2019 6th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/ 2019 5th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom)

A Survey on Cryptography: comparative study between RSA vs ECC Algorithms, and RSA vs El-Gamal Algorithms

1st Fatma Mallouli
Deanship of Preparatory Year and Supporting Studies
Imam Abdulrahman Bin Faisal University
Dammam, Saudi Arabia
amhellal@iau.edu.sa

2nd Aya Hellal
Deanship of Preparatory Year and Supporting Studies
Imam Abdulrahman Bin Faisal University
Dammam, Saudi Arabia
fmmallouli@iau.edu.sa

3th Nahla Sharief Saeed
Community college
Imam Abdulrahman Bin Faisal University
Dammam, Saudi Arabia
nssalih@iau.edu.sa

4rd Fatimah Abdulraheem Alzahrani
Deanship of Preparatory Year and Supporting Studies
Imam Abdulrahman Bin Faisal University
Dammam, Saudi Arabia
falzahrani@iau.edu.sa

***Abstract*—Internet security and data protection should be guaranteed for all users. Therefore, security is a major concern when exposing information to networks. In todays world, the information is never enough protected the way it should be. Cryptography is one of the most effective and efficient components of network security. Cryptography is a technique to apply ensure the secure and reliable transaction between the sender and the receiver when transferring unintelligible information. Moreover, only the authorized receiver can have the right to decrypt the information that was sent and encrypted by the sender. The cryptography plays an essential role in order to provide security to these networks. In this paper, we observe encryption as well as decryption time of different algorithms with the random size of data packets. Firstly, this work introduces the fundamental concepts of Cryptography: encryption and decryption operations. Secondly, compares between the most popular algorithms RSA , El-Gamal and Elliptic Curve (ECC). Our comparison is based on key size length that affects the running time. Finally, we conclude our survey by focusing on the different outcomes between the RSA and Elliptic curve algorithms.**

***Index Terms*—Encryption, decryption, asymmetric key, symmetric key, cryptography, RSA, Elliptic Curve.**

I. Introduction

Cryptography [1] [2], is a technique to store and transmit data in a particular format in a way only intended users can read and process. The encryption of the data prevents attackers from reading private messages. Electronic security was becoming more and more essential as the Internet, and other media devices become more pervasive. Cryptography is a security tool utilized to secure email messages, Credit Card data [3], corporate information, and any relevant data transmitted through all types of media and the various fields like wired networks and wireless networks. The cryptography is classified into two major categories: Symmetric Key Systems and Asymmetric Key Systems, but it can be classified regarding other attributes. The main objectives of cryptography are confidentiality, authentication, integrity, Non repudiation, access control, and availability. RSA and ECC , El-Gamal are of the most famous techniques used to perform encryption and decryption. These techniques have different key sizes, and eventually different execution time. In the present paper we propose to present three majors algorithms used for cryptography. Note that, we introduce the main concepts used in cryptography, the remainder of this paper is organized as follows: in the second section, we introduce and compare between El-gamal algorithm and RSA. In the third section, we introduce elliptic curve algorithm and we compare it with RSA. Finally, we discuss results and we conclude.

A. Cryptography

Cryptography is simply hiding information in a systematic manner such that only authorized parties to have access to the right information. Doing so can be considered as an art, but it is a science. Cryptosystem broadly classified into two major categories, first is symmetric (Figure 1) and other is asymmetric (Figure 2) based on the concepts of the key.

B. Concepts Used in Cryptography

The following paragraph is a description of some of the concepts used in cryptography [5].
Encryption: The process of encoding plain text messages into ciphertext messages is called encryption.
Decryption: The reverse process of transforming ciphertext messages back to plain text is called decryption.
Plain Text: The raw communication written or said in any human language. It takes the form of plain text. It is read and understood or heard and understood by the sender, the recipient, or by any other third party that can access that

978-1-7281-1661-7/19/$31.00 ©2019 IEEE
DOI 10.1109/CSCloud/EdgeCom.2019.00022

IEEE computer society

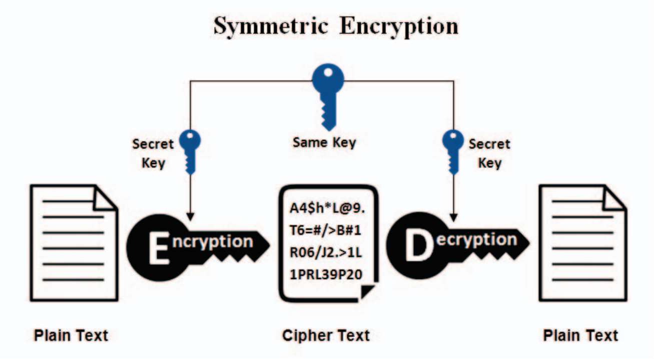

Fig. 1. The general idea of symmetric-key cryptography [4]

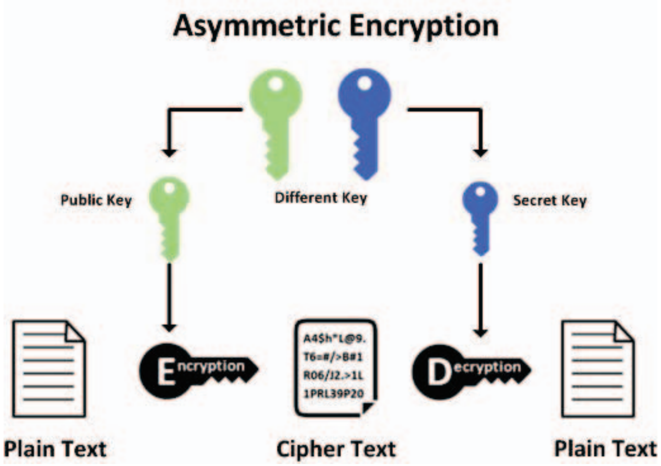

Fig. 2. The general idea behind asymmetric-key cryptography [4]

message.

Cipher Text: Cipher means a code or a secret message. When a plain text is codified using any suitable scheme the resulting message is called a ciphertext.

Key: the key is one of the most important parts of performing encryption and decryption. The choice the key used is what makes the process of cryptography secure.

Symmetric key: also known as secret key cryptosystems. Only one key is used in both encrypting and decrypting processes.

Asymmetric key: contrary to the Symmetric, Asymmetric use two different keys: one for encryption and one for decryption. This system is also known as a public key cryptosystem.

C. Need of Cryptography

Cryptography [6] is used to achieve many goals, and some of the goals are the following list shows: the goals are the following list shows:

- Access Control: this means the unique confirmation of the group with correct authentication that is eligible to log into the delivered message.
- Data Integrity: is the process in which the access of modulating the database belongs to a specific group or person.
- Non-Repudiation: while the sender and receiver agree that acknowledge the delivery of the report.
- Authentication: Are the phenomena to offer identity to a special person in order to break special resource using keys.
- Confidentiality: is the ultimate objective of encryption and decryption that ensure that only the receiver of the message is the cipher-key owner.

II. RSA ALGORITHM

RSA is an encryption algorithm, and it is an abbreviation of Rivest Shamir Adleman ,which was invented by professors Leonard Adleman ,Adi Shamir, and Ron Rivest in Massachusetts lab (MIT) in the year 1978 [7]. RSA is using the asymmetric encryption key that has two different keys, one is a public key which is known by everyone and will be using for the encryption process. While the other key is a private key that will be used for the decryption process of the encrypted message. Asymmetric encryption is unlike the symmetric encryption which is using only one key for both the encryption and decryption processes. The primary advantage of the asymmetric encryption key is to have strong encryption that will make the decryption of the original text difficult and cannot be predicted by hackers . There are several steps to implement the RSA algorithm on a plain text. Adki and Hatkar [8] have summarized the steps of RSA algorithm as the following; first, two prime numbers a and b should be selected. Then, there should be modulus for the public, and private keys called n that is multiply by b. Next, an e should be selected which is a public key and is not a factor of $(a-1)(b-1)$. After that, a private key called d should be calculated as the following $(d*e)$ mod $(a-1)(b-1) = 1$. The encryption will be calculated as C= Me mod n, where C is the ciphertext, and M is the original text. Lastly, the decryption will be calculated as $M = Cd$ mod n, where C is the ciphertext, and M is the original text. Also, to ensure a high level of security the key size should be greater than 1024 bits; to make it difficult for the hacker to identify [9]. The following example (Example1) will explain better the process.

Example1: To demonstrate the RSA public key encryption algorithm, let's start it with 2 smaller prime numbers 5 and 7. Generation the public key and private key with prime numbers of 5 and 7 can be illustrated as:

- Given p as 5
- Given q as 7
- Compute $n = p * q : n = 5 * 7 = 35$
- Compute $m = (p-1) * (q-1) : m = 4 * 6 = 24$
- Select e, such that e and m are coprime numbers:
- $e = 5$
- Compute d, such that d*e mod m = 1: d = 29
- The public key $\{n, e\}$ is = $\{35, 5\}$
- The private key $\{n, d\}$ is = $\{35, 29\}$
- With the public key of $\{35, 5\}$, encryption of a cleartext M represented as number 23 can be illustrated as:
- Given public key $\{n, e\}$ as $\{35, 5\}$
- Given clear text M represented in number as 23

- Divide B into blocks: 1 block is enough
- Compute encrypted block $C = M \wedge e \bmod n$:

$C = 23 \wedge 5 \bmod 35 = 6436343 \bmod 35 = 18$ The ciphertext C represented in number is 18 With the private key of 35, 29, decryption of the cipher text C represented as number 18 can be illustrated as: Given private key n,e as 35,29 Given ciphertext C represented in number as 18 Divide C into blocks: 1 block is enough Compute encrypted block:

$M = C \wedge d \bmod n:$

$M = 18 \wedge 29mod35 = 18 * 18 \wedge 28 \bmod 35$

$= 18 * (18 \wedge 4) \wedge 7 \bmod 35$

$= 18 * (104976) \wedge 7mod35$

$= 18 * (104976 \bmod 35) \wedge \bmod 35$

$= 18 * (11) \wedge 7 \bmod 35$

$= 18 * 19487171 \bmod 35$

$= 350769078 \bmod 35$

$= 23$

The clear text M represented in number is 23.

III. EL-GAMAL ALGORITHM

The El-Gamal algorithm [10] is known as a asymmetric cryptosystem. It is so powerful in terms of encrypting and decrypting. This algorithm present the same form in order to encrypt within the public key and private key environment. Therefore, encryption is not the same as signature verification. signature creation depends on the El-Gamal signature algorithm. The main disadvantage of El-Gamal is the need for randomness, and its slower speed (especially for encrypting and decrypting).the main disadvantage that present o El-Gamal algorithm is that the use expensing the message by one or two factors, which take place during encryption. Consequently, such message expansion is negligible if the cryptosystem is used only for exchange of secret keys El-Gamal encryption.

IV. COMPARISON EL-GAMAL ALGORITHM AND RSA

El-Gamal is not semantically secure. El-Gamal algorithms [10] can not only be used in data encryption, but in digital signature and the security relies on the problem of divergence logarithm in finite domains. Firstly, choose a prime number p, and two random number g, x, where $g < p$ and $x < p$, calculate $Y = g \wedge x(\bmod p)$, of which y, g, and p are the public Comparison of El-Gamal and RSA algorithms has been done on the basis of security and time consumption for encryption and decryption. This paper analyze that ElGamal algorithm is more secure as compared to RSA algorithm because it generates more complex cipher text and it was also slow because when we encrypt and decrypt it, it generates more than one public keys. The research in this paper [11] presents the problem that ElGamal digital signature security is constantly being challenged and increasingly becomes iserious, an improved ElGamal comparison is proposed. Although, ElGamal algorithm is considered secure and reliable [12] and It has the advantage of making the same plaintext that gives a different cipher text, each time it is encrypted. But it has its own disadvantages. The main problem that only one random number is used. Also analysis showed another major disadvantage: the cipher text is twice as long as the plaintext. El-Gamal Algorithm is comparable to RSA as showed in Table2.

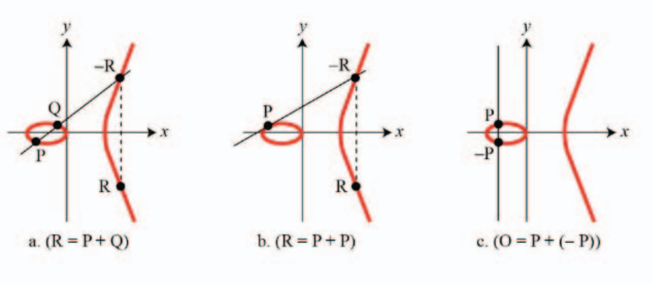

Fig. 3. Three adding cases in an elliptic curve

TABLE I
SUMMARY TABLE ON SYMMETRIC ALGORITHMS OF RSA AND EL-GAMAL

S.NO	Factors	RSA	El-Gamal
1	Developed	1978	1985
2	Key Length Value	>1024 bits	1024 bits
3	Type of Algorithm	Asymmetric	Asymmetric
4	Security Attacks	Timing Attack	Meet-in-The middle Attack
5	Simulation Speed	Fast	Fast
6	Scalability	No Scalability occurs	Good scalability
7	Key Used	Different key used for Encrypt and Decrypt Process	Different key used for Encrypt and Decrypt Process
8	Power Consumptin	High	Low
9	Hardware and Software Implementation	Not very efficient	Faster and efficient

V. ELEPTIC CURVE ALGORITHM

Neal Koblitz and Victor S. Miller independently introduced Elliptic Curve cryptography in 1985 and 1987 [13]. Elliptic curve cryptography transforms a mathematical problem in to an EE applicable computer algorithm. In general, public key cryptography brings the complex problem into a cryptosystem. Elliptic Curve cryptography (ECC) [14] is based upon the algebraic structure of elliptic curves over a finite field. Figure 3 represents different illustrations of an elliptic curve.

Example 2: $(p = 7, n = 2, a = 1, b = 6)$

$y^2 = x^3 + x + 6$

(Note:$4 + 27 * 36 = 976 = 3$ mod7)

There are 49 integer points on this "curve"

Ex: $(3, 6) \rightarrow 3 \wedge 3 + 3 + 6 = 36 \bmod 7 = 1 = 6 \wedge 2 \bmod 7$

$(4, 2) \rightarrow 4 \wedge 3 + 4 + 6 = 74 \bmod 7 = 4 = 22 \bmod 7$

$(6, 5) \rightarrow 6 \wedge 3 + 6 + 6 = 228 \bmod 7 = 4 = 52 \bmod 7$

Points on the "curve" for which there are solutions:
$(1,1),(1,6),(2,3),(2,4),(3,1),(3,6),(4,2),(4,5),(6,2),(6,5)$
Note: $(3,1),(2,3),(6,2)$ are on the same line.
$y = 2x + 7, y = x/3$ are the same line
(7 mod 7 = 0, $1/3$ is the inverse of 3 which is - 2).

VI. COMPARISON BETWEEN ECC AND RSA ALGORITHMS

The primary advantage of the RSA algorithm is the use of a private key, which is not transmitted with the encrypted text, which makes it impossible to be known by the hacker. Also, providing a digital signature by the public key in RSA give it a powerful feature [5]. The digital signature can be defined as an online signature that will provide two main points, first is that the message was sent to the required person with no changes, second, is that the identity of the sender is guaranteed [15]. On the other hand, the main disadvantage of the RSA algorithm is its slow processing [5]. ECC is based upon the algebraic structure [16] of elliptic curves over a finite field. The main advantage of ECC over other public key algorithms like RSA, key exchange. It requires shorter key lengths to make sure the same level of security. For example, 160 bit key in ECC is considered to be as secure as 1024 bit key in RSA. Other than this ECC in particularly appropriate for wireless communication. Elliptic Curve Cryptography has become the cryptographic choice for networks and communication devices due to its size and efficiency benefits. Elliptic curve cipher uses very small keys and is computationally very efficient, which makes it ideal for the smaller, less powerful devices being used today by most individuals to access network services. Elliptic curve cryptography is more complicated than RSA. As in RSA single encryption algorithms is used. ECC can be implemented in different ways. ECC uses arithmetic algorithms as the main objective operations for high-level security functions such as encryption for gaining confidentiality and a digital signature for authentication. ECC can be implemented in software and in hardware. ECC follows generic procedure like parties agree on publicly-known data items and each user generates their public and private keys [9] [17] [15] [13] [18] [19].
Overall ECC is more efficient and secure than RSA as shown in Table 2.

TABLE II
COMPARISON BETWEEN RSA AND ECC

Security Bit Level	RSA	ECC
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	512

VII. CONCLUSION

This paper presents a survey of the main important cryptographic algorithms such us ECC, El-Gamal and RSA.

These algorithms are studied in order to be compared. Comparisons prove that the cost of transmission is enormously reduced in ECC. The result shows the performance of ECC that are useful. We have surveyed these algorithms security because they are mostly used.

REFERENCES

[1] W. Stallings, *Network Security Essentials - Applications and Standards (4. ed., internat. ed.)*. Pearson Education, 2010.

[2] A. Kahate, *Cryptography and Network Security*. McGraw Hill Education, 2013. [Online]. Available: https://books.google.com.sa/books?id=xCDZAgAAQBAJ

[3] P. S. S. H. Vikrant M. Adki, "A survey on cryptography techniques," *International Journal of Advanced Research in Computer Science and Software Engineering*, 2016.

[4] http://www.ssl2buy.com/wiki/symmetric-vs-asymmetric-encryption-what-are-differences.

[5] V. K. Mitali and A. Sharma, "A survey on various cryptography techniques," *International Journal of Emerging Trends Technology in Computer Science*, vol. 3.

[6] S. K. G. Omar G. Abood, "A survey on cryptography algorithms," *International Journal of Scientific and Research Publications*, vol. 8, 2018.

[7] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, Feb. 1978. [Online]. Available: http://doi.acm.org/10.1145/359340.359342

[8] H. Adki, V. M., "A survey on cryptography techniques," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 6, 2016.

[9] S. A. Ritu Tripathi, "Comparative study of symmetric and asymmetric cryptography techniques," *International Journal of Advance Foundation and Research in Computer*, vol. 1, 2014.

[10] R. S. Jamgekar and G. S. Joshi, "File encryption and decryption using secure rsa," *International Journal of Emerging Science and Engineering (IJESE*, pp. 11–14, 2013.

[11] X. Li, X. Shen, and H. Chen, "Elgamal digital signature algorithm of adding a random number," *JNW*, vol. 6, pp. 774–782, 2011.

[12] AnnapoornaShetty, S. Shetty, and K. Krithika, "A review on asymmetric cryptography ?rsa and elgamal algorithm," 2014.

[13] http://www.certicom.com.

[14] R. Ansah, E.-P. Samuel, D. Attuabea, B. Adjei, B.-R. K Bawuah, and P. Antwi, "Relevace of elliptic curve cryptography in modern-day technologie," vol. 3 (2), pp. 1–10, 01 2018.

[15] A. U. Hardik Gohel, "Study of cyber security with advance concept of digital signature," *International Journal of Advanced Research in Computer Science*, vol. 6, 2015.

[16] R. Ansah, R. Boadi, W. Obeng-Denteh, and A. Y Omari-Sasu, "Review of the birch and swinnerton-dyer conjecture," vol. 2016, pp. 182–189, 08 2016.

[17] D. M. Behrouz A Forouzan, *Cryptography and Network Security*. McGraw-Hill Education, 2011.

[18] G. Shen and B. Liu, "Research on efficiency of computing kp in elliptic curve system," in *2010 6th International Conference on Wireless Communications Networking and Mobile Computing (WiCOM)*, Sep. 2010, pp. 1–4.

[19] V. G. N. G. Sheueling Chang, Hans Eberle, "Sunmicrosystems laboratories howeccworks-usletter.pdf."