Advances and Applications in Mathematical Sciences
Volume 20, Issue 11, September 2021, Pages 2645-2652

CRYPTOGRAPHIC ALGORITHMS ON LOW POWER DEVICES USED IN SMART CITY: ISSUES AND ENHANCEMENTS

MUNEER AHMAD DAR[1], SYED NISAR BUKHARI[2] and MUJTABA SHAFI[3]

[1]National Institute of Electronics
and Information Technology, Srinagar
Jammu and Kashmir, India
E-mail: muneer@nielit.gov.in
nisar@nielit.gov.in

[3]University of Kashmir
Hazratbal, Srinagar, J&K
E-mail: mujtabashafi@gmail.com

Abstract

The secret data stored in a device having restricted potential to carry out the established cryptographic algorithms like RSA, ECC, DES and AES, is a massive test for the researchers. These devices like the smartphone and many other hand held gadgets are enormously used in smart city where millions of such devices are used to exchange a very critical data collected by these devices. The data over collection and the exchange of data among the communicating devices are some of the challenges that need to be addressed. These devices have a limited capability in terms of processor speed and are not as good as a desktop PC to execute the well known cryptographic algorithms. This paper evaluates the implementation of traditional cryptographic algorithms on these hand held devices with the intension to compare them and find out the issues in implementing such algorithms on these devices. The Android Studio is used to present the proof of concept evaluation of these algorithms. This paper also presents an enhanced Elliptic Curve Cryptographic key exchange solution as an alternative to the traditional cryptographic algorithms.

I. Introduction

World is moving towards urbanization with over 50% of the population

2010 Mathematics Subject Classification: 94A60.
Keywords: Cryptography, RSA, ECC, DES, AES, Smartphone, Android Studio.
Received October 13, 2020; Accepted November 6, 2020

living in cities. To comply with the main objective of smart city that is to cater everything smartly, be it education, public service, logistics, transport and many other facilities that the administration is trying to incorporate smartly to its citizens, the role of smart hand held device is very critical as almost everyone is carrying a smartphone these days. The smartphone has a capability to remain always connected and continuously sends the data to the other communicating devices.

With this hand held device used extensively in today's world particularly in smart city, the concerns pertaining to safeguarding the data and privacy of a common citizen is at risk as these devices have a limited capability to store the huge data collected over the network and are not computationally good enough to execute the cryptographic algorithms. Be it doing the transactions or getting socially connected with the friends and family, the smart phone sends and receives very confidential information and it must be encrypted so that the intruders are not able to gather the information for any adversity. The cryptographic algorithms which are broadly categorized into symmetric and asymmetric algorithms are well enough to encrypt the data but the only issue is with their computational power. This paper addresses the issues pertaining to the implementation of such algorithms on Android based smart phones and proposes an enhanced algorithm which is computationally feasible for such devices.

This paper is ordered as the section II provides the review of existing work/research done by the researchers. Section III presents the comparative evaluation of the existing cryptographic algorithms. Section IV highlights the issues of executing these algorithms on devices which are limited in their resources. Within this section we present an enhanced elliptic curve cryptographic solution for such devices and to end with we illustrate our conclusion related to our research in section V.

II. Existing Research

In this section, we focus on the existing research done by the researchers to find out how we can secure a common user in a smart city. Researchers focused on different ways both active and passive to deal with their security. The most of the research is done by the passive way [5]. The researchers

focused on the distributed means to protect the solitude and safety of users one of the method is the smart grid technique [6]. The research done in [6] [7] to secure the users in a smart city is not well suited for the resource constrained devices. The data over collection by these devices in a smart city is discussed in [2]. This research mainly focused on putting the data in a cloud and performing the main computational techniques in cloud. Similar research is done in [1] wherein security architecture is proposed to secure the users in a smart city. The proposed architecture makes use of the cloud. A much better methodology is implemented in [6-16] wherein specialized servers are deployed to enforce the security in these devices.

III. Comparative Evaluation

In this section, the various symmetric and asymmetric algorithms are discussed and their comparative evaluation based on flexibility, modifications and the recognized attacks which the intruders can use to compromise the security and privacy of smartphone users. In symmetric algorithms, the data is encrypted by the secret key and the cipher text is converted into the original text by making use of the same key. The well known algorithms which come under this category are Data Encryption Standard (DES), 3-DES, CAST-128 bit, BLOWFISH, IDEA, Advanced Encryption Standard (AES) and RC4. Many attacks like brute force attack, dictionary attacks are able to break the algorithm.

Table 1. Comparison of Cryptographic Algorithms.

Algorithm	**Type and Structure**	**Suppleness and Adjustment**	**Vulnerable to Attacks**
Data Encryption Standard	Symmetric & Multiple rounds Structure	Not Applicable	Yes
3 Data Encryption Standard	Symmetric & Multiple rounds Structure	Extendable	Yes
Carlisle Adams and Stafford(CAST-128)	Symmetric & Multiple rounds Structure	Extendable	Yes
BLOWFISH	Symmetric & Multiple rounds Structure	Extendable	Yes
Information Data Encryption Algorithm	Symmetric & Substitution and Permutation	Not Applicable	Yes

	structure		
Advanced Encryption Standard	Symmetric & Substitution and Permutation structure	Extendable	Yes
RC6	Symmetric & Multiple rounds Structure	Extendable	Yes
Rivest-Shamir-Adleman (RSA)	Asymmetric & Prime number Factorization	Extendable	Yes

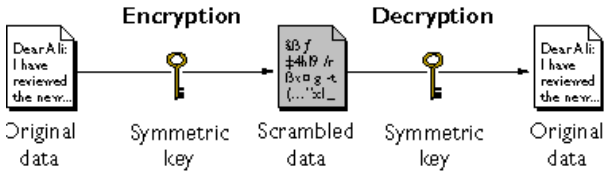

Figure 1. Symmetric Key Cryptography.

In case of Asymmetric Key Cryptography two different key called as public and private keys are used for the encryption and decryption of the data. The well known algorithm under this category is RSA

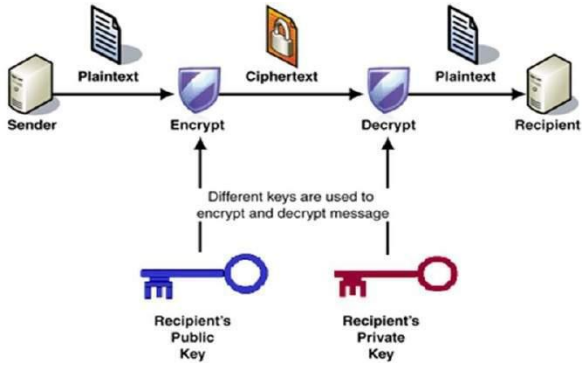

Figure 2. Asymmetric Key Cryptography.

III. Issues and Enhancements

The symmetric key algorithms are faster in computing the cipher text and decrypt but the issue with these types of algorithms is that if someone gets access to the key with which the sender has encrypted, the whole data will be compromised. As the sender has to send the key to the receiver, the

key may get compromised and the security of data is of high risk.

The well known RSA algorithm which is widely used is computationally very expensive and is not suitable for low resource devices. The key length of 512 is required in RSA as compared to ECC which requires only 106 bits. The performance comparison of RSA and ECC is given in the table below.

Table 2. Performance comparison of RSA and ECC.

RSA with key length in bits	ECC with key length in bits	Proportion of RSA/ECC
512	106	5:1
768	132	6:1
1024	160	7:1
2048	210	10:1

The ECC is an Asymmetric, public key cryptographic technique in which the communicating devices are generating two key named as public and a private key. The public key is distributed to all the devices while as the private key is hidden and kept secret by the client encrypting or decrypting the message [3]. The domain parameters of the elliptic curve are a sextuple:

$$T = (P, a, b, G, n, h).$$

An ECC (Elliptic curve) is presented by the equation

$$y^2 = x^3 + ax + b$$

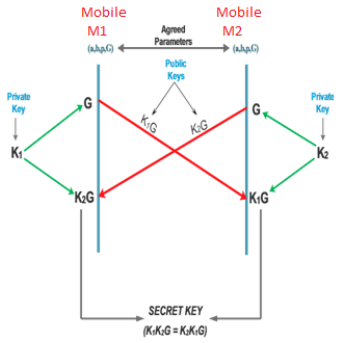

Figure 3. Diffie-Hellman Elliptic Curve Based Key Exchange.

Discrete Logarithm Problem. The toughness of breaking the ECC key depends on the logarithmic problem say if we are given two point X and Y on the curve with $K\,X = Y$. It takes exponential time to find out the value of K if X and Y is known to us. So it makes it a discrete logarithmic problem and we would not be able to find out the value of K as it is infeasible.

ECC Public Key Cryptosystem. In the public key elliptic curve cryptosystems, presume that entity A wishes to push a message 'm' to individual B securely. Arrangement of a points on the arc can be evaluated as N so as to, $NPo = Po + Po + . + Po, \ldots, N\ time = o(\infty)$.

Public/Private Key Generation Using ECC. Both the sender and the receiver of the message use the same parameters on the ECC. The parameters include the G which is the generator point on the ECC arc. If the communication is in between Mr X and Mr Y, Mr X generates a random number Na which has be less the N (one of the area parameters). This Na is a private key of Mr X and he/she generates the public key as $Pa = G^{*}.Nb$ (Generator point multiplied with random number Na) Similarly, Mr Y generates a random number Nb which has to be less than N and sets it as his private key and determines his public key as $Pa = G^{*}.Nb$ (Generator point multiplied with random number Nb).

Generation of common shared key. After a trade of the public key between the two gatherings, Mr X figures his Normal Key by Processing Key $(A) = Na * .Pub\ (B)$ Mr Y records his Regular Key by Registering Key $(B) = Na * .Pub\ (A)$ Both Mr X and Mr Y have a common key as under: $Na * .Pub\ (B) = Na * (Nb * G) = Nb * (Na * G) = Nb * Pub\ (A)$.

Encryption. Now Mr X wants to encrypt a message Msg and sends it to Mr Y. Mr X randomly picks a number N and a private key Pri_A. The public key is generated by calculating $\text{Pub}\ (A) = \text{Pri\_A}\ {}^{*}G$ and generates a text called as cipher text.

Decryption. Now the reverse process is used by Mr Y to decrypt the cipher text.

IV. Conclusion

The use of smart hand held devices used in the communication of users in a smart city with huge and confidential data can lead to various challenges. The usage of the traditional algorithms is not feasible as it may delay the execution of various smart activities in a smart city. The symmetric algorithms are fast as compared to Asymmetric algorithms as the identical key is employed by the sender as well as by the receiver for the encryption and decryption. We found that the transmission of key exchange in Asymmetric algorithms is of utmost importance. The Elliptic Curve Cryptographic key exchange is considered as a better algorithm than any of the other algorithms like RSA, DES and others. The only issue with the ECC is the Man in the middle vulnerability which may lead to a massive attack. In this research we modified the Elliptic Curve Cryptography so that it is not vulnerable to such attacks.

Furthermore, it is concluded that the over collection of data in a smart city leads to many challenges and it is proposed that the services of cloud may be utilized and as such the security and privacy of citizens is safeguarded.

References

[1] Muneer Ahmad Dar, Security Architecture for Low Resource Devices in Smart City using Cloud International Journal of Informatics Visualization DOI http://dx.doi.org/10.30630/joiv.4.3.407 4, (3) 2020.

[2] Y. Li, W. Dai, Z. Ming and M. Qiu, Privacy Protection for Preventing Data Over-Collection in Smart City, in IEEE Transactions on Computers, doi: 10.1109/TC.2015.2470247. 65 (5) (2016), 1339-1350

[3] Dar, Muneer Ahmad, Khan, Ummer and Bukhari, Syed. Lightweight Session Key Establishment for Android Platform Using ECC. 10.1007/978-981-13-3122-0_33. (2019).

[4] A. Muneer, Dar and J. Parvez, Security Enhancement in Android using Ellipic Curve Cryptography, Int. J. Secur. its Appl., 11 (6) (2017), 27-34.

[5] H. Zhu, R. Lu, C. Huang, L. Chen and H. Li, An Efficient Privacy-Preserving Location-Based Services Query Scheme in Outsourced Cloud, in IEEE Transactions on Vehicular Technology, doi: 10.1109/TVT.2015.2499791. 65 (9) (2016), 7729-7739.

[6] M. Qiu, W. Gao, M. Chen, J.-W. Niu, and L. Zhang, Energy efficient security algorithm for power grid wide area monitoring system, IEEE Trans. Smart Grid 2(4) (2011), 715-723.

[7] J. Blom, D. Viswanathan, M. Spasojevic, J. Go, K. Acharya and R. Ahonius, Fear and the

city: Role of mobile services in harnessing safety and security in urban use contexts," in Proc. SIGCHI Conf. Human Factors Comput. Syst. (2010), 1841-1850.

[8] A. Paverd, A. Martin, and I. Brown, Security and privacy in smart grid demand response systems, in Proc. 2nd Int. Workshop Smart Grid Security (2014), 1-15.

[9] D. Damopoulos, G. Kambourakis, M. Anagnostopoulos, S. Gritzalis, and J. Park, "User privacy and modern mobile services: Are they on the same path?" Personal Ubiquitous Comput. 17 (7) (2013), 1437-1448.

[10] Muneer. A. Dar, S. Nisar Bukhari and U. I. Khan, Evaluation of Security and Privacy of Smartphone Users, 2018 Fourth International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB), Chennai, doi: 10.1109/AEEICB.2018.8480914. (2018), 1-4.

[11] Muneer A. Dar and J. Parvez, Smartphone operating systems: Evaluation & enhancements, International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT), Kanyakumari, doi: 10.1109/ICCICCT.2014.6993056. (2014), 734-738.

[12] Muneer A. Dar and J. Parvez, Enhancing security of Android and IOS by implementing need-based security (NBS), 2014 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT), Kanyakumari, doi: 10.1109/ICCICCT.2014.6993055. (2014), 728-733.

[13] U. Iqbal, M. A. Dar and S. Nisar Bukhari, Intelligent Hospitals based on IOT, 2018 Fourth International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB), Chennai, doi: 10.1109/AEEICB.2018.8480947. (2018), 1-3.

[14] M. A. Dar, A novel approach to restrict the access of malicious applications in android, 2017 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), Coimbatore, doi: 10.1109/ICIIECS.2017.8275927. (2017), 1-4.

[15] V. Dattana, K. Gupta and A. Kush, A Probability based Model for Big Data Security in Smart City, 2019 4th MEC International Conference on Big Data and Smart City (ICBDSC), Muscat, Oman, doi: 10.1109/ICBDSC.2019.8645607. (2019), 1-6.

[16] R. Srinivasan, A. Mohan and P. Srinivasan, Privacy conscious architecture for improving emergency response in smart cities, 2016 Smart City Security and Privacy Workshop (SCSP-W), Vienna, doi: 10.1109/SCSPW.2016.7509559. (2016), 1-5.