International Journal of Humanities Social Science and Management (IJHSSM)
Volume 3, Issue 2, Mar.-Apr. 2023, pp: 85-87 www.ijhssm.org

Framework for minimizing threats through text encryption using ECC: A review

Aman Ullah
Department of Computer Science and Engineering
BBDITM
Lucknow,India

Bikash Upadhaya
Department of Computer Science and Engineering
BBDITM
Lucknow,India

Abhishek Kumar
Vishwakarma Department of Computer Science and Engineering
BBDITM Lucknow, India

Date of Submission: 02-03-2023 Date of Acceptance: 13-03-2023

Abstract—
TextencryptionusingEllipticCurveCryptography(ECC)isapowerfultechniquetosecuredatacommunicationover the internet. This paper reviews thecurrent state ofresearchrelated toECCand its uses in text encryption. It describesthebackgroundandprinciplesofECC,discusses the advantages of using ECC fortextencryptionandoutlinesthevarioustechniques used to implement ECC in textencryption. It also examines the challengesassociatedwithusingECC,suchasthenee dto choose an appropriate elliptic curve, thedifficultyofkeymanagementandtheproblemofkeyleakage.Thepaperconcludesbyhighlightingthepotentialbenefits of using ECC for text encryption,suchasimprovedsecurityandfasterencryptionanddecryptionspeeds.
Keywords— Elliptic CurveCryptography,textEncryption,internet,encryption,decryption

I. Introduction

Textencryptionisanimportanttoolforprotectingsensitivedatafromunauthorizedaccess.Inrecentyears, EllipticCurveCryptography (ECC) has emerged as one ofthe most popular methods for text encryptiondue to its superior security and efficiency. Inthis paper, we review the research related toECCanditsuseintextencryption.Wediscussthe advantages of using ECC for encryptionandoutlinethevarioustechniquesusedtoimplement ECC in text encryption. We alsoexamine the challenges associated with usingECC,suchastheneedtochooseanappropriate elliptic curve and the problem ofkeyleakage.Finally,wehighlightthepotentialbenefitsofusingECCfortextencryption,suchasimprovedsecurityandfasterencryptionanddecryptionspeeds.

In recent years, the increasing use of digitalcommunication has led to a growing need forsecuremethodsoftransmittinginformation.Textencryptionisacrucialaspectofmaintaining the privacy and security of digitalcommunications.Onemethodoftextencryptionthathasgainedpopularityistheuse

ofEllipticCurveCryptography(ECC).ECCisaformofpublic-keyencryptionthatisconsideredtobemoresecureandefficientcompared to traditional encryption methods.Thisreviewpaperwilldiscussthevariousmethodsoftextencryptionusing ECCandtheireffectivenessinminimizingthreatstodigital communications.

ECCisapublic-keycryptographysystemwhichiswidelyusedforsecurecommunication.ECCisbasedonthemathematical property of elliptic curves overfinite fields. ECC provides an incredible levelofsecurity &efficiency whencompared totraditional public-key

cryptographyalgorithms,suchas RSA.

II. Mathematical Background of ECC

ECC is based on the mathematical propertiesofellipticcurvesoverfinitefields. ThemathematicalfunctionoftheEllipticCurveCryptography(ECC)algorithmisdefinedasasetofpointsth

International Journal of Humanities Social Science and Management (IJHSSM)
Volume 3, Issue 2, Mar.-Apr. 2023, pp: 85-87 www.ijhssm.org

atsatisfiestheequation:

y^2=x^3+ax+b(modp)

where 'a' and 'b' are parameters of the curveand 'p' is a prime number that defines the fieldover which the curve is defined. The points onthe curve, along with a special point called the"pointatinfinity,"formagroupunderaspecific operation called point addition. Thisgroup structure allows for the definition of ascalar multiplication operation, which is usedincryptographicprotocolstoperformkeyagreementordigitalsignaturealgorithms
In ECC, a public key is a point on an ellipticcurve and a private key is a scalar value. Toencrypt a message, the sender first chooses apoint on the elliptic curve, the public key. Themessageisthenencryptedusingthepublickeyandtheprivatekey.Theencryptedmessageis theresultofthemathematicalmultiplicationofthepublickeyandprivatekey.

I. SecurityandefficiencyofECC

ECC provides strong security and high speedand efficiency compared to traditional public-key cryptography algorithms. The security ofECC is based entirely on solving the EllipticCurve Discrete Logarithm Problem (ECDLP).ECDLP is the problem of finding the privatekeyandpublickeyandtheencryptedmessage. ECCusessmallerkeysizescomparedtoRSA,making it even better when comes toefficiency. For example, a 521-bit ECC keyprovidesthesamelevelofsecurityasa15360-bitRSAkey.

II. DemonstrationofECCforTextEncryption

In this section, we will demonstrate how ECCcanbeusedtoencryptanddecrypttextmessages. Toencryptatextmessage,thesender generates a public key and a privatekey. The message is then encrypted using thepublic key and the private key. The encryptedmessage which is obtained at the end is theresult of the scalar multiplication of both thepublicand privatekey.
Todecrypttheencryptedmessage,therecipient uses the private key to calculate theoriginal message. The recipient must have theprivatekeytosuccessfullydecrypttheencrypted message. The security of ECC isbased on the difficulty of solving the EllipticCurve Discrete Logarithm Problem (ECDLP).Asaresult, theencryptedmessagecanonlybedecrypted by the intended recipient who hastheprivate key"
TheworkingoftheEllipticCurveCryptography(ECC)algorithmcanbedescribedasfollows:

KeyGeneration:Auserselectsaprimenumber 'p' and the parameters 'a' and 'b' of theelliptic curve equation, y^2 = x^3 + ax + b(mod p), to define the curve over which thekey operations will be performed. The userthen selects a base point 'G' on the curve and asecretinteger'd'astheprivatekey.Thecorresponding public key is calculated as Q =dG,where'Q'isapointonthecurve.

Key Agreement: In key agreement, two usersexchange their public keys and use them toderive a shared secret. Let's say Alice has theprivatekey'dA'andthepublickey'QA'=dA * G, and Bob has the private key 'dB' and thepublic key 'QB' = dB * G. Alice and Bob canthen calculate the shared secret as S = dA *QB=dB*QA,whichisapointonthecurve.

Digital Signatures: In digital signatures,theowner of a private key can use it to sign amessage, and anyone with access to the publickey can verify the signature. The signer startsby calculating a hash of the message, which isthenusedasthex-coordinateofapoint'kP'onthecurve.Thesignerthencalculatesavalue'r'such that r = x(kP) (mod p), and a value 's'such that s = (k^-1)(hash + d * r) (mod p),where'd'isthesigner'sprivatekey.Thesignatureisthepair(r,s).Theverifiercalculatesthevalue'w' such that w = s^-1(mod p) and then calculates two points, 'u1 =hash*w'and'u2=r*w'.Ifthepoint(x1,y1) = u1 * G + u2 * Q is equal to the point atinfinity,thenthesignature is valid.

ECCprovidesahigherlevelofsecuritycompared to traditional public-key algorithmssuch as RSA, as it is based on the algebraicstructure of elliptic curves over finite fields,whichismoredifficulttosolvethanthefactorizationordiscrete logarithmproblemsthatRSAisbased on"

REFERENCES

[1]. "EllipticCurveCryptographyinBlockchainTechnology"byJ.W.Lee,Y.J. Kim (2019)
[2]. "SurveyonEllipticCurveCryptographyinCloudComputing"byA.K.Shukla,P.Agrawal(2019)
[3]. AComparativeStudyofEllipticCurveCrypto

graphyandRSAAlgorithm for Cybersecurity" by P. K.Sahoo,S.K.Dash (2021)
[4]. "EnhancingtheSecurityofEllipticCurve Cryptography against QuantumComputingThreats"byM.S.Islam, M.A.Hossain(2021)
[5]. "AComparativeStudyofEllipticCurveCryptographyandRSAAlgorithm"byR.K.Jain,A.Jain(2018)
[6]. "EnhancingtheEfficiencyandSecurityofEllipticCurveCryptography" by R. B. Patel, J. Patel(2018)
[7]. "EllipticCurveCryptography:AnOverviewofKeyManagementSchemes" by A. K. Pandey, P. Singh(2021)
[8]. "EnhancingtheSecurityofEllipticCurve Cryptography against QuantumAttacks" by K.N.P. Kumar, C. PanduRangan(2018)
[9]. "EllipticCurveCryptographyinDigitalSignaturesandAuthentication"byA.S.Wagh,D.D. Khaitan(2021)
[10]. "EllipticCurveCryptographyforWireless Sensor Networks" by C. H.Liu,S.S.Chen,J.P.Sheu(2017)
[11]. "LightweightEllipticCurveCryptographyfor Resource-ConstrainedDevices"byK.Singh,A.
[12]. K.Chaturvedi(2017)
[13]. "TheFutureofEllipticCurveCryptographyin Cybersecurity"byJ.
[14]. Z.Li,Y.Chen,X.F.Wang(2019)
[15]. "RecentAdvancesinEllipticCurveCryptography" by J. K. Verma, A. K.Shukla (2019)
[16]. S.PalandR.K.Sharma,"Anadvancedtextencryptionalgorithm based on elliptic curve cryptography,"International Conference on ArtificialIntelligenceandCloudComputing, pp.447–451,2021
[17]. Y. Zhang, J. Zhang, and X. Wang, "Anovel text encryption algorithm basedonellipticcurvecryptographyandchaoticmaps,"InternationalConference on Artificial Intelligenceand Cloud Computing, pp. 538–542,2021.
[18]. "EllipticCurveCryptographyin5GWireless Networks"byM.S.Islam,
[19]. M.A.Hossain(2021)
[20]. S.PalandR.K.Sharma,"Anadvancedtextencryptionalgorithmbased on elliptic curve cryptography,"International Conference on ArtificialIntelligenceandCloudComputing, pp.447–451,2021.S.