International Journal on Emerging Technologies **12**(1): 07-12(2021)

ISSN No. (Print): 0975-8364
ISSN No. (Online): 2249-3255

Evaluation of Cryptographic Algorithms on Low Power Devices used in Smart City

Muneer Ahmad Dar
Scientist-C, National Institute of Electronics and Information Technology (NIELIT) Srinagar, (J&K), India.

(Corresponding author: Muneer Ahmad Dar)
(Received 29 September 2020, Revised 13 November 2020, Accepted 03 December 2020)
(Published by Research Trend, Website: www.researchtrend.net)

ABSTRACT: The large volume of critical data exchanged through open networks in a smart city is vulnerable and the privacy of users is at risk. The cryptographic algorithms are applied to such data and the data is exchanged through the networks in encrypted form. The various devices are used in a smart city to exchange such critical information. One of the important devices in such communication is the Smartphone, capable of doing everything that can be done with a traditional computer. As the resource of such hand held devices is limited in terms of storage and processing capabilities, the cryptographic algorithms like RSA, ECC, DES, AES which are very complex and well suited for high speed computers are not feasible for such low power devices. This paper evaluates the time complexity of various cryptographic algorithms on smart phones with limited configuration. The objective of this investigation is to find out how much time these traditional algorithms are taking on low runtime memory and low processor device. The Android virtual device (AVD) is created that abstracts for these low end devices. These algorithms are executed and are compared to find out how they can run without much delay to a common user in a smart city. The comparative analysis of RSA, ECC, DES and AES is performed and the proof of the evaluation is done on Android platform by making use of the Android Studio. The real challenge of this study is the actual implementation in a real smart city environment where millions of users are getting connected and sharing the resources, other important aspect is the data over collection in a smart city with data coming from everywhere. This paper addresses these issues with real time implementation.

Keywords: Smart City, Cryptography, Smartphone, AVD, RSA, ECC, DES, AES, Android.

I. INTRODUCTION

The smart devices are extensively used in smart city to perform various activities like smart public service, smart buildings, smart education, smart banking and many more. The main limitation of these devices is the lack of computational capabilities to execute the traditional algorithms like RSA, DES and AES. As the users are making use of these devices to do everything smartly, the tremendous amount of data is collected by these devices and this over collected data includes the confidential data which is shared among the IOT devices and the servers. The high end desktops are able to execute the cryptographic algorithms, but it is the low end device, a Smartphone which has a limitation in terms of memory and the computational capabilities to execute these algorithms. A Smartphone and IOT devices are always connected with the internet in a smart city and are prone to the cyber attacks [1-3].

This paper is divided into five sections. In section II, the cryptographic algorithms are revised so that a proper understanding can be developed to compare these algorithms in subsequent sections. In section III, the review of existing research done by researchers in this direction is elaborated. In section IV, the comparative analysis of these cryptographic algorithms is done on Android platform with the android virtual device. The results of this comparative evaluation is presented in this section In section V, the conclusion of our research is drawn.

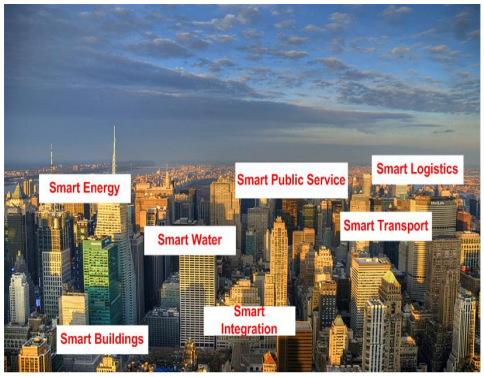

Fig. 1. Smart City.

II. REVIEW OF CRYPTOGRAPHY

The cryptography can be broadly categorized into Symmetric and Asymmetric Cryptography. In Symmetric encryption a secret-key is used for both encryption of the plain text and decryption of the cipher text as shown in Fig. 2.

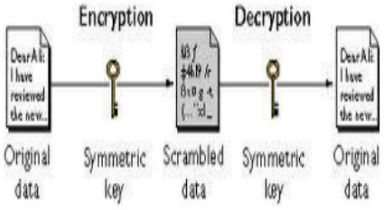

Fig. 2. Symmetric Key Cryptography

The secret key that is used for both encryption and decryption must be confidential within the open network. This sharing of the secret key is a challenge in smart city where the intruders are always trying to launch the cyber attacks. The various algorithms which fall under this category are DES, AES, 3DES, BLOWFISH etc. These algorithms are comparatively faster than the Asymmetric Algorithms [2].

The other way of using encryption is the public key cryptography called as Asymmetric Encryption. It makes use of two keys- one is public and another is private. The private keys are not disclosed in any means in the network and are kept confidential with the sender and the receiver. As such the sharing of confidential keys is eliminated in public key cryptography. The RSA and ECC are the well known algorithms which come under this category [2].

The public key cryptography has a reasonable level of security when it comes to using the traditional algorithms on the high end computers. But at the same time these algorithms are not truly explored on the devices which are low in memory and computational capabilities. In this section, we will try to understand some of the well known cryptographic algorithms.

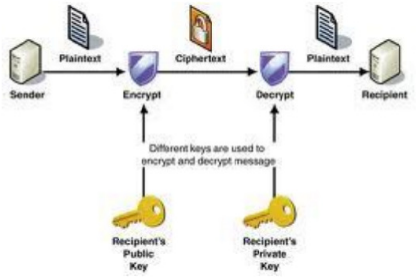

Fig. 3. Asymmetric Key Cryptography.

RSA. The top recognized Asymetric key cryptography was developed by Rivest, Shamir & Adleman (RSA) of MIT in 1977. This public-key cryptography scheme based on exponentiation in a finite (Galois) field over integers modulo a prime exponentiation takes $O((\log n)^3)$ operations (easy). Uses large integers (eg. 1024 bits) security due to cost of factoring large numbers factorization takes $O(e^{\log n \log \log n})$ operations (hard). The following table illustrates the RSA algorithm along with an example.

Table 1: RSA Algorithm with Example.

RSA Algorithm	RSA Example
1. Select two large primes at random - p, q 2. Compute their system modulus N=p.q note ø(N)=(p-1)(q-1) 3. Selecting at random the encryption key e where 1<e<ø(N), gcd(e,ø(N))=1 . Solve following equation to find decryption key d e.d=1 mod ø(N) and 0≤d≤N 5. Publish their public encryption key: KU={e,N} *6.* Keep secret private decryption key: KR={d,p,q}	1. Select primes: p=17 & q=11 2. Compute $n = pq$ =17×11=187 3. Compute ø(n)=(p–1)(q-1)=16×10=160 4. Select e *:* gcd(e,160)=1; choose e=7 5. Determine d*:* de=1 mod 160 and d < 160 Value is d=23 since 23×7=161= 10×160+1 6. Publish public key KU={7,187} 7. Keep secret private key KR={23,17,11}

To encrypt a message M the sender obtains public key of recipient KU={e,N} and then computes: $C=M^e \bmod N$, where 0≤M<N and to decrypt the cipher text C the owner uses their private key KR={d,p,q} computes: $M=C^d \bmod N$ note that the message M must be smaller than the modulus N (block if needed)

Elliptic Curve Cryptography One of the leading public key cryptography which is considered as a good alternative for low power devices is the Elliptic Curve Cryptography (ECC). The equation used in ECC is $y^2 = x^3 + ax + b$

Where a, b Є K and $4a^3 + 27b^2 \neq 0$.

Elliptic curve makes use of six parameters T = (P, a, b, G, n, h)

The Elliptic Curve Cryptography is secure and its security depends on the intricacy of Elliptic Curve Discrete Logarithm Problem. The two points P and Q on an elliptic curve are such that kP = Q, where k is a scalar. Given P and Q, it is computationally infeasible (hard) to acquire k, if k is effectively large. k is the discrete logarithm of Q to the base P.

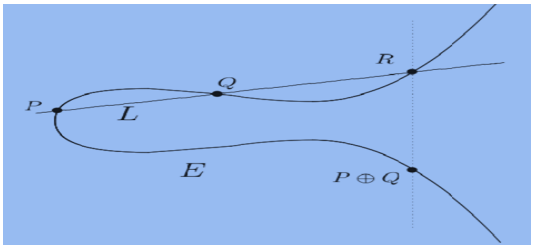

Fig. 4. Point Addition in Elliptic Curve.

AES The symmetric cryptographic technique developed by Rijmen-Daemen in Belgium. Its key size varies with 128/192/256 bits and has 128 bit data . Unlike DES which has a Feistel structure, AES is a iterative and processes blocks of 4 columns of 4 bytes. AES operates on entire data in each round and is very resistant against well known attacks with a simple design. The detailed working of AES is in the Fig. 5.

Table 2: ECC Key Exchange.

ECC Key Exchange Algorithm

Algorithm 2: Secure_Key_Exchange (Pub_a, Pub_b)
{
DEVICE_1 chooses a random number Na such that Na < N where N is a prime field. This is Na's Private Key
DEVICE_1 calculates the public key as Pub_a = Na * G [G is the generator point]
DEVICE_1 generates the secret key as S_Key = Na * Pub_b [Pub_b is public key of DEVICE_2]
The secret key shared is
S_Key = Na * Pub_b = Na * (Nb * G) as Pub_b = Nb * G as generated by DEVICE_2
Return S_Key [Na *Pub_b = Nb * Pub_a]
}

DES This is the most widely used block cipher and was adopted in 1977 by National Bureau of Standards (NBS) now known as National Institute of Standards and Technology (NIST). It encrypts 64-bit data using 56-bit key.

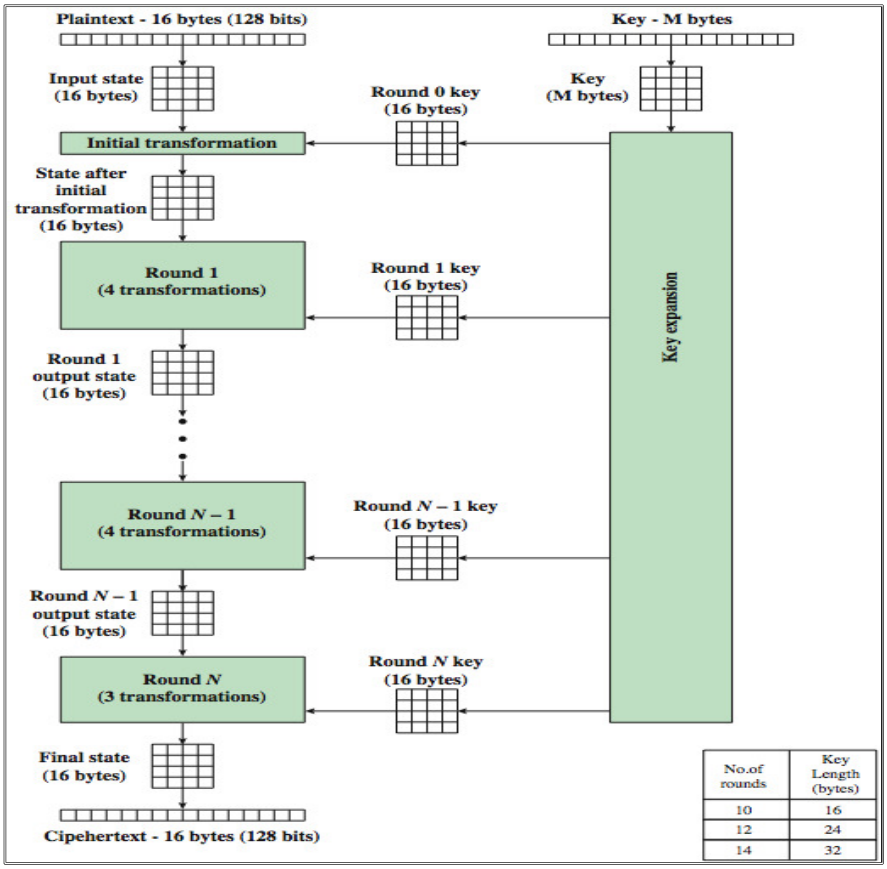

Fig. 5. AES Working.

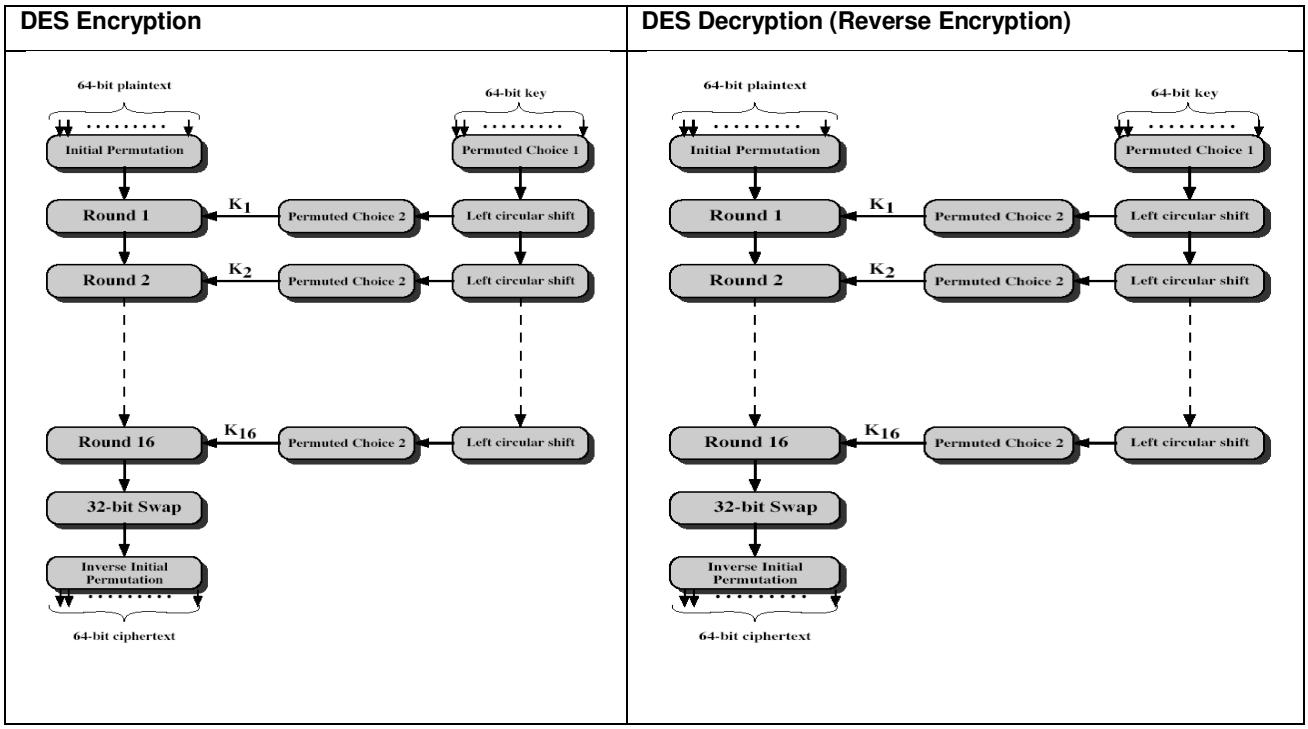

Fig 6. DES Encryption/Decryption.

The summary of these algorithms is in the table below

Table 3: Quantitative Comparison of Cryptographic Algorithms.

Algorithm	Type & Structure	Flexibility and Modification	Recognized Attacks
RSA	Asymmetric & Prime Factorization	YES, With Multi Prime RSA and Multi power RSA	Factoring the Public Key
ECC	Asymmetric & Elliptic Curve	YES	Man In the Middle Attack
DES	Symmetric & Feistel Structure	Not Applicable	Brute Force Attack
3DES	Symmetric & Feistel Structure	YES, can be extended from 56 to 168 bits	Brute Force Attack, Chosen Plaintext, Known Plaintext
CAST-128	Symmetric & Feistel Structure	YES, with 128 and 256 bits	Chosen Plaintext Attack
BLOWFISH	Symmetric &Feistel Structure	YES, 64-448 key length in multiplies of 32	Dictionary Attack
IDEA	Symmetric & Substitution-Permutation	Not Applicable	Differential Timing Attack, Key-Schedule Attack
AES	Symmetric & Substitution-Permutation	YES, 256 key length in multiples of 64	Side Channel Attack
RC6	Symmetric & Feistel Structure	YES, 128-2048 key length in multiples of 32	Brute Force Attack, Analytical Attack

III. RELATED WORK

In this section, we discuss the related research done in the area of resource constrained devices used in a smart city. There are active and passive ways of dealing with the defenses against the various threats and attacks by the intruders, Researchers mainly focused on the passive ways of security [8]. In a classical smart city, the issues related to defenses against the malicious applications have various characteristics, including security service, how data is organized, authorization and management of keys. The various solutions proposed for the security of users in a smart city are mainly of distributed in nature and are obtained from the distributed systems [9]. One of such techniques is a smart grid technique [9]. The methods defined in [9, 10] are not enough for securing the users in a smart city particularly for the use of low resource device like a Smartphone. The main reason for the scarcity of the security protocols is the lack of resources of a smart device used in a smart city [10]. The protection of users from over collection of data within a smart [1]. Their [1] research mainly focused on putting the users data on the cloud and did not came up with a solution to ease the pressure from these low power devices to execute an algorithm that is feasible for them. The lightweight session key establishment for android platform using ECC was elaborated [2] and a more robust and computationally feasible approach was implemented.
The Security and protection based on cloud in smart cities [14]. Different partners are distinguished and a system for start to finish security/protection highlights for trustable information obtaining, scattering and administration arrangement is created. A different approach is introduced in [15] where the appearance of secure equipment in individual IT gadgets propels provisioning of information security at the edges of the web by means of individual information servers running on advanced mobile phones set-top boxes, secure compact tokens and so forth. A five dimensional model of residents' security in smart urban areas [16]. These are: character protection, query security, identity security and area security, impression protection and proprietor protection. The researchers in this paper show how existing security improving innovations can be utilized to save residents' protection.

IV. COMPARATIVE ANALYSIS AND RESULTS

To setup the experiment to compare different algorithms on a smartphone with low computational capabilities and to find out the results, we will use the Android Virtual Devices (AVD) that portrays a smartphone, a smart watch or an android TV. The AVD manager is used from within the Android Studio that helps us to manage and create the virtual devices.

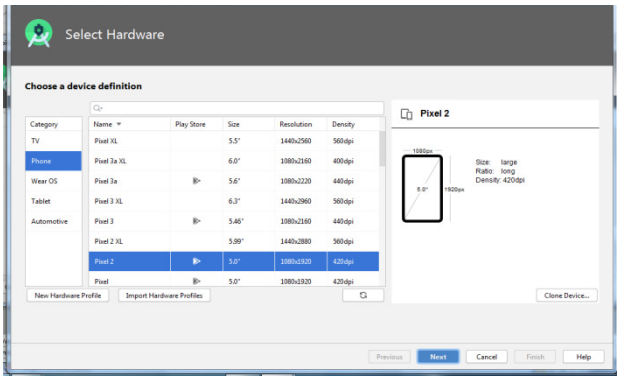

Fig. 7. Creating the Android Virtual Device.

Using the AVD manager in Android Studio, the following virtual device with different hardware configuration is created. The experiment is conducted on this device so that a comparative evaluation is done and the results can be evaluated.

Table 4: AVD with the configuration.

Device Name	Target Platform	Configuration	Memory and Storage
Google Nexus One	API Level 25 (Nougat)	System Image X86	2048 MB

After execution of these algorithms in the Android Studio, the time complexity is calculated. The repeated results are calculated and the results are shown in figures below.

Fig. 8. RSA Execution on Android.

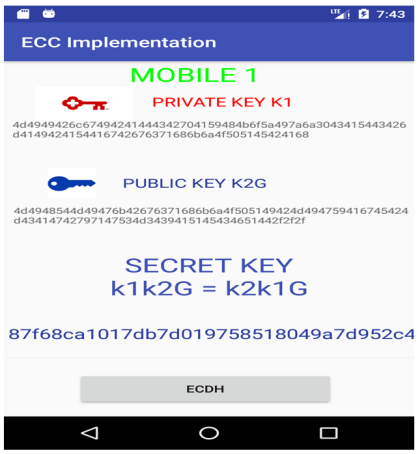

Fig. 9. ECC Implementation on Android.

After execution of these algorithms, the following results are obtained. It can be established that the Elliptic Curve cryptography is well suited for these low end devices. This paper implemented these algorithms on Android Virtual Devices (AVD) that portrays a smartphone and a real device with the capability to execute the ECC algorithms in a smart city. The data over collection is also addressed by making use of the cloud.

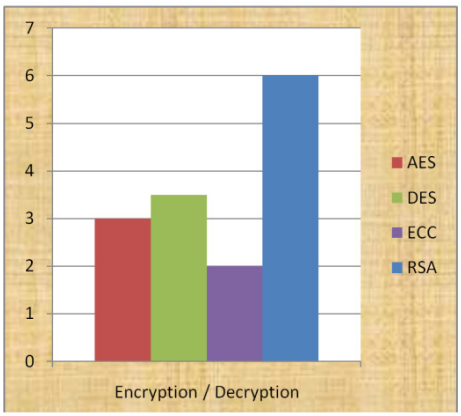

Fig. 10. Time Comparison of Cryptographic Algorithms on Smartphone.

V. CONCLUSION

In this research, the various algorithms are compared on the low end smartphone which are extensively used in a smart city. These algorithms are explained and there working is understood so that a detailed comparison can be drawn with the objective to find out which algorithm has an edge on any other algorithm [1-2]. The experiment is conducted on the Android Virtual Device which has a limited resource and represents a smartphone in a smart city. The results clearly indicate that the Elliptic Curve Cryptography is well suited for these low end devices. The traditional Cryptographic algorithms are computationally very expensive when implemented on the low power devices. If we use a key length of 1024 in RSA, same security can be provided by the ECC with a key length of 160. This research can further be extended to compare these algorithms on different devices with different configurations.

VI. FUTURE SCOPE

This research is very useful for the implementation of Smart City projects where millions of hand held devices are used for the collection of data. This research can be further enhanced to incorporate the use of cloud so that the data over collection by these devices can be taken care of.

Conflict of Interest. No.

REFERENCES

[1]. Li, Y., Dai, W., Ming, Z., & Qiu, M. (2015). Privacy protection for preventing data over-collection in smart city. *IEEE Transactions on Computers*, *65*(5), 1339-1350.

[2]. Dar, M. A., Khan, U. I., & Bukhari, S. N. (2019). Lightweight Session Key Establishment for Android Platform Using ECC. In *Advances in Computer, Communication and Control* (pp. 347-359). Springer, Singapore.

[3]. Dar, M. A., & Parvez, J. (2016). Novel Techniques to Enhance the Security of Smartphone Applications. *International Journal of Interactive Mobile Technologies, 10*(4), 32-36.

[4]. Khatoun, R., & Zeadally, S. (2017). Cybersecurity and privacy solutions in smart cities. *IEEE Communications Magazine*, *55*(3), 51-59.

[5]. *Symantec Internet Security Threat Report*, Symantec, Mountain View, CA, USA, 2018. Accessed: Jun. 2018. [Online]. Available: https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-2018-en.pdf

[6]. Hossain, M., Noor, S., & Hasan, R. (2017). HSC-IoT: A hardware and software co-verification based authentication scheme for Internet of Things. In *2017 5th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud)* (pp. 109-116). IEEE.

[7]. Zoran Hercigonja, (2016). Comparative Analysis of Cryptographic Algorithms. *International Journal of Digital Technology and Economy, Algebra University College*, *1*(2), 127-134.

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

[9]. Blom, J., Viswanathan, D., Spasojevic, M., Go, J., Acharya, K., & Ahonius, R. (2010). Fear and the city: role of mobile services in harnessing safety and security in urban use contexts. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 1841-1850).
[10]. Paverd, A., Martin, A., & Brown, I. (2014). Security and privacy in smart grid demand response systems. In *International Workshop on Smart Grid Security* (pp. 1-15). Springer, Cham.
[11]. Dar, M. A., Bukhari, S. N., & Khan, U. I. (2018). Evaluation of Security and Privacy of Smartphone Users. In *2018 Fourth International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB)* (pp. 1-4). IEEE.
[12]. Dar, M. A. & Parvez, J. (2014). Smartphone operating systems: Evaluation & enhancements. The *2014 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT),* Kanyakumari, 734-738, doi: 10.1109/ICCICCT.2014.6993056.
[13]. Dar, M. A., & Parvez, J. (2014). Enhancing security of Android & IOS by implementing need-based security (NBS). In *2014 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT)* (pp. 728-733). IEEE.
[14]. Khan, Z., Pervez, Z., & Ghafoor, A. (2014). Towards cloud based smart cities data security and privacy management. In *2014 IEEE/ACM 7th International Conference on Utility and Cloud Computing* (pp. 806-811). IEEE.
[15]. Anciaux, N., Nguyen, B., Bonnet, P., Popa, I. S., Bouganim, L., & Pucheral, P. (2013). Trusted Cells: A Sea Change for Personal Data Services.
[16]. Martínez-Ballesté, A., Pérez-Martínez, P. A., & Solanas, A. (2013). The pursuit of citizens' privacy: a privacy-aware smart city is possible. *IEEE Communications Magazine*, *51*(6), 136-141.
[17]. Dar, M. A., & Parvez, J. (2017). Security enhancement in Android using ellipic curve cryptography. *International Journal of Security and Its Applications*, *11*(6), 27-34.
[18]. Ahmad, D. M., & Javed, P. (2016). Security comparison of android and ios and implementationof user approved security (uas) for android. *Indian Journal of Science and Technology*, *9*(14), 1-7.
[19]. Dar, M. A., & Parvez, J. (2016). Smartphone Malware Threat, an Experimental Evaluation of Smartphone Security. *International Journal of Computer Science and Information Security*, *14*(8), 109-113.
[20]. Dar, M. A., & Parvez, J. (2013). Evaluating Smartphone Application Security: A Case Study on Android. *Global Journal of Computer Science and Technology Network, Web & Security*, *13*(12), 9-15.
[21]. Dar, M. A., & Parvez, J. (2014). A novel strategy to enhance the android security framework. *International Journal of Computer Applications*, *91*(8), 37-41.

How to cite this article: Dar M. A. (2021). Evaluation of Cryptographic Algorithms on Low Power Devices used in Smart City. *International Journal on Emerging Technologies, 12*(1): 07–12.