Introducing an Encryption Algorithm based on IDEA

Osama Almasri[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: ***International Data Encryption Algorithm (IDEA) is one of the encryption algorithms that is widely used for security purpose. IDEA block cipher operates with 64-bit plain text block and 64-bit cipher text block, and a 128-bit key controls it. The fundamental design of the algorithm is using three different algebraic operations: bitwise Exclusive OR, multiplication modulo, and addition modulo. Having the largest number of weak keys is one of the drawbacks of IDEA. In addition, a new attack during round six of IDEA's operations has been detected. In this paper, we propose and describe the new design and preliminary implementation of a more secure encryption algorithm based on IDEA, and it is named DS-IDEA. Increasing the size of the key from 128 bits to 512 bits will increase the complexity of the algorithm. The algorithm's complexity is increased by increasing the amount of diffusion (multiplicative additive block) in a single round. It is implemented to provide better security to the user's password within the Online Password Management System (OPMS) in order to protect the user's data within the database from hackers and other forms of unauthorized access.***

Keywords: International Data Encryption Algorithm (IDEA), Double Secure-IDEA (DS-IDEA), Multiplicative Additive (MA), Online Password Management System (OPMS)

1. Introduction

Single key encryption or conventional encryption are terms that are often used to refer to symmetric encryption. It was the only type of encryption in use in the development of public-key encryption. It remains the most widely used of the two types of encryption: symmetric encryption and asymmetric encryption [1]. Symmetric encryption has five components as illustrated in Fig. 1:

- **Plain text:** This is the original message that is intelligible and is fed into the algorithm as input.
- **Encryption algorithm:** It performs various operations and transformations on the original message (plain text).
- **Secret key:** It is shared between the sender and the recipient, and is used as an input to the algorithm.
- **Cipher text:** It is the algorithm's output. It is scrambled message and unintelligible that depends on the plain text and encryption key.
- **Decryption algorithm:** The reverse operation is applied on the cipher text to get the plain text (original).

The International Data Encryption Algorithm (IDEA) is one of the symmetric encryption algorithms that can be implemented in e-learning systems [2]. It is a post Data Encryption Algorithm (DES) that has better security and covers some of the DES problems. It is characterized by high-speed encryption/decryption process, with resisting and correlation analysis [3]. Because of the weaknesses in the algorithm's keys, and the attack in round six of its operations, the necessity to increase the algorithm's security has become paramount [4].

The proposed scheme of algorithm is named Double Secure-IDEA or DS-IDEA. It is a modified version of IDEA; a modification is done by increasing the key size and the amount of the diffusion process (MA blocks). Any organization over the world must protect their user's data by the fulfillment of three major factors: confidentiality, integrity, and availability (CIA). Password confidentiality is more challenging, and this involves a number of security controls along with decisions involving the characteristics of the passwords themselves. Those CIA factors are applied by implementing the proposed algorithm within a workable prototype named Online Registration System, in which the component of the proposed Online Password Management System (OPMS) is embedded.

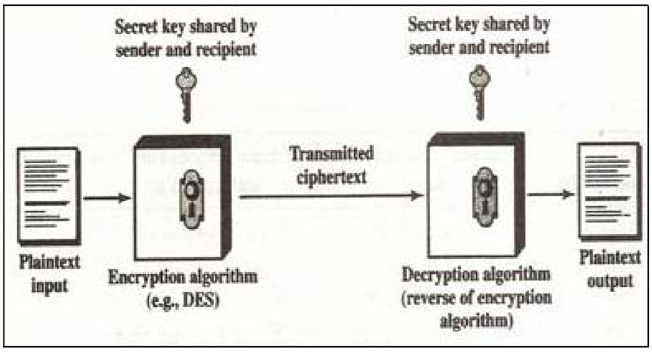
Secret key shared by sender and recipient
Secret key shared by sender and recipient
Transmitted ciphertext
Plaintext input
Encryption algorithm (e.g., DES)
Decryption algorithm (reverse of encryption algorithm)
Plaintext output

Figure 1: General model of symmetric encryption [1]

2. Background and Related Work

2.1 Brief description of IDEA algorithm

IDEA is a symmetric block cipher that was published in 1991 by Lai, Massey, and Murphy [5]. IDEA is a modification of Proposed Encryption Standard (PES) that was published by Lai and Massey in 1990 [6]. PES is a replacement of DES, and IDEA was originally named Improved Proposed Encryption Standard (IPES), but was later changed to IDEA in 1992 [7].

The block cipher IDEA encrypts a 64-bit block of plain text and a 64-bit of cipher text, and a 128-bit key controls it. The algorithm (refer to Fig. 2) consists of eight identical rounds plus a half round for output transformation. The fundamental design in IDEA is the use of the mixing of three incompatible algebraic groups: bit-by-bit XOR, addition modulo 216, and multiplication modulo 216+1. There are 216 possible 16-bit blocks: 0000000000000000… 1111111111111111. Schneier [8] breaks the algorithm into fourteen steps for each eight complete rounds. The plain text is a fixed size (64-bit block) that is divided into four 16-bit blocks (X1|| X2|| X3|| X4). The key is a 128-bit block. It is divided into eight 16-bit sub keys. The division into 16 bits is because all of the algebraic operations used in the encryption and decryption process operate at 16-bit numbers. The last output round is four 16-bit sub keys. Each round uses six 16-bit sub keys and the remaining two sub keys are used in the next round by implementing left shifting by 25 positions. The total sub keys is 52 {52=8 rounds*6 sub keys + (4 sub keys "output transformation")} [3]. The encryption and decryption of sub keys are shown in Table 1.

Table 1: Encryption and decryption of the sub keys [3]

Round No.	*Sub keys of Encryption*	*Sub keys of Decryption*
1	$Z_1^{(1)}$ $Z_2^{(1)}$ $Z_3^{(1)}$ $Z_4^{(1)}$ $Z_5^{(1)}$ $Z_6^{(1)}$	$Z_1^{(9)-1}$ $-Z_2^{(9)}$ $-Z_3^{(9)}$ $Z_4^{(9)-1}$ $Z_5^{(8)}$ $Z_6^{(8)}$
2	$Z_1^{(2)}$ $Z_2^{(2)}$ $Z_3^{(2)}$ $Z_4^{(2)}$ $Z_5^{(2)}$ $Z_6^{(2)}$	$Z_1^{(8)-1}$ $-Z_2^{(8)}$ $-Z_3^{(8)}$ $Z_4^{(8)-1}$ $Z_5^{(7)}$ $Z_6^{(7)}$
3	$Z_1^{(3)}$ $Z_2^{(3)}$ $Z_3^{(3)}$ $Z_4^{(3)}$ $Z_5^{(3)}$ $Z_6^{(3)}$	$Z_1^{(7)-1}$ $-Z_2^{(7)}$ $-Z_3^{(7)}$ $Z_4^{(7)-1}$ $Z_5^{(6)}$ $Z_6^{(6)}$
4	$Z_1^{(4)}$ $Z_2^{(4)}$ $Z_3^{(4)}$ $Z_4^{(4)}$ $Z_5^{(4)}$ $Z_6^{(4)}$	$Z_1^{(6)-1}$ $-Z_2^{(6)}$ $-Z_3^{(6)}$ $Z_4^{(6)-1}$ $Z_5^{(5)}$ $Z_6^{(5)}$
5	$Z_1^{(5)}$ $Z_2^{(5)}$ $Z_3^{(5)}$ $Z_4^{(5)}$ $Z_5^{(5)}$ $Z_6^{(5)}$	$Z_1^{(5)-1}$ $-Z_2^{(5)}$ $-Z_3^{(5)}$ $Z_4^{(5)-1}$ $Z_5^{(4)}$ $Z_6^{(4)}$
6	$Z_1^{(6)}$ $Z_2^{(6)}$ $Z_3^{(6)}$ $Z_4^{(6)}$ $Z_5^{(6)}$ $Z_6^{(6)}$	$Z_1^{(4)-1}$ $-Z_2^{(4)}$ $-Z_3^{(4)}$ $Z_4^{(4)-1}$ $Z_5^{(3)}$ $Z_6^{(3)}$
7	$Z_1^{(7)}$ $Z_2^{(7)}$ $Z_3^{(7)}$ $Z_4^{(7)}$ $Z_5^{(7)}$ $Z_6^{(7)}$	$Z_1^{(3)-1}$ $-Z_2^{(3)}$ $-Z_3^{(3)}$ $Z_4^{(3)-1}$ $Z_5^{(2)}$ $Z_6^{(2)}$
8	$Z_1^{(8)}$ $Z_2^{(8)}$ $Z_3^{(8)}$ $Z_4^{(8)}$ $Z_5^{(8)}$ $Z_6^{(8)}$	$Z_1^{(2)-1}$ $-Z_2^{(2)}$ $-Z_3^{(2)}$ $Z_4^{(2)-1}$ $Z_5^{(1)}$ $Z_6^{(1)}$
Output transfor-mation	$Z_1^{(9)}$ $Z_2^{(9)}$ $Z_3^{(9)}$ $Z_4^{(9)}$	$Z_1^{(1)-1}$ $-Z_2^{(1)}$ $-Z_3^{(1)}$ $Z_4^{(1)-1}$

The following steps are the encryption process in each round [3]:

1. First multiplication between X_1 and the first sub key Z_1.
2. Addition operation of X_2 with the second sub key Z_2.
3. Addition operation between X_3 and the third sub-key Z_3.
4. Second multiplication between X_4 and the fourth sub-key Z_4.
5. Calculating Bitwise XOR from the results of steps 1 and 3.
6. Calculating Bitwise XOR from the results of steps 2 and 4.

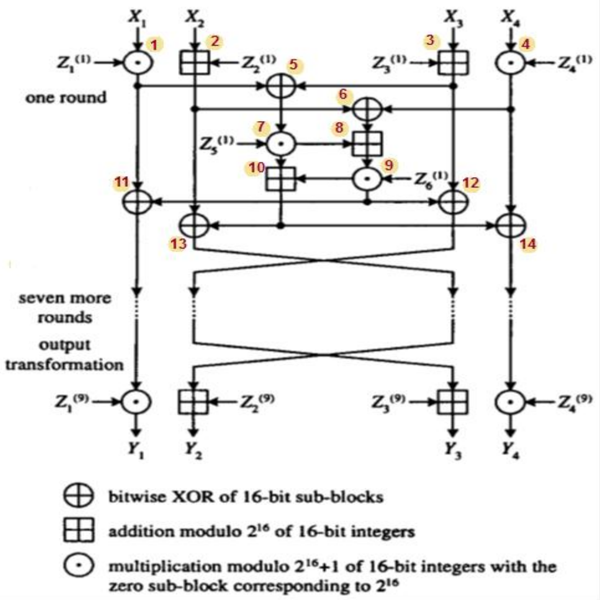

Figure 2: Structure of IDEA encryption process [3]

The decryption process is an essential process that is applied on cipher text to transform it into the original message (plain text). The computational process for the decryption is the same as that used for the encryption of the plain text. The difference compared to the encryption is that the 16-bit sub keys are generated in reverse order.

The IDEA encryption algorithm has some features which claim for use [9]:

- High level security not keeping the algorithm a secret, but rather upon ignorance of the secret key.
- Easily understood.
- Available online.
- Widely used range of application and efficiently such as distance learning.

2.2 A proposed encryption algorithm based on IDEA

The drawback of IDEA is that large numbers of weak keys were found in the algorithm. In addition, the attack that has been detected in round 6 is also one of the algorithm's drawbacks [10], [11]. This paper discusses the improvement that is made to the IDEA algorithm to make it more secure. Increasing the key size from 128 bits to 512 bits is a main factor in algorithmic complexity. Also, increasing the IDEA's strength can be made by exploiting the operations of confusion and diffusion. The modified design is named Double Secure-International Data Encryption Algorithm (DS-IDEA). The block size of the sub keys in the modified version will be increased due to the key size. So, to ensure decreasing the number of sub key blocks, this will increase the sub key block size to become more than 16-bit. The block size should be 16-bit because of the algebraic operations that operate on 16-bit numbers. The other modification in the design is using S-Box to decrease the number of bits from 32 bits to 16 bits of each sub key block.

The encryption process consists of eight identical steps (named encryption rounds) and followed by last round called output transformation. The key size is 512 bits, and the plain text size is 128 bits. The plain text is processed in 8 blocks of 16 bits each. DS-IDEA (proposed method) can be processed as two sub blocks of 64 bits. Two sub blocks are running in parallel with each other. Each round uses two MA blocks and 12 sub keys of 32 bits each. In IDEA 128-bit key is divided into 8 sub keys of 16 bits each; each round uses 6 sub keys and the remaining two sub keys are used in the next round after applying left shifting by 25 positions. In the proposed design 512-bit key is divided into 16 sub keys of 32-bit each. Each round uses 12 sub keys of 32-bit each; the remaining four sub keys are used in the next round. S-box should implement on the 16 sub keys to transform 32-bit to 16-bit of each sub key, then 12 sub keys are processed by applying the addition and multiplication modulo.

In the first round, the first four 16-bit sub key is combined with two of 16-bit plain text blocks using addition modulo 2^{16}, and with another two 16-bit plain text blocks using multiplication modulo $2^{16}+1$. The results are then processed, whereby two more 16-bit sub keys are included in the calculation and the third algebraic group operator, the bitwise XOR, is used. Each round consists of two further divisions i.e. transformation, followed by sub encryption. Transformation uses 8 sub key, whereas sub encryption uses 4 sub keys. The process of the first round of encryption is illustrated in Fig. 3. The last round of output transformation uses 8 sub keys, whereas the total keys will be 104 sub keys of 16 bits each that gives the cipher text. The decryption process is almost the same as the encryption process, but in a reverse sequence. Fig. 3 describes the structural design of the encryption round of DS-IDEA. From Fig. 3 the following relations can be written:

- $W_{11} = I_{11} \oplus MA_{R1} (I_{11} \oplus I_{13} , I_{12} \oplus I_{14})$
- $W_{12} = I_{13} \oplus MA_{R1} (I_{11} \oplus I_{13} , I_{12} \oplus I_{14})$
- $W_{13} = I_{12} \oplus MA_{L1} (I_{11} \oplus I_{13} , I_{12} \oplus I_{14})$
- $W_{14} = I_{14} \oplus MA_{L1} (I_{11} \oplus I_{13} , I_{12} \oplus I_{14})$
- $W_{15} = I_{15} \oplus MA_{R2} (I_{15} \oplus I_{17} , I_{16} \oplus I_{18})$
- $W_{16} = I_{17} \oplus MA_{R2} (I_{15} \oplus I_{17} , I_{16} \oplus I_{18})$
- $W_{17} = I_{16} \oplus MA_{L2} (I_{15} \oplus I_{17} , I_{16} \oplus I_{18})$
- $W_{18} = I_{18} \oplus MA_{L2} (I_{15} \oplus I_{17} , I_{16} \oplus I_{18})$

"W_{11}" denotes the word that is 16-bit, and the first index on the left means the first word. The right index refers to the round number. *"I"* refers to the input (plain text) that is 16-bit block. The processes of round one that described above are repeated in each of the subsequent seven encryption rounds using 16-bit sub keys for each combination.

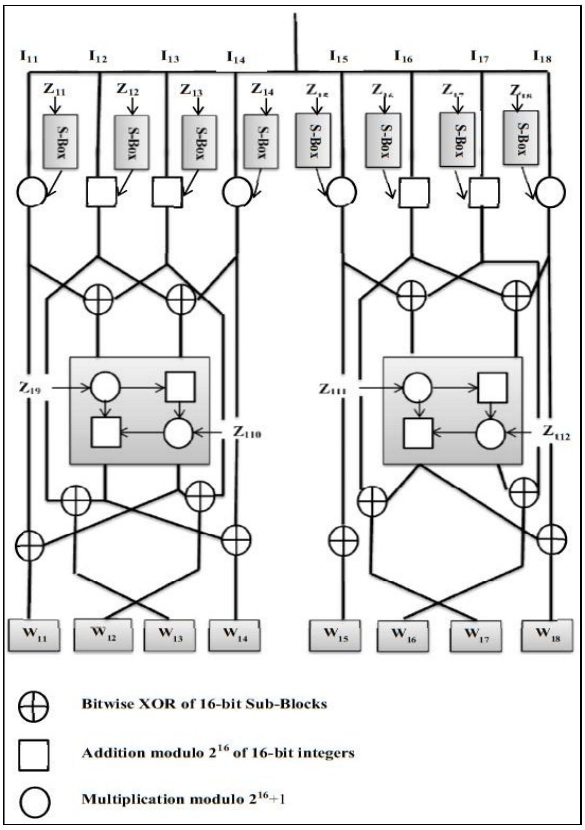

Figure 3: Structural design of first encryption round of DS-IDEA

3. Research Methodology for Implementing the Proposed Algorithm

Fig. 4 depicts the research methodology in the implementation of DS-IDEA within the prototype.

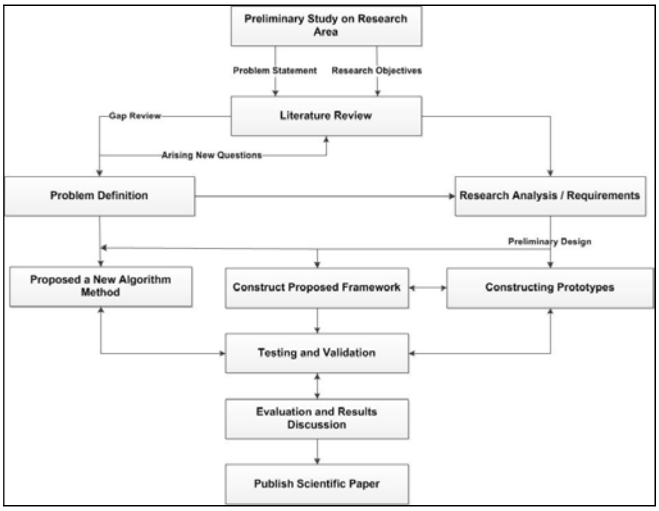

Figure 4: Research methodology

3.1 Implementing DS-IDEA within OPMS

The online system is a platform that provides data and information online with the objective of improving the user's experience. Nowadays, the most appropriate way to disseminate and present information to a large group of people in the world is using websites. The goal of the website design is to provide plenty information to visitors or users in an organized manner. In addition, there must be a reliable transfer of secure information. There are other factors such as simplicity, user friendliness, layout, ease of rendering in the browser and so on that are closely related with the quality of the website.

Organizations must protect the password by three major factors, which are confidentiality, integrity, and availability, so that all authorized users can use passwords successfully as needed. Reducing the risk of compromise of password-based authentication systems are an effective password management.

Password confidentiality is more challenging and involves a number of security controls along with decisions involving the characteristics of the passwords themselves. Ensuring integrity and availability using typical data security controls, such as imposing privileges and access controls to prevent attackers from overwriting the password are in place.

The objective of the research is to implement the proposed encryption method in providing better security to users' passwords within the Online Password Management System (OPMS) in order to protect the user's data within the database from hackers or attackers.

The protection process is done by implementing a symmetric encryption algorithm named International Data Encryption Algorithm (IDEA) on the passwords. The algorithm will be improved by modifying the size of the secret key that is used in both the encryption and decryption operations on the data. The proposed algorithm is known as Double-Secure IDEA (DS-IDEA).

The research elaborates on a number of issues that are related to web design and development, and it focuses on the security measures that are applied within OPMS. These concepts will be illustrated and demonstrated in the design of system that we have designed so far. Testing results from implementing the proposed method of the encryption algorithm on system password fields for evaluating the security strength is the one of the primary aims of this research. The system can be considered as a working prototype. It deals with the maintenance of university, staff, and students' information through the Online Registration website. This system involves the automation of registration process that is used by the administrators and students. Fig. 5 shows a simplified structure of the OPMS, which implements the proposed algorithm, DS-IDEA.

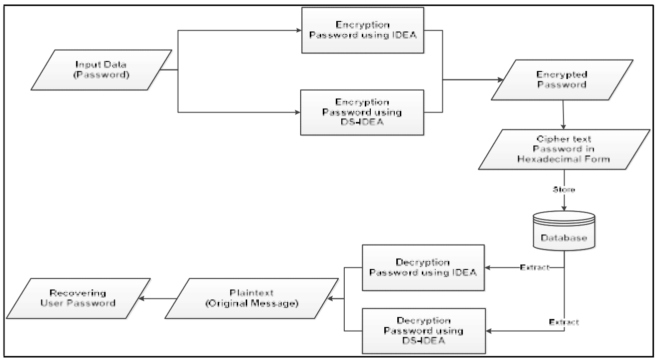

Figure 5: A simplified structure of Online Password Management System (OPMS) [3]

Fig. 6 shows a prototype of an online course registration using OPMS [3]

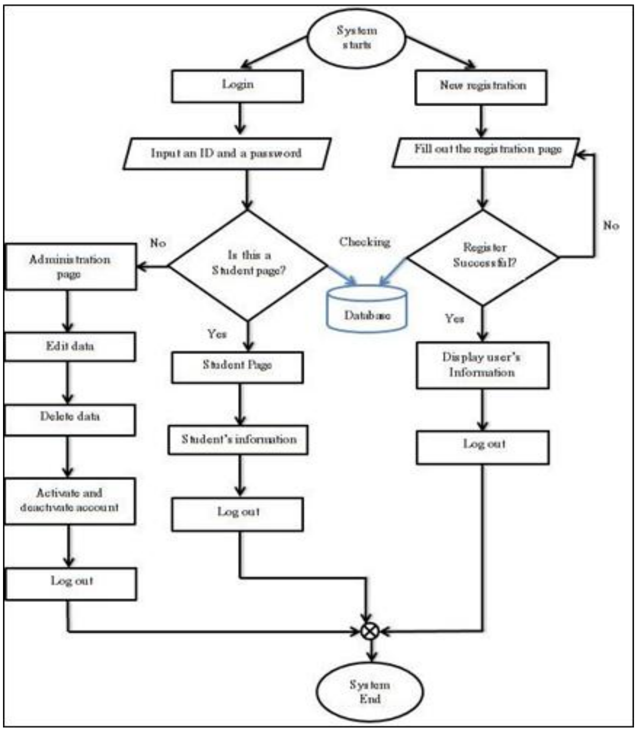

Figure 6: A simplified course registration prototype [3]

Fig. 7 illustrates a diagram representing OPMS within a workable online registration prototype.

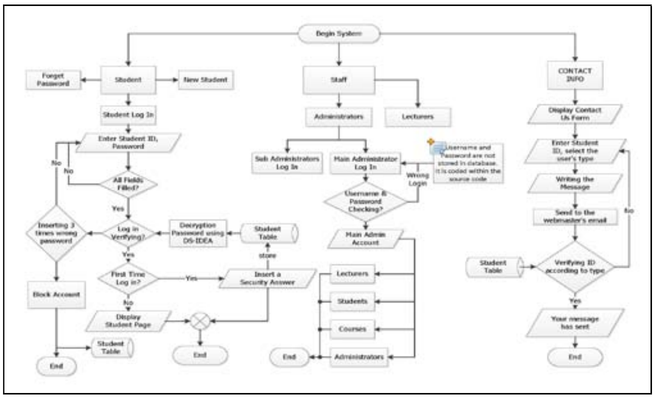

Figure 7: The framework of the online registration system using OPMS and DS-IDEA

Fig. 8 shows the home page interface of the system coded with Active Server Page (ASP).

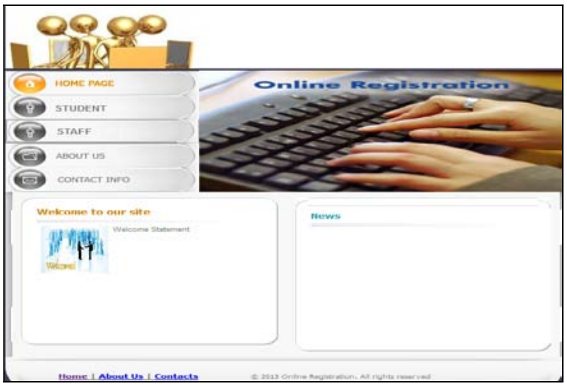

Figure 8: The home page of online registration prototype

3.2 Preliminary experimental results

In this section, we discuss the results that we obtained from implementing the standard algorithm (IDEA) and the proposed modified algorithm, DS-IDEA. We implement both algorithms on the password field in the prototype to compare the results. The password is stored in the database–in encrypted form under two fields; one uses the IDEA algorithm and the other uses DS-IDEA.

The aim of the comparison is to get results to demonstrate that the modified algorithm is stronger and more secure than the original IDEA algorithm. The comparison is conducted only on the cipher text using an online tool named *"HOW SECURE IS MY PASSWORD?"*[12]. This site can accept any password to be analyzed, and an estimation of how long it would take for a personal computer to crack each one of them is produced.

Judge Herbert B. Dixon Jr [13], Tony de Souza-Daw [14], and Scott Granneman [15] have recommended using this site to test the passwords' security and strength. Table 2 demonstrates using 5 different passwords as plain text and cipher text, and shows the time the cracker needs in order to breach the password through the implementation of IDEA [12]. Table 3 shows the same five passwords encrypted using DS-IDEA [12]. Each password is comprised of at least 8 characters containing at least one digit and one special character.

Table 2: Five different passwords encrypted using IDEA [12]

Plain text	*Cipher text*	*Time to Crack*
ghaleb2!	U2FsdGVkX1/EpfScwgj8QDP2D+PBukwVoA==	It would take a desktop PC about 174 *septendecillion* years to crack the password
osama87#	U2FsdGVkX19YI5tvCW7LY6rOKHpbACQJ	18 *duodecillion* years
leb28-*&	U2FsdGVkX1917Hl3Bv5Z/vh3HVzSLu99aQ==	16 *sexdecillion* years
_!omar873	U2FsdGVkX1/614cyIQa2fsT1orHLTN7Bzw==	16 *septendecillion* years
2131987hey&	U2FsdGVkX1/eLhpdVNxR1EnnNsGur3+GWA==	174 *sexdecillion* years

Table 3: Same passwords encrypted using DS-IDEA [12]

Plain text	*Cipher text*	*Time to Crack*
ghaleb2!	U2FsdGVkX1/ldmZTWQfHYZluqeIwoa7Lzw==	It would take a desktop PC about 16 *octodecillion* years to crack your password
osama87#	U2FsdGVkX18EVJrd6SlhER12F4gQoqZR	18 *duodecillion* years
leb28-*&	U2FsdGVkX18KuJOm8QgiC4Wl6UEmY6ZL8A==	50 *octodecillion* years
_!omar873	U2FsdGVkX1+8GH12vHmveKeg5LF1mmgVIQ==	296 *octodecillion* years
2131987hey&	U2FsdGVkX19Wdxfm6OnJiM7kLxM3cUXMzQ==	50 *septendecillion* years

From Table 2 and Table 3, we discovered that the time to crack each password requires many more years. The site uses terms to express the number 10 raised to the power of 54, as in the word *"septendecillion"*. *"duodecillion"* means 10^{39}, *"octodecillion"* is 10^{57}, and *"sexdecillion"* means 10^{51}. By the comparison between values of years, we proved that the proposed algorithm (DS-IDEA) is more secure than IDEA.

4. Conclusion and Future Work

The proposed algorithm, DS-IDEA, has two features: increasing the key size (512 bits) that leads to increasing the degree of *diffusion*, and using the S-Box to reduce the key block size from 32 bits to 16 bits. The total number of sub keys becomes 104 compared to 52 sub keys with the original IDEA to enhance the complexity of *confusion*. This will also reduce the probability of attacks. Furthermore, using two multiplicative additive blocks enhances the *diffusion*. This contributes in making the algorithm to become more secure and less susceptible to cryptanalysis. The development of the Online Password Management System (OPMS) that implements the DS-IDEA algorithm has started and is progressing well. It has gone through some initial testing's and evaluations with very encouraging results, and we are in the process of improving the algorithm's performance.

In the future, the DS-IDEA is going to be enhanced by including more security operations that can strengthen the confidentiality, integrity and availability of data that are encrypted using this algorithm. We also plan to apply this modified version of IDEA to other web-based systems in e-business, e-commerce, and e-learning environments with slightly different methods of implementation.

Acknowledgment

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

References

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

[2] 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: Feb. 15 2013]

[3] O. Almasri, H. Mat Jani, Z. Ibrahim, O. Zughoul, "Improving Security Measures of E-Learning Database," International Organization of Scientific Research-Journal of Computer Engineering (IOSR-JCE), 10 (4), pp. 55-62, 2013

[4] A. Biryukov, J. Nakahara Jr, B. Preneel, J. Vandewalle, "New Weak-Key Classes of IDEA," In Proceedings of the International Conference on Information and Communications Security (ICICS), pp. 315-326, 2002.

[5] Mediacrypt AG, "The IDEA Block Cipher," cryptonessie.org, 2000. [Online] Available: http://cryptonessie.org [Accessed: Aug. 2, 2013]

[6] X. Lai, J.L. Massey, "A Proposal for a New Block Encryption Standard," Advances in Cryptology -

EUROCRYPT ’90, Lecture Notes in Computer Science, Springer-Verlag, pp. 389-404, 1991.

[7] N. Hoffman, “A Simplified IDEA Algorithm,” Cryptologia, 31 (2), 2007

[8] B. Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C, John Wiley & Sons, India, 2007.

[9] R. Zimmermann, A. Curiger, H. Bonnenberg, H. Kaeslin, N. Felber, W. Fichtner, “A 177 Mb/s VLSI Implementation of the International Data Encryption Algorithm,” IEEE Journal on Solid-State Circuits, pp. 303-307, 1994.

[10] H.P. Singh, S. Verma, S. Mishra, “Secure-International Data Encryption Algorithm,” International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, 2 (2), pp. 780-792, 2013

[11] X. Lai, J. Massy, S. Murphy, “Markov Ciphers and Differential Cryptanalysis,” In Proceedings of the Workshop on the Theory and Application of Cryptographic Techniques Brighton, pp. 17-38, 1991

[12] H. Collidar, "HOW SECURE IS MY PASSWORD," howsecureismypassword.net, Version 4.0, 2009-2013. [Online]. Available: https://howsecureismypassword.net/. [Accessed: Aug. 2, 2013].

[13] J.H.B. Dixon Jr, “Cybersecurity ... How Important Is It?,” The Judges’ Journal, 51 (4), pp. 36-39, 2012.

[14] 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 (MoMM ‘11), pp. 248-251, 2011.

[15] S. Granneman, “Securing Your Mac & Networks,” In Mac OS X Snow Leopard for Power Users, Scott Granneman (eds.), Apress, pp. 237-266, 2010.

Author Profile

Osama Almasri received the B.Sc. degree in Computer Systems Engineering from Mamoun Private University of Science and Technology in 2009. During 2011-2013, he is studying Master of Information Technology (Coursework and Research) at Universiti Tenaga Nasional.

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.