ISSN: 0067-2904

A Study of Graph Theory Applications in IT Security

Turkan Ahmed Khaleel*[1], Ayhan Ahmed Al-Shumam[2]
[1]Department of Computer Engineering, Engineering College, University of Mosul, Mosul, Iraq
[2]Department of Computer Engineering Technology, Engineering Technology College, Northern Technology University, Mosul, Iraq

Received: 27/8/2019 Accepted: 2/5/2020

Abstract

The recent developments in information technology have made major changes in all fields. The transfer of information through networks has become irreplaceable due to its advantages in facilitating the requirements of modern life through developing methods of storing and distributing information. This in turn has led to an increase in information problems and risks that threaten the security of the institution's information and can be used in distributed systems environment.

This study focused on two parts; the first is to review the most important applications of the graph theory in the field of network security, and the second is focused on the possibility of using the Euler graph as a Method Object that is employed in Remote Method Invocation (RMI) technique. This algorithm was compared with the most popular algorithms, such as RSA and 3DES. The results were acceptable and need to be improved in the future.

Keywords: Graph Theory, Information Technology Security, Network Security, Cryptography.

دراسة لتطبيقات نظرية الرسم البياني في أمن تكنولوجيا المعلومات

توركان احمد خليل *[1]، ايهان احمد خليل شمام[2]

[1]قسم هندسة الحاسوب، كلية الهندسة، جامعة الموصل ، نينوى، العراق

[2]قسم هندسة تقنيات الحاسوب، كلية التقنية الهندسية، الجامعة التقنية الشماليه ، نينوى، العراق

الخلاصة

أحدثت التطورات الحديثة في تكنولوجيا المعلومات تغييرات كبيرة في جميع المجالات. ويعد نقل المعلومات عبر الشبكات أمر لا يمكن الاستغناء عنه بسبب مزاياه في توفير سبل الحياة العصرية والحديثة وذلك من خلال تطوير طرق لخزن المعلومات وتوزيعها ، مما أدى هذا إلى زيادة مشاكل التعامل مع المعلومات والمخاطر التي تهدد أمن المؤسسة المعلوماتية والتأثير عليها والذي يمكن ان يستخدم في بيئة النظم الموزعة.

ركزت هذه الدراسة على محورين: الأول مراجعة أهم تطبيقات الرسم البياني في مجال أمان الشبكة ، بينما يركز المحور الثاني على إمكانية استخدام الرسم البياني اويلر (Euler) ككائن تابع واستخدامه بتقنية استدعاء الطرائق عن بعد (RMI). تمت مقارنة هذه الخوارزمية مع الخوارزميات الأكثر شيوعًا مثل 3DES و AES و Blowfish و RSA حيث كانت النتائج مقبولة وتحتاج إلى تحسين في المستقبل.

*Email: turkan@uomosul.edu.iq

1. Introduction

Information is one of the most important parts of an organization. Its protection and preservation are essential and need to be periodically provided with strong and non-porous security. Information security consists of a combination of systems, processes and internal controls that provide assurance of the integrity and confidentiality of data and operating procedures in the organization. Providing these components has become increasingly complex and expensive. In turn, awareness of information security has increased and many institutions have implemented a high level of information security to protect their data and information [1].

Information technology (IT) security is now essential for all organizations to ensure the security of their data, protect their privacy and ensure that they are stored and transmitted in an unalterable third-party security. IT security is based on four procedures of the organization that protects the organization's ability to operate, enable secure operation of applications employed on the organization's IT systems, protect and use the data collected by the institutions, and finally protect the technology assets used in an organization. There are also challenges and risks that involve the security of IT applied in the institutions, especially in encryption [2]. For this reason, there has been a need to introduce other techniques such as graph theory.

The problem of IT security is to provide resources efficiently while maintaining the privacy of users. There has been a need to use graph theory in systems representation. For easier handling, graph theory provides simple solutions to many problems in networking and information security [3]. Thus, this paper examines some applications of graph theory in IT security.

In this study, the researchers focused on two important parts. The first part focused on giving a simple overview of some applications of graph theory in security with the mentioning of some works related to this study. While the second part includes a method of using the Euler graph in encrypting the message sent on one side of the sender and decrypting it on the other side by relying on the same graph. This algorithm was programmed using Java RMI technology to program network applications and provide independence of computers and operating systems.

2. IT Security

The goal of IT security is to enable any organization to achieve all its mission objectives and actions through the implementation of regulations, taking into account the risks associated with information technology to the organization, its partners and customers. Maintaining the security of information technology means maintaining the security of systems connected to the Internet from inappropriate intrusion, preventing unauthorized access to their data or software or the use of illegal third parties. IT security strategies focus on maintaining control over five core parts of most information systems: data, users, operating, applications and networks [4].

•**Data security**: Needs supervision of both internal users (leadership, staff, etc.) and external users (servicers, clients, etc.) [4].

•**User security level**: Certifies that only the permitted entities have admission to any part of the enterprise IT organization. Security procedures here include passwords and dual verification procedures. Moreover, information security includes protecting and storing information in a safe place and providing protection for its use or transmission [4].

• **Operating security level:** IT must be viewed from a cross-cutting perspective on the operating system and encouraging of security professionals to look for vulnerabilities in their IT [4].

• **Application Security level:** Includes providing protection to applications against any interference that may interrupt or interfere with the processing of any application or program. In general, standard application security measures often include programs such as encryptions and firewalls that prevent unauthorized access to programs or platforms and their functionality [4].

•**Network security level:** Includes the security of a wide range of computers and operators who are interconnected and share applications and information safe from intrusion. Network security includes both hardware and software and all tools to manage access to any port, terminal or database anywhere in the network [4].

Encryption plays an active and important role in IT security. It provides confidentiality by encrypting the message content, verifying authentication and achieving integrity by verifying the contents of the message. In this research, the Hamiltonian graph interface was used to encode information by representing them in the form of an object placed on the server and accessed remotely.

It can be used at any of the previously mentioned levels. It is possible to encrypt messages at the levels of data security or network security and others.

3. Graph Theory Applications

Graph theory has become a very important component in many applications in the field of network security. Unfortunately, understanding the graph theory and its applications is one of the most difficult and complex missions. In this study, the authors reviewed some main applications of graph theory in IT security. Some aspects of graph theory applications were covered, especially with regard to encryption. There are some complex issues that can encounter developed algorithms only after study and analysis; therefore, it is important to express them in the best possible way which makes the process written in the program easier [5]. Table (1) summarizes some related works that have applied graph theory in different types of networks and information security field.

Table 1- Some related works on graph theory applications

Year	Title	Authors	Journal	Applications
2013	Cryptanalysis and Improvements on Some Graph-Based Authentication Schemes	Eftekhari and Abdullah	Journal of Discrete Mathematical Sciences and Cryptography	In this paper [6], the researchers analyzed two graph-based authentication protocols. The weaknesses of each method were clarified. They proposed a new scheme without addressing the method of determining the number of nodes.
2014	Encryption Algorithm Using Graph Theory	Mahmoud and Etaiwi1	Journal of Scientific Research& Reports	In this paper [7], the researchers presented a symmetric Cryptographic algorithm to encode data for the purpose of transferring by using a coding table. However, they did not mention the possibility of its application in distributed systems.
2014	Network Security Using Graph Theory	Sen and Samanta	IJIRT	In this paper [8], the researchers focused on the possibility of using graph theory concepts in network monitoring and assessing the importance of individual routers within a network giving traffic pattern.
2014	Formal Security Model for Virtual Machine Hypervisors in Cloud Computing Systems	Zegzhda and Nikolsky	Nonlinear Phenomena in Complex Systems.	In this paper [9], the possibility of using graph theory in some security models for some virtualization software used in cloud systems is described.
2015	On Attack Graph Model of Network Security	Sahakyan, and Alipour	International Journal of Information Content and Processing	In this paper [10], the researchers suggested a general model of offensive graphs and an outline of the algorithm to generate the attack graph. However, they did not use this algorithm to implement the distributed systems.
2016	A Graph Based Message Encryption Algorithm	Dutta, et. al.	International Journal of Pharmacy & Technology	In this paper [11], an algorithm for encryption using the Euler graph is proposed by using encoder tracking the Hamilton circle from the encoded graph. However, the

				researchers had a problem applying it where each graph carries one letter of a message.
2018	An Application of Graph Theory in Cryptography	Amudha, Sagayaraj and Sheela	International Journal of Pure and Applied Mathematics .	In this paper [12], the researchers suggested same algorithm mentioned in paper [11] where the messages were encoded by the Euler graph. They used Hamilton circle as a key to secure the data, but they also had two problems. The first is that letters are converted to uppercase, which means that this dialogue can only be used for English letters. The second problem is that each graph holds only one letter at a time.
2018	Application of Graph Theory Concepts in Computer Networks and its Suitability for the Resource Provisioning Issues in Cloud Computing-A Review	Rangaswamy and Gurusamy	Journal of Computer Science.	In this paper [13], the researchers made some suggestions concerning the graph theory to address the problems of working with core resources and providing secure cloud computing environments.
2018	A Secure Enhancement for Encoding/ Decoding data using Elliptic Curve Cryptography	Abdullah, K. E., and Ali	Iraqi Journal of Science	In this paper [14], a new method for converting the text message to a point on the curve or point to a text message was investigated in an effective and safe way, as this method relies on repeated values on the axis to create the search table for encoding/decoding operations.
2019	Proposal Hybrid CBC Encryption System to Protect E-mail Messages	Hashem	*Iraqi Journal of Science*	In this paper[15], the researcher suggested a hybrid Cipher Block Chaining encryption system for email protection. The proposal was relied on the incorporation of coding technologies.
2019	Key Generator to Encryption Images Based on Chaotic Maps	Yousif and Kashmar	Iraqi Journal of Science	In this paper[16], the researchers presented a method for generating a new key based on chaotic maps that are used to encode images

4. Model Discerption

In IT, the distributed applications are significantly required. To create a distributed application, we need to allow methods such as Java Remote Procedure Call (RMI) to be called RMI is an RPC (remote procedure call) equivalent [17]. It is an application programming interface that provides a mechanism for creating a distributed application in Java. RMI provides a remote connection between applications that use both stub and skeletal objects [17], as shown in Figure- 1. In this study, the

authors relied on the theory of coding graph presented in previous references [11, 12] which only encoded English words after they were converted to capital letters. They relied on the development of a general algorithm to coding and decoding messages in any language. Also, they made some modifications, set up two algorithms and implemented them using Java language and RMI. The RMI is an equivalent object of RPC [13]. It is important in distributed systems used in information technology, in addition to its advantage to allow RMI system for an object running in the Java Virtual Machine (VM) to call the methods of an object running in another Java VM. RMI provides remote communication between programs written in the Java programming language [13], as shown in Figure- 1.

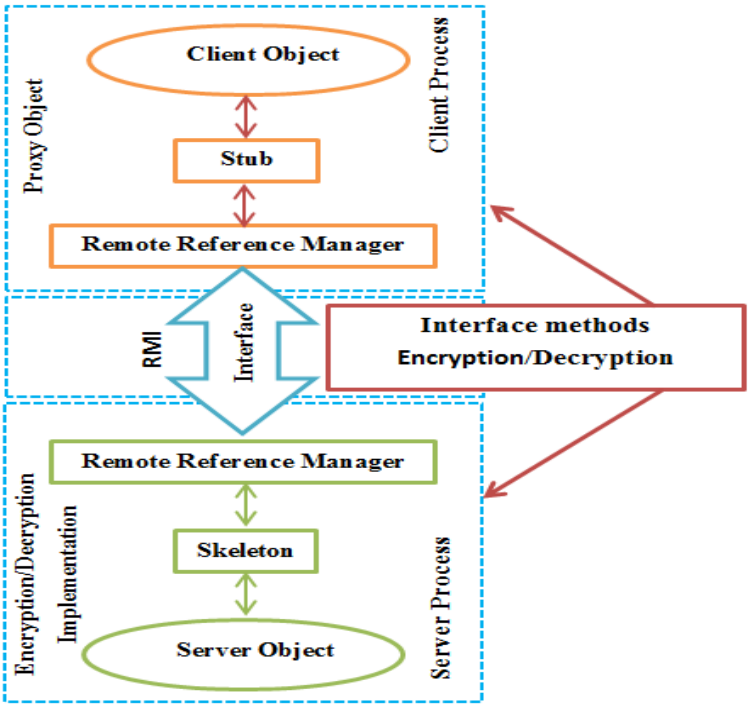


Figure 1- Model Description

4.1 Encryption Method Algorithm

1- Get the message stream (input).
2- For each character, take ASCII value in binary format.
3- For each binary number, evaluate XOR_{32} (XOR with the binary equivalent of 32).
4- Create graph A (V, E) where A is graph, V is the vertices and E is edges, as in the following steps:
4.1- Count the number of once (1's bit) for each binary number, store the result in one dimensional array (M).
4.2- Create adjacency matrix (A) which is symmetric matrix, where its size is equal to number of once (1's) bit in array M.
4.3- Store zeros for diagonal elements of the matrix A.
4.4- Count (L) the number of zeros (0's bit) that follows after each once (1's bit) for every binary number.
4.5- If the binary stream ends with a once (1's bit) and followed by L number of zeros (0's bit), then L=L+1.
4.6- If the last element of binary number is equal to 1, then put 1 in the last element in row 1 of A.
5- Create one dimensional array B that continues the upper main diagonal matrix A.
6- Add the last element at the row one in adjacency matrix (A) to B.
7- The adjacency matrix B is sent to the receiver side (output).
8- The above steps are repeated until Hamiltonian circuit tracing reaches to the end vertex.

4.2 Decryption Method Algorithm

1- Get the adjacency matrix B that is received (input).
2- For each element of B, do the following:

2.1 Create adjacency matrix C, where its size is equal to the size of B.
2.2 For i=1 to size -1 of B, put the element of B (i) in the upper main diagonal matrix C.
2.3 Put the last element of B in the last element in row 1 of C.

3- To get back the original massage (A), the steps (6-2) used in the encryption algorithm are applied backwards.

4- Output message(A).

5. Results

In this study, the above algorithms (encryption and decryption) are programmed as interface methods and implemented in the server side. The authors create two classes, one for the server sides and the other for the client side, according to the steps mentioned to configure RMI. The program was applied to send three messages in three different languages (Arabic, Turkish, and English). An example of the message used in this study is "سلام", "PEACE" and "BARIŞ", respectively. The results are presented in Tables- (2-4).

Table 2- Some results for message "سلام"

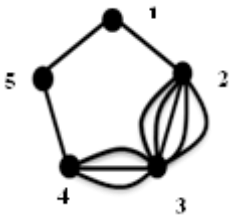
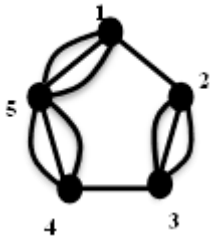
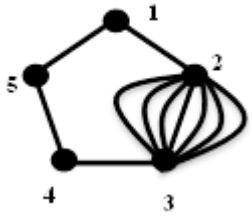
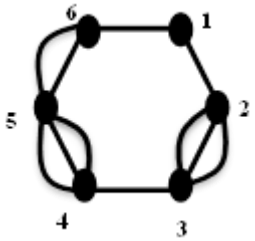
Alphabet	س	The adjacency Matrix	The Graph
ASCII Code	1587	$س = \begin{bmatrix} 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 5 & 0 & 0 \\ 0 & 5 & 0 & 3 & 0 \\ 0 & 0 & 3 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \end{bmatrix} \Leftrightarrow$ س	
Binary Number	11000110011		
XOR_{32}	11000010011	Send [1 5 3 1 1]	
Alphabet	ل	The adjacency Matrix	The Graph
ASCII Code	1604	$ل = \begin{bmatrix} 0 & 1 & 0 & 0 & 3 \\ 1 & 0 & 3 & 0 & 0 \\ 0 & 3 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 3 \\ 3 & 0 & 0 & 3 & 0 \end{bmatrix} \Leftrightarrow$ ل	
Binary Number	11001000100		
XOR_{32}	11001100100	Send [1 3 1 3 3]	
Alphabet	ا	The adjacency Matrix	The Graph
ASCII Code	1575	$ا = \begin{bmatrix} 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 7 & 0 & 0 \\ 0 & 7 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \end{bmatrix} \Leftrightarrow$ ا	
Binary Number	11000100111		
XOR_{32}	11000000111	Send [1 7 1 1 1]	
Alphabet	م	The adjacency Matrix	The Graph
ASCII Code	1605	$م = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 3 & 0 & 0 & 0 \\ 0 & 3 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 3 & 0 \\ 0 & 0 & 0 & 3 & 0 & 2 \\ 1 & 0 & 0 & 0 & 2 & 0 \end{bmatrix} \Leftrightarrow$ م	
Binary Number	11001000101		
XOR_{32}	11001100101	Send [1 3 1 3 2 1]	

Table 3- Some results for message "PEACE"

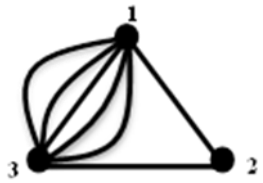
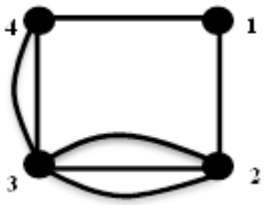
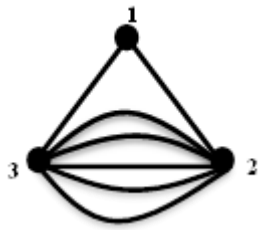
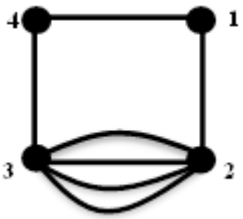
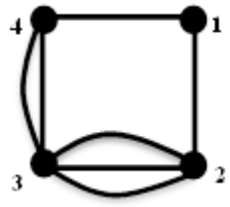
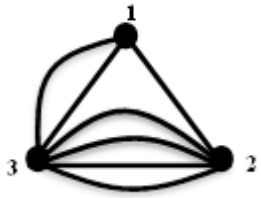
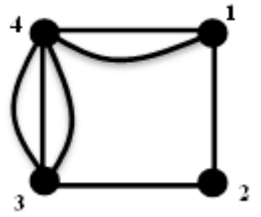
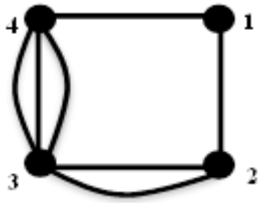
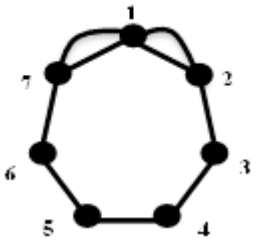
Alphabet	P	The adjacency Matrix	The Graph
ASCII Code	80	$P=\begin{bmatrix}0&1&5\\1&0&1\\5&1&0\end{bmatrix}\overset{P}{\Leftrightarrow}$	
Binary Number	1010000		
XOR_{32}	1110000	Send [1 1 5]	
Alphabet	E	The adjacency Matrix	The Graph
ASCII Code	69	$E=\begin{bmatrix}0&1&0&1\\1&0&3&0\\0&3&0&2\\1&0&2&0\end{bmatrix}\overset{E}{\Leftrightarrow}$	
Binary Number	1000101		
XOR_{32}	1100101	Send [1 3 2 1]	
Alphabet	A	The adjacency Matrix	The Graph
ASCII Code	65	$A=\begin{bmatrix}0&1&1\\1&0&5\\1&5&0\end{bmatrix}\overset{A}{\Leftrightarrow}$	
Binary Number	1000001		
XOR_{32}	1100001	Send [1 5 1]	
Alphabet	C	The adjacency Matrix	The Graph
ASCII Code	67	$C=\begin{bmatrix}0&1&0&1\\1&0&4&0\\0&4&0&1\\1&0&1&0\end{bmatrix}\overset{C}{\Leftrightarrow}$	
Binary Number	1000011		
XOR_{32}	1100011	Send [1 4 1 1]	
Alphabet	E	The adjacency Matrix	The Graph
ASCII Code	69	$E=\begin{bmatrix}0&1&0&1\\1&0&3&0\\0&3&0&2\\1&0&2&0\end{bmatrix}\overset{E}{\Leftrightarrow}$	
Binary Number	1000101		
XOR_{32}	1100101	Send [1 3 2 1]	

Table 4- Some results for message "BARIŞ"

Alphabet	B	The adjacency Matrix	The Graph
ASCII Code	66	$A = \begin{bmatrix} 0 & 1 & 2 \\ 1 & 0 & 4 \\ 2 & 4 & 0 \end{bmatrix} \overset{B}{\Leftrightarrow}$ Send [1 4 2]	
Binary Number	1000010		
XOR_{32}	1100010		
Alphabet	A	The adjacency Matrix	The Graph
ASCII Code	65	$A = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 4 \\ 1 & 4 & 0 \end{bmatrix} \overset{A}{\Leftrightarrow}$ Send [1 4 1]	
Binary Number	1000001		
XOR_{32}	1100001		
Alphabet	R	The adjacency Matrix	The Graph
ASCII Code	82	$R = \begin{bmatrix} 0 & 1 & 0 & 2 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 3 \\ 2 & 0 & 3 & 0 \end{bmatrix} \overset{R}{\Leftrightarrow}$ Send [1 1 3 2]	
Binary Number	1010010		
XOR_{32}	1110010		
Alphabet	I	The adjacency Matrix	The Graph
ASCII Code	73	$I = \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 2 & 0 \\ 0 & 2 & 0 & 3 \\ 1 & 0 & 3 & 0 \end{bmatrix} \overset{I}{\Leftrightarrow}$ Send [1 2 3 1]	
Binary Number	1001001		
XOR_{32}	1101001		
Alphabet	Ş	The adjacency Matrix	The Graph
ASCII Code	350	$Ş = \begin{bmatrix} 0 & 2 & 0 & 0 & 0 & 0 & 2 \\ 2 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 2 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} \overset{Ş}{\Leftrightarrow}$ Send [2 1 1 1 1 1 2]	
Binary Number	101011110		
XOR_{32}	101111110		

A cipher algorithm using Euler Graph was compared in this research with the following traditional Cryptographic algorithms: 3DES, AES, Blowfish and RSA. The results show that each encryption algorithm has its own strengths and weaknesses. To choose an appropriate encryption algorithm for an application, we must have knowledge of the performance, strength and weakness of each algorithm. As shown in Figure-2, the speed of coding and decoding when implementing the Blowfish algorithm is better than that for all algorithms, while the worst implementation time is recorded when implementing the RSA algorithm. All of 3DES, AES, and Euler Graph require an average execution time.

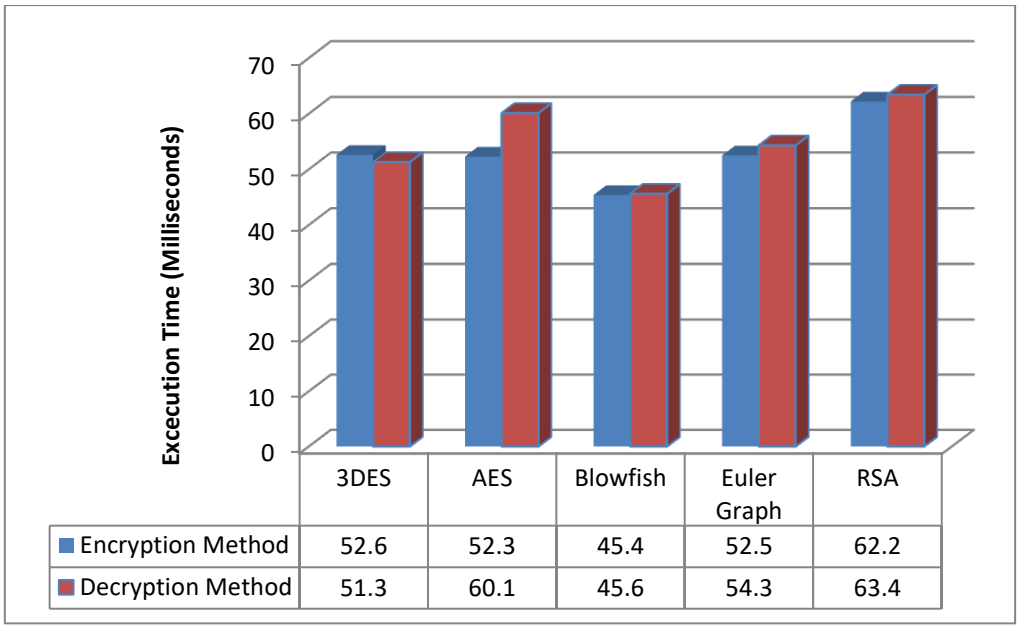


Figure 2- Execution time comparisons of some cryptographic algorithms

6. Conclusions

The results of this study showed that the Euler graph encoding method used with RMI technology is efficient, regardless of message language. Additionally, the time to implement the Euler graph encoding method with RMI technology is shorter when compared with the traditional encryption algorithms such as AES, 3DES and RSA, while it is not faster than the Blowfish encryption algorithm. In future works, it is necessary to employ traditional algorithms and link them with the techniques of RMI used in distributed systems, which cannot be dispensed within information technology.

References

1. Zhu H., Wu J., Shi H., Wang C., Li Y. **2018**. Discussion on Information Security Technology of Big Data System. *Journal of Physics: Conference Series*. **1087**(1): 1-6.
2. Cavusoglu, H.; Mishra, B. and Raghunathan, S. **2004.** A Model for Evaluating IT Security Investments. *Communications of the ACM*. **47**(7): 87-92.
3. Sadowsky, G.; Dempsey, J. X.; Greenberg, A.; Mack, B. J. and Schwartz, A. **2003**. *Information Technology Security Hand Book*, ISBN 0-9747888-0-5, P:8.
4. Browning, J. **2015**. *Security Features in the Teradata Database*, Teradata Corporation.
5. Hassan, M. A. and Chickade, A. **2011**. A Review of Interference Reduction in Wireless Networks Using Graph Coloring Methods. *International Journal on Applications of Graph Theory in Wireless Ad Hoc Networks and Sensor Networks* (GRAPH-HOC), **3**(1).
6. Abdullah, H. O. and Eftekhari, M. **2013**. Cryptanalysis and Improvements on Some Graph-Based Authentication Schemes. *Journal of Discrete Mathematical Sciences and Cryptography*, **16**(4-5):297-306.
7. Mahmoud, W. and Etaiwi, A. **2014.** Encryption Algorithm Using Graph Theory. *Journal of Scientific Research & Reports*, **3**(19): 2519-2527.
8. Sen, S. Samanta, S. **2014.** Network Security Using Graph Theory. *IJIRT*, **1**(4): 223- 230.
9. Zegzhda, D. P. and Nikolsky, A. V. **2014.** Formal Security Model for Virtual Machine Hypervisors in Cloud Computing Systems. *Nonlinear Phenomena in Complex Systems*, **17**(3): 253– 262.
10. Sahakyan, H. and Alipour, D.**2015.** On Attack Graph Model of Network Security. *International Journal of Information Content and Processing*, **2**(1): 26-42.
11. Dutta, A., A.; Sandhu, P. S. and Thandeeswaran, R. **2016.** A Graph Based Message Encryption Algorithm, *International Journal of Pharmacy and Technology*, **8**(4): 26339-26345.
12. Amudha, P.; Sagayaraj, A. C. C. and Sheela, A. C. S. **2018**. An Application of Graph Theory in Cryptography. *International Journal of Pure and Applied Mathematics*, **119**(13): 375-383.

13. Rangaswamy, K. D. and Gurusamy, M. **2018**. Application of Graph Theory Concepts in Computer Networks and its Suitability for the Resource Provisioning Issues in Cloud Computing-A Review, *Journal of Computer Science*, **14**(2): 163-172.
14. Abdullah, K. E., and Ali, N. H. M., **2018.** A Secure Enhancement for Encoding/ Decoding data using Elliptic Curve Cryptography, *Iraqi Journal of Science*, **59**(1A): 189-198.
15. Hashem, S. H., **2019.** Proposal Hybrid CBC Encryption System to Protect E-mail Messages, *Iraqi Journal of Science*, **60**(1): 157-170.
16. Yousif, A. and Kashmar, A. H., Key Generator to Encryption Images Based on Chaotic Maps, *Iraqi Journal of Science*, **60**(2): 362-370.
17. Grosso, W., **2001**. *Java RMI: Designing & Building Distributed Applications, O'Reilly Media*, first edition, Pp: 572.