S.Uma Mageshwari

Abstract: *Cryptography is the vast discipline to provide security at a greater level for our information. The Diffie Hellman (DH)Algorithm and Elliptic Currve Cryptography(ECC) are two different approaches to provide unique key. Using keys, data can be encryted(plaintext to ciphertext) and decrypted(ciphertext to original text).While transmitting data in a network, it should be safeguard from third party. The unique identification of key helps us to transmit data in a secured manner as well as an intruder not able to identify the key.The keys shows an important role in keeping the information confidential. This paper highlights the significance of keys , Diffie – Hellman algorithm with sample output and basics of Elliptic Curve Cryptography.*
Keywords: *Diffie Hellman, ECC, Key.*

Date of Submission: 22-10-2018 Date of acceptance: 05-11-2018

I. Literature Review

[8] **T.Subashri, Arjun.A, and Ashok.S:**This manuscript describes Voice Over Internet protocol for sending secured voice data over the networks. The Diffie Hellman and Elliptic curve algorithm terminology has been specified obviously. The AGI (Asterisk Gateway Interface) server has been used for implementation of ECC.
[9] **Bidyut Jyoti Saha, Kunal Kumar Kabi, Arun:** This article designates DES (Data Encryption Standard) and Henon map. By using Henon Map, a key is created .Using DES, the image can be encrypted with the produced key. This image can be used to correlate with the points over the elliptic curve.
[10] **Dariush Abbasinezhad- Mood, Morteza Nikooghadam:**This paper works on key distribution for Smart Grid using ECC. The best part of this paper is about the security and privacy for the communicating devices and the privacy solutions has been discussed obviously.

II. Introduction

[1] In 2002, Diffie and Hellman(DH) defines the first public key algorithm .Using this algorithm a secured key is recognized and it is swapped with two partiesand it can be used for encrypting succeeding messages. This key exchange procedure is used commercially.Elliptic Curve Cryptography(ECC) is a public key cryptography and which is conveyed by Victor Miller and Neal koblitz in the year 1985. ECC is the fastest key generationwhich accomplishes the computations on Elliptic Curve. Elliptic Curve Cryptography provides a stronger security than the other cryptographic alogorithms.[3]The correlation between DH and ECC is that DH practices modular arithmetic to compute the secret key whereas ECC practices algebraic curve to generate key.DH works on multiplicative set of integers whereas ECC works on muliplicative set of points on the curve.

III. Classification Of Keys

[2] The Cryptographic keys can be classified such as:

- ***Data Encryption Key :*** It is generated by using AES(Advanced Encrytion Standard), RSA(Rivest Shamir Adleman).
- ***Authentication Key:*** This is created by HMAC(Hash Message Authentication Code).
- ***Digital Signature Key:*** This is achieved by DSA(Digital Signature Algorithm).
- ***Key Encryption Key:*** The key must be wrapped with another key to achieve authentication and integrity.
- ***Master Key:*** This master key encrypts several subordinate keys.
- ***Root Key:*** It is the highest key which is used to authenticate and for signing Digital Certificates.

IV. Diffie Hellman Algorithm

[1]Diffie – Hellman algorithm is a mechanism of exchanging keys between two persons in a secured manner. If two persons namely P and Q wants to do secured data transmission, then a key need to be identified using the following steps:

1. Identify any two prime numbers 'm'and 'n'
2. Let P and Q shares secret number is identified as 'a' and 'b'
3. Calculate P=n*mod a ^{m}
4. Calculate Q=n*mod b ^{m}
5. Key1=Q*mod a ^{m}
6. Key2=P*mod b ^{m}
7. Key1=Key2(a unique key is generated)

This generated key has been used for encryption and decryption process.

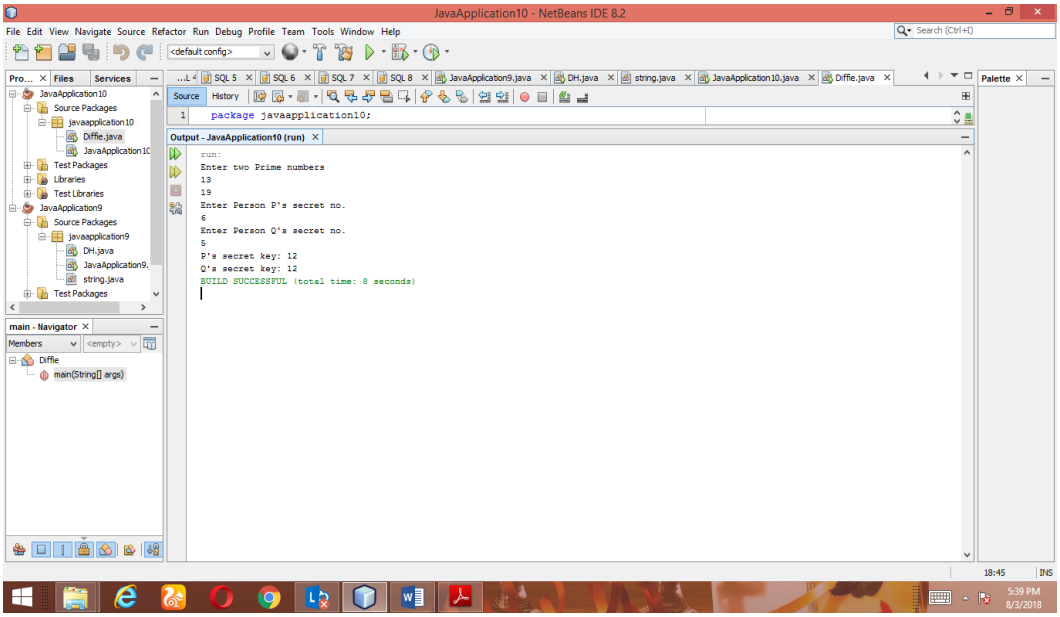

Figure 2: Output : Unique shared key

V. Elliptic Curve Cryptography

An Elliptic Curve equation is represented as: $p^2=q^3+cq+d$ where p,q,c,d are known as real numbers. The set of points (p,q) on an Elliptic Curve should satisfy an elliptic curve equation.

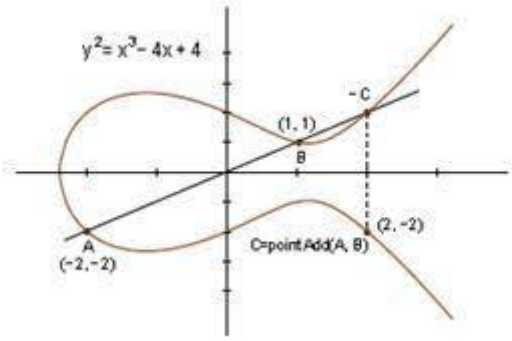

Figure 3: Sample Elliptic Curve

The ECC should satisfy the following properties:

- ***Closure :*** For all m,n in P the result of the operation m.n must be in P.
- ***Associativity:*** For all m,n and o in P, the equation (m.n).o=m.(n.o) .
- ***Identity element:*** There exists an elemnt r in A, such that for all elements m in P, the equation r.m=m.r= m.
- ***Inverse element:*** For each m in P, there exists an element n in P such that m.n=n.m=r where r is the identity element.
- ***Commutativity:*** For all m,n in P, m.n=n.m.

Different values for a and b yields a different elliptic equation. If there is no repeated roots in cubic polynomial q^3+cq+d, then the curve is called Non- singular Elliptic Curve.Otherwise, it is known as Singular Elliptic Curve.

Security Aspect

Since the elliptic curve is used for secure transmission of informaion,the key cannot be guessed. The various attacks like Cryptanalysis and Man-in –the -middle appears to be infeasible to detect the messages.ECC uses very less memory space, so it is fit for safeguarding mobile devices.

VI. Conclusion

Secrecy is accomplished for the information by implementing any Cryptographic algorithms. This paper enlightens about producing a key using Diffie- Hellman algorithm and Elliptic Curve Crptography.The implementation of Diffie Hellman algorithm is carried out which generates the unique key on both sides. The key from the Diffie Hellman can be used to map up with the points on the Elliptic curve to make available for enhanced security.

References

[1]. Cryptography and Network Security – William Stallings, Fourth Edition, PHI,2006.
[2]. https://www.cryptomathic.com/news-events/blog/classification-of-cryptographic-keys-functions-and-properties.
[3]. https://security.stackexchange.com/questions/46802/what-is-the-difference-between-dhe-and-ecdh
[4]. Certicom,https://www.certicom.com/ecc
[5]. Elliptic Curve Cryptography: a gentle introduction, http://andrea.corbellini.name/2015/05/17/elliptic-curve-cryptography-a-gentle-introduction/
[6]. HimjaAgrawal, Prof.P.R.Badadpure,'A Survey Paper on Elliptic Curve Cryptography', International Research Journal of Engineering and Technology(IRJET),Vol.3, Issue No.4,April 2016. e-ISSN: 2395- 0056.
[7]. D.Lohit Kumar,Dr.A.R.Reddy, Dr.S.A.K.Jilani,'Implementation of 128 – bit AES algorithm in MATLAB', International Journal of Engineering Trends and Technology(IJETT), Vol.33, Issue No.3,March 2016,ISSN: 2331-5381.
[8]. T.Subashri, Arjun.A, and Ashok.S, ' Real Time Implementation of Elliptic Curve Cryptography Over a Open Source VOIP server', IEEE, 5th ICCCNT-2014, July 11-13,2014,Hefei, China.
[9]. Bidyut Jyoti Saha, Kunal Kumar Kabi, Arun, 'Digital Image Encryption using ECC and DES with Chaotic Key Generator', International Journal of Engineering Research & Technology(IJERT), ISSN: 2278-0181, Vol.2, Issue 11, November-2013.
[10]. Dariush Abbasinezhad- Mood, Morteza Nikooghadam, 'Anonymous ECC – Based Self – Certified Key Distribution Scheme for Smart Grid', IEEE Transactions on Industrial Electronics, DOI: 10.1109/TIE.2018.2807383, IEEE,2018.

S.Uma Mageshwari. " A Study On Diffie Hellman Algorithm And Elliptic Curve Cryptography" IOSR Journal of Computer Engineering (IOSR-JCE) 20.6 (2018): 09-11.