Proposing an Encryption Algorithm based on DES

Omar Zughoul[1], Hajar Mat Jani[2]

[1]Universiti Tenaga Nasional, College of Graduate Studies,
Jalan IKRAM-UNITEN, 43000 Kajang, Selangor, Malaysia

[2] Universiti Tenaga Nasional, College of Information Technology,
Jalan IKRAM-UNITEN, 43000 Kajang, Selangor, Malaysia

Abstract: ***In this paper, a new method for key generation using Data Encryption Standard (DES) is proposed in order to make it more secure than DES algorithm, but at the same time faster than 3DES algorithm. Some parts of the DES are modified to improve its security and performance aspects. The proposed algorithm is named XS-DES (Extra Secure DES). We modify the process of key generation to improve its level of security, and present the proposed algorithm's design structure in more detail. We increase the size of the key from 64 bits into 128 bits, and then split the key into two halves, left and right (Kl, Kr), and each one consists of 64 bits. XS-DES will be used to encrypt some important information inside the database, like passwords, exam scores, and other confidential details. In other words, to increase the security in the database and protect it from attackers, all critical information must be encrypted using a strong encryption algorithm and a more secure algorithm (XS-DES) is proposed here. A workable Online Examination System (OES) that applies XS-DES and the original DES algorithms is developed. It has gone through some preliminary testings and a comparison is performed between the results of these algorithms based on their strengths in handling database attackers.***

Keywords: Database Security, DES, 3DES, and XS-DES.

1. Introduction

The challenges for the security of databases increased because of the enormous popularity of e-business. In these days, the insider attacks gathered more attention than outsider attacks [1]. The insiders have a big opportunity to attack and it is difficult to compromise them. The attackers can steal the information from the database in many ways and it is easy for them because the information and data are stored as plain text.

Cryptography is the art and science of protecting information from undesirable individuals by converting the information into a form non-recognizable by its attackers while the information are being stored and transmitted [2]. There are two basic techniques for encrypting data and information; the first one is "Symmetric cryptography", which means using the same key to encrypt/encode and decrypt/decode its data. The second one is "Asymmetric", which needs the usage of both public and private keys. Symmetric requires knowing the private key by the party encrypting the data and the party decrypting the data. Asymmetric permits the use of your public key by anyone to encrypt the data but the only person who can decrypt it is the one who has the private key.

2. Database Security

The security of database becomes so important in industrial, government domain and in organizations and companies. There are huge amounts of data and confidential information stored in organizations' databases and some of these data and information are considered sensitive and important. In other words, these details should not be readable except for authorized people.

One of the solutions for avoiding the risk of attackers is to encrypt the data inside the database, which means that there is a need to create a cipher text from plain text or in other words convert a plain text (original text) to cipher text (text after encrypt) to make the original text unreadable and without any meaning.

There are three major elements of data security; the first is "confidentiality", which means that the data is only readable by authorized people; the second is "integrity", which ensures that the data sent and received are the same without any interferences or changes. And the third is "authentication", which ensures that users are well-identified [3].

3. Data Encryption Standard (DES)

Data encryption standard (DES) algorithm is a strong cipher; however, according to Grabbe [4], its key length is too short to provide much security against a "well-financed" attacker. In addition, DES is a block cipher algorithm which means that it takes a fixed length of the message and encrypts it (encrypts the block), and returns a string in the same size. DES is the first encryption algorithm recommended by NIST (National Institute of Standards and Technology).

It has been developed in the early 1970s by IBM for NBS (National Bureau of standards). After that, in 1976 the NBS selected a modified version of DES after deliberation with the NSA (National Security Agency) and published for the US in 1977 as a Federal Information Processing Standard (FIPS) [5]. After 25 years of researching and analyzing, researchers found that the only security problem with DES is its key length, which is, too short [6].

Data Encryption Standard (DES) algorithm has been a popular secret key encryption algorithm and it is used in many commercial and financial applications. Although it was introduced in 1976, it has proven resistant to all forms of cryptanalysis. However, as stated by Chang [7], its key size is too small by current standards and its 56-bit key space can only be searched in approximately 22 hours". Fig.1 below shows how DES algorithm works:

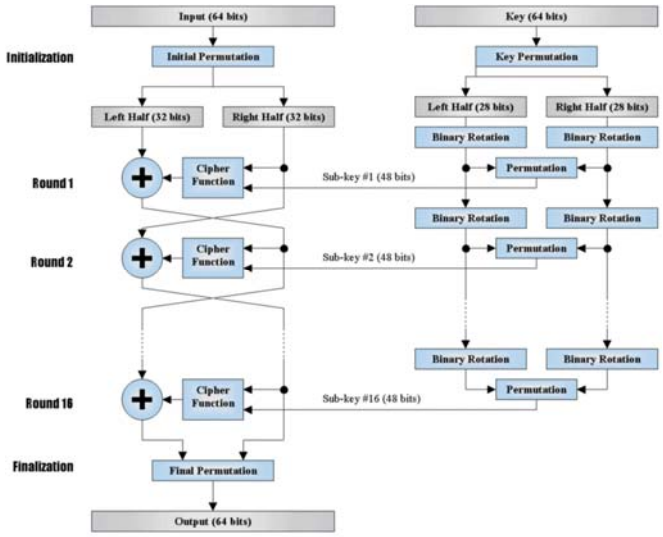

Figure 1: DES algorithm

3.1 DES encryption

There are two steps to encrypt the message using DES, the first one is the *key generation*, and the second one is the *message*. We will start with the key generation.

3.1.1 Key generation

The key of DES algorithm originally consists of 64 bits. It is reduced to 56 bits through a fixed table, which is called PC1 (Table 1). The new key has 56 bits; here, the key splits into two parts or two 28-bit halves. The first one is called C0 and the second one called D0 where each one consists of 28 bits. To get C1, D1, both C0 and D0 are rotated one bit to the left using a fix table which is called shifting table or iteration (Table 2). Then, C1and D1 are combined to get the 56 bits, out of which we choose the 48-bit key K1 using the key choice table called the permuted choice table 2, or PC-2 (Table 3). To generate all keys, the same steps in generating the first key are repeated for 16 rounds [8].

In general, for each key Ki (i > 0), Ci and Di must first be obtained by rotating each Ci-1and Di-1 one bit to the left, respectively, using the shifting table (Table 4), i.e., C1and D1 is obtained from C0, D0, C2 and D2 from C1, D1 and subsequently, Cn, Dn is obtained from Cn-1, Dn-1 where n takes the value from 1 to 16, because DES has to undergo 16 rounds for the keys and messages. Then, the 48-bit key Ki is produced by combining Ci and Di and using PC-2. That is, C1 and D1 are used to generate the key output K1 by combining them and permuted the combination using PC-2, C2 and D2 to generate K2, and so on until finally, Cn, Dn are combined and permuted to get Kn, where n is from 1 to16.

Table 1: PC-1

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	**61**	53	45	37	29
21	13	5	28	20	12	4

Table 2: Iteration

Round	*Left Shifts*
1	1
2	1
3	2
4	2
5	2
6	**2**
7	2
8	2
9	1
10	2
11	2
12	2
13	2
14	2
15	2
16	1

Table 3: PC-2

14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

3.1.2 The message

DES (and most of the other major symmetric ciphers) is based on a cipher known as the Feistel block cipher. The basic principle of Feistel ciphers is that the plain text block is split into two halves and each half is used to encrypt the other half over a predetermined number of rounds. Thus, DES is a symmetric, 64-bit block cipher as it uses the same key for both encryption and decryption and only operates on 64-bit blocks of data at a time. In general, DES algorithm divides a message into blocks where each block consists of 64 bits.

The encryption begins with an initial permutation using the fixed initial permutation (IP) table, which rearranges the 64 bits of the message data in a fixed pattern. The result of the initial permutation is divided into two blocks L0 and R0, and each block consists of 32 bits. Subsequently, DES generates L1 to L16 and R1 to R16 using the formula, which is given as the following:

$$L_j = R_{j-1} \quad (1)$$

$$R_j = L_{j-1} (+) F(E(R_{j-1}), K_j) \quad (2)$$

where j = 1, 2, ... , 16. (2)

Thus, for example, from equation (1), when j = 1, L1 = R0 while R1= L0 (+) F(E(R0), K1) according to equation (2). Equation (2) can be further described as follows. For any j, F(E(R j-1), K j) means that the function F takes the 32-bit R half, i.e., R j-1, and 48-bit sub-key Kj, in which E(R j-1) denotes that the 32-bit R j-1 is expanded to 48 bits using the E-box expansion permutation table.

The expansion of R j-1 to 48 bits is because K1 is 48 bits. The result of E(R j-1) is then XORed (+) to the key Kj. Next, the XOR result will then be grouped to 8 blocks where each block consists of 6 bits. This result is then passed

through S-Box substitution to get 32-bit result and then the permutation using the P-box permutation is applied to permute the output of the S-box without changing the size of the data. Finally, this result is then XORed (+) to the key L j-1 in order to get Rj as in equation (2). These steps are then iterated 15 more rounds to produce L2 and R2, L3 and R3 and so on until L16 and R16. The total number of iteration is 16 rounds if including L1 and R1.

At the end of the 16th round, the 32-bit Li and Ri output quantities are swapped to create what is known as the pre-output. Finally, the pre-output is passed through the final permutation (Fb) using the (IP^{-1}). In other words, the final permutation is the inverse of the initial permutation; the table is interpreted similarly, that is IP^{-1} is the inverse of the IP table. This final process is converting the Fb into hexadecimal (the encrypted text) such that the output of IP^{-1} is the 64-bit cipher text.

3.2 DES decryption

Any symmetric algorithm has only one key for encryption and decryption (Feistel cipher block), and uses similar algorithms for encryption and decryption, but the application of the sub keys is reserved [9].

4. TDES (3DES)

TDES or 3DES is the American National Standards Institute's (ANSI)-sanctioned encryption algorithm standard used by all debit-capable transaction terminals for PIN encryption. TDES (also known as Triple-DES) was developed to add more security protection in combating potential security breaches by being more secure than its predecessor, Data Encryption Standard (DES).

The 3DES was developed after it became clear that DES by itself was too easy to crack. It uses three 56-bit DES keys, giving a total key length of 168 bits. Encryption using 3DES is simply encryption using DES with the first 56-bit key, decryption using DES with the second 56-bit key, and encryption using DES with the third 56-bit key. Because 3DES applies the DES algorithm three times (hence the name), 3DES takes three times as long as standard DES [10].

Decryption using 3DES is the same as the encryption, except it is executed in reverse order. In other words, 3DES means you need to encrypt with key 1, decrypt with key 2, and again encrypt it with key 3. Fig. 2 below shows a general architecture of 3DES.

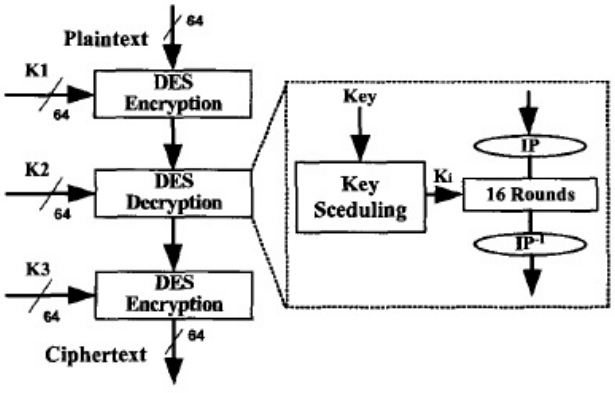

Figure 2: 3DES algorithm

5. Online Examination System (OES)

There are many application software or applications created for online examinations and in this section some of them are described.

TCExam [11], is open source software (free) which is simple and efficient, it is developed using popular LAMP platform (GNU-Linux, Appache server, MySQL, and PHP programming language). Any server that can run PHP can support this software.

SpeedExam [12] is not an open source but it is also not expensive. It is customized for schools, colleges, and universities. It was designed for practice and tests. Multiple-choice questions, multiple answers, true/false questions, and yes/no question are supported by this software. It can also import questions from Excel sheet. This software can be installed into mobile devices.

VirtualX [13] is an online examination system, which is open source; it is an effective system for saving the time, and also in getting fast result. It supports 12 different types of questions and 5 different types of reports for examinees with graphical analysis. It also supports a feedback management. It is useful for universities, schools, companies, and E-learning organizations.

Exambuilder [14] supports multiple-choice questions, true/false question, multiple correct answers, fill-in the blank and matching; the software will distribute the question randomly. This software supports gap analysis reports - "These reports grade the student on each question pool and provide remediation activities if the performance is below a threshold that you set".

The first version of Adit [15] was created in 2006 and the last one in 2012. And the requirements for this system are: any windows operating system except windows 95/98/ME, the processor is 1 GHz or higher, memory 512 or higher, and 80 MB of disk space. The last version is comprehensive, which means that it supports all kinds of examination questions. In addition, it supports four kinds of tests, which are assessment, survey, personality, and script.

Our system is created to increase the efficiency of OES by using a secure algorithm, which is XS-DES. Fig. 3 below shows the main interface of our system.

Figure 3: The main page of OES

Here, we will explain where we can apply our proposed method to make an OES more secure. When a student enters into an OES, there are two options; the first one is Login, which includes the Admin, Examiner and Student logins,

and each one has a specified level of authority to perform some tasks. Admin can add or delete students, he/she also can add or delete Examiner, and he/she can approve the exams. The Examiner can just evaluate the exam paper and send the result; he/she cannot see the students' name, because the system will generates fake name to the students'. The second option is Register, which is meant for new students (without an account).

Once a student logs into the system, he/she has three tasks that he/she can perform. He/she can first select the desired exam file, and secondly (second task), answer and submit the exam; after that he/she can request (third task) for the results. Whenever there is a request for exam results, the OES will send an email containing the decrypted results.

It should be noted that the student has to register first to allow him/her to take the exam, and during the registration process he/she must enter his/her name, filed, password, and email, when he/she login in the first time he/she will choose security question and answer it. If all fields were filled and the ID does not exist, then the student's information will be created and stored in the database to allow him/her take the exam later.

6. Extra Secure DES (XS-DES)

Researchers found that the only security problem in DES is its key, which is not very powerful and also too short, as stated by Deshmukh and Qureshi [16].

Thus, the 3DES becomes the choice to solve this problem of DES. 3DES uses three keys (K1, K2, K3) where each key consists of 56 bits. The plain text block is encrypted with the first key (K1), then decrypted with the second key (K2) and, finally, encrypted with the third key (K3). To decrypt the cipher text, the steps are reversed, that is decrypt with K3, encrypt with K2, decrypt with K1 and XOR the previous cipher text block.

DES is faster than 3DES but, 3DES is more secure than DES [17]. Our system needs an encryption algorithm, which is more secure than DES, but at the same time faster than 3DES. So, in order to accomplish this objective, we propose a new algorithm named XS-DES (Extra Secure-DES).

We propose to increase the size of the key from 64 bits to 128 bits, and split the key into two halves: left and right (Kl, Kr), and each one consists of 64 bits. Here, the proposed algorithm will decrease each key to 56 bits by applying the PC-1; after that it will divide each key into two parts (C0, D0). Then, (C1, D1) will be generated from (C0, D0) and the next (Ci, Di), i = 2, 3, ..., 16 will be obtained through similar step iteration. K1 will be produced by combining the left side from Kl (C0 from left key) and right side from Kr (D0 from right key). The last operation is to decrease the size of a key to 48 bits to encrypt the message. Fig. 4 shows our proposed method for the *key generation* in DES.

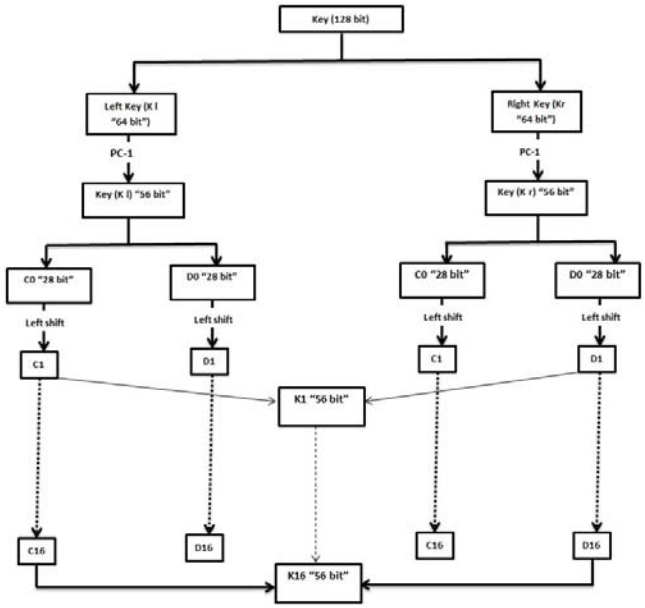

Figure 4: XS-DES

7. Comparison: DES and XS-DES

In this section we present a comparison between DES and our proposed algorithm, which is XS-DES. We perform this comparison to show that our proposed algorithm is more secure than DES, and at the same time faster than 3DES.

In terms of time, our method will be faster than 3DES, because 3DES will encrypt using key one, then decrypt using key two, and encrypt again using key three; this process will take more time. In XS-DES, it just encrypts using the same key, and there is no need to perform 3 processes. From the reduction of the number of steps, XS-DES will require less execution time (faster).

In terms of security level, we test these algorithms using an online tool, which is the website "howsecureismypassword.Net"; this website shows how many years attackers need to hack the encrypted password [18]. Many researchers like Judge Herbert [19] and Tony de Souza-Daw [20] also used this tool to test their passwords.

We choose five passwords and encrypt them through DES, and XS-DES. Then, we put the cipher text for each one in this tool. Table 4 and Table 5 below show these results.

Table 4: Results [18]

Plain text	Algorithm	Cipher text	Time To Hack
omarzug87!	DES	U2FsdGVkX18e9YPt/tWxfIkHSJwM5kP1Qjbbpk8jtfk=	It would take a desktop PC about A tresvigintillion years to crack this password
	XS-DES	U2FsdGVkX1+MTV3/DFb6z/Ynm9GVtfVtBnAD68Wxgvo=	It would take a desktop PC about *"121"* tresvigintillion years to crack this password
@OMARz87	DES	U2FsdGVkX1+97zSYAfnNYrhht4t9lkvvaKJsRL2tclU=	It would take a desktop PC about "61" unvigintillion years to crack this password
	XS-DES	U2FsdGVkX1+a7XZbFHWoqhwezWoW8A0t2x15Jpa7/Po=	It would take a desktop PC about "121" tresvigintillion years to crack this password
@zug12om$	DES	U2FsdGVkX19z/tFTuIn8+Y7aA/zLrwOlK+iPI9nK4dBa8li3ileIVg==	It would take a desktop PC about "773" trigintillion years to crack this password
	XS-DES	U2FsdGVkX18QgsWluh4YhIS06yj64d/rCE++VnKR/efA+CKLfS4Lpg==	It would take a desktop PC about "68" googol years to crack this password

Table 5: Results [18]

Plain text	Algorithm	Cipher text	Time To Hack
omar87__	DES	U2FsdGVkX1+MJ8GLaCotCF4cDCOhw7NtWwcWY0Rc6FI=	It would take a desktop PC about *"802"* vigintillion years to crack the password.
	XS-DES	U2FsdGVkX18M/LlHMwLv5R96YifxF8RIIIXFryjQV4c=	It would take a desktop PC about "13" duovigintillion years to crack This password.
_!omar87	DES	U2FsdGVkX19cEJW3G4mf46WctRFDUirEerd9eP6s+Yc=	It would take a desktop PC about *"4"* duovigintillion years to crack this password
	XS-DES	U2FsdGVkX19JgNWrofyN4ZqVB7Co3Z/lAbHXpQGY8eY=	It would take a desktop PC about *"121"*tresvigintillion years to crack this password

8. Conclusion and Future Work

Encryption algorithms are important for any database for encrypting confidential data, information, and more importantly, the passwords. Encryption algorithms are used to encrypt data and make it unreadable. This is done in order to prevent any attackers from seeing these confidential details.

In this paper, we propose a new method to encrypt the data and information, and the encryption algorithm is named XS-DES, which is originally based on DES. We increase the key size of the algorithm and add a new method in the key generation's step. After applying our method to a workable prototype and performing several preliminary testings, we achieved positive results, which proved that our method is more secure than DES algorithm.

A workable prototype of the Online Examination System (OES) that uses the proposed XS-DES algorithm has been developed. It has been tested to demonstrate if the introduced XS-DES algorithm has achieved its objectives, and the results are acceptable.

In the future, the XS-DES will be applied to other web-based applications related to education and other types of online business applications so that more people can benefit from the proposed encryption method.

Acknowledgment

This research was partially supported by the Ministry of Education (MOE) Malaysia under the Fundamental Research Grant Scheme (FRGS).

References

[1] D. Manivannan, R. Sujarani, "Light Weight and Secure Database Encryption Using TSFS Algorithm," School of Computing Pursuing M.Tech (CSE), School of Computing, SASTRA University, 2010.

[2] A.A. Zaidan, B.B. Zaidan, M. Anas, "High Securing Cover-File of Hidden Data Using Statistical Technique and AES Encryption Algorithm," World Academy of Science Engineering and Technology (WASET), Vol.(54), ISSN: 2070-3724, pp. 468-479, 2009.

[3] R. Raitman, L. Ngo, N. Augar, & W. Zhou, "Security in the Online E-learning Environment," Fifth IEEE International Conference on Advanced Learning Technologies, ICALT, pp. 702-706, 2005.

[4] J.O. Grabbe, "The DES Algorithm Illustrated," Laissez Faire City Times, 2(28), pp.12-15, 1992.

[5] R. Davis. "The Data Encryption Standard in Perspective," Communications Society Magazine, IEEE, 16(6), pp 5-9, 1987.

[6] C. Ding, "The Data Encryption Standard in Detail," Department of Computer Science, Hong Kong University of Science and Technology, China, 2000.

[7] H. S. Chang, "International Data Encryption Algorithm," jmu.edu, googleusercontent.com, Fall 2004. [Online]. Available: users.cs.jmu.edu, http://scholar.googleusercontent.com/scholar?q=cache:WXJPT0eEM7EJ:scholar.google.com/+International+Data+Encryption+Algorithm&hl=en&as_sdt=0,5. [Accessed: June 15 2013].

[8] O. Zughoul, H. Mat Jani, A. Shuib, O. Almasri. "Privacy and Security in Online Examination Systems," Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727 10(4), 2013.

[9] S. William, W Stallings, Cryptography and Network Security, Pearson Education, India, 2006.

[10] D. Patel, “Triple-DES ASIC Implementation for the Current Flattening Support Architecture,” In Masters Abstracts International, 45(03), 2006.
[11] A. Nicola, “In E-exam software,” tcexam.org, 2001-2012. [Online]. Available: http://www.tcexam.org. [Accessed: Mar. 26, 2013].
[12] "In Online Examination System,” speedexam.net, 2012. [Online]. Available: http://www.speedexam.net/online-exam-software.html. [Accessed: Mar. 26, 2013].
[13] "In Online Examination System," sourceforge.net, 2013. [Online]. Available: http://virtualx.sourceforge.net/virtualx.html. [Accessed: March. 27, 2013].
[14] "In Online Examination System," exambuilder.com, 2011. [Online]. Available: http://www.exambuilder.com/. [Accessed: March. 28, 2013].
[15] "In Online Examination System," aditsoftware.com, 2005-2012. [Online]. Available: http://www.aditsoftware.com/history/. [Accessed: March. 28, 2013].
[16] A.P. Deshmukh, R. Qureshi, “Transparent Data Encryption-Solution for Security of Database Contents,” The Smithsonian/NASA Astrophysics Data System, eprint arXiv: 1303.0418, 2013.
[17] C.M. Wee, P.R. Sutton & N.W. Bergmann, “An FPGA Network Architecture for Accelerating 3DES-CBC,” International Conference on Field Programmable Logic and Applications. pp. 654-657, 2005.
[18] H. Collidar, "HOW SECURE IS MY PASSWORD," howsecureismypassword.net, Version 4.0, 2009-2013. [Online]. Available: https://howsecureismypassword.net/. [Accessed: Aug. 15, 2013].
[19] J.H.B. Dixon Jr, “Cyber Security ... How Important Is It?” The Judges’ Journal, 51 (4), pp. 36-39, 2012.
[20] T. de Souza-Daw, O. Pui & N.H. Le, “Multimedia Curriculum for an Introductory Course for Information Technologist,” In Proceedings of the 9th International Conference on Advances in Mobile Computing and Multimedia, pp. 248-251, 2011.

Authors Profiles

Omar Zughoul received the B.S degree in Computer Information System from Yarmouk University in 2011, he stay in Malaysia to study Master of Information Technology.

Dr. Hajar Mat Jani is currently a Senior Lecturer at Universiti Tenaga Nasional (UNITEN), Malaysia. She received her Bachelor of Science (Computer Science) and Master of Science (Computer Science) degrees from The University of Georgia and Western Michigan University, U.S.A., respectively. She holds a Ph.D. degree in Software Engineering from University of Malaya, Malaysia.