A Security System Using Seal, Blowfish and Idea Algorithm for Credit Card Data

Soleman[(1)]
Faculty of Computer Science, Information Systems
Borobudur University
Jakarta, Indonesia
solemediagrafik@gmail.com

Azlan Irwan[(2)]
Department of Computer Science, Faculty of Information Technology
Budi Luhur University
Jakarta, Indonesia
azlanirwan9@gmail.com

DOI: 10.31364/SCIRJ/v8.i12.2020.P1220830
http://dx.doi.org/10.31364/SCIRJ/v8.i12.2020.P1220830

***Abstract*— Document privacy is very important with communication technology in an innovative era of globalization. However, when the document changes hands or the document is sent, there is still a risk of data damage and the document can be changed by an unrelated party so that document security is necessary. If the confidentiality and authenticity of documents are damaged by irresponsible parties, the information is no longer useful. For this reason, a text encryption application was created using the SEAL, Blowfish and IDEA algorithms. A combination of these three algorithms will create better algorithm security for the company. The IDEA algorithm is a symmetric cryptography with high security which is not based on the confidentiality of the algorithm but emphasizes the security or confidentiality of the key used. The goal is to produce stronger and more secure data security, a combination of the SEAL algorithm for data encryption and the IDEA algorithm is used to maintain data confidentiality and security by going through the description process, as well as the Blowfish algorithm to maintain the confidentiality of user login data, so that only the person concerned can read the information. The important files that the researcher will secure are Emboss files in the form of credit card data and customer data with a Microsoft Office extension (.doc, .docx, xlx, .xlsx) and with text extension. The results of testing the SEAL, Blowfish and IDEA Algorithms are the time obtained to encode and decode is directly proportional to the size of the file being processed (the smaller the file size is processed, the faster the encode and decode process, the larger the file size, the longer it takes. encode and decode process).**

***Keywords*—** cryptography, idea, blowfish, seal, microsoft

I. Introduction

Data security is a crucial aspect in information and communication systems involving computers. Data security is necessary so that information that should be addressed to certain people does not leak to other parties. Therefore, we need a security system that can prevent leakage, misuse of the data and produce stronger and more secure data security. Like the case study of leaks in Indonesia (Cyber-crime-indonesia, 2016) there are 36.6 million incidents of cyber attacks. Indonesia is considered the country most at risk of experiencing IT Security attacks with a percentage of 23.54%. Threat Exposure Rate (TER), measured from the percentage of PCs affected by malware attacks, whether successful or failed [4]. Not only that it happened based on data (itgid.org, 2017) theft and breach (data breach) of 250 thousand Twitter user data (email and password), 6 million personal user data Facebook users were exposed because of a bug in the system. More than 50 million e-mails and passwords of users of Livingsocial, an e-commerce site have been stolen. Evernote reset about 50 million user accounts after the data theft occurred [8]. CNN Indonesia (CnnIndonesia., 2016) reported that cyber crime cases were mostly handled by Ditreskrimsus Polda Metro Jaya throughout 2016. Of the 1,627 cases handled by the police, 1,207 cases were cyber crime cases. Of the 1,207 case reports, a maximum of 699 cases have been resolved [3]. A new case study in Indonesia (Cnnindonesia., 2020) data leakage at the Unicorn Tokopedia company experienced a leak of 91 million data from e-commerce service users. This means that they have taken the data of all Tokopedia users. Successfully obtained data such as user names, email addresses and other transaction identities [2]. Data security at BNI, to be precise, in the Credit Card division, has been very vulnerable to misuse of data, data security is only done simply and does not pay much attention to the level of security. The source of sending data to the destination is only via email and the LAN network so that it is possible for irresponsible parties to collect data. This can result in data fraud, which can harm BNI and customers. The current system at BNI allow users who want to send data in the form of Excel or Documents to other users through a network share folder without any password or security so that the data can be very easily accessed by people and can be misused. Based on these problems, a security and authenticity of text data will be applied. To maintain the security and confidentiality of messages, data, or information in a computer network, some encryption is needed to create messages, data or information so that data leakage does not occur. This system uses cryptography in the encryption process using the SEAL algorithm and decryption to maintain the security and authenticity of documents using the IDEA algorithm and user

http://dx.doi.org/10.31364/SCIRJ/v8.i12.2020.P1220830

login using the Blowfish algorithm application method. According to (Yani Parti Astuti, 2016) these algorithm is neatly arranged, can be carried out easily, is simple, and is guaranteed safety. Until now, no cryptanalyst has managed to break through the security created by the Blowfish algorithm with 16 turns [14]. According to research conducted by (Kholidya Yuli Wardani, 2017), "IDEA has a strong and secure encryption function. However, the simplicity of IDEA's key schedule resulted in IDEA having a weak key. The encryption process in IDEA uses a mixture of operations from three algebraic groups. It is this mixture of three operations that ensures IDEA's safety [9].

II. Material And Methods

A. *Analysis Technique*

The experimental method is a combination of the SEAL Algorithm that will be used for encrypting uploaded data and the IDEA algorithm for decrypting the encrypted data, in this case the allocation of Emboss data at BNI Bank. Experimental experiments were carried out on customer data and credit card data. In each experiment using the same data. As for some of the experiments carried out in this study, namely:

- *Data collection:* at this stage data is collected from BNI Bank. The data obtained are some examples of Emboss data, namely customer data extending doc, and excel, *while customer credit card data in .txt extension.*
- *Process SEAL Algorithm:* implemented as data encryption and IDEA algorithm for decryption, while the Blowfish algorithm is used for user data security on the data to be tested.\
- *Data analysis:* discusses whether embossed data encryption can facilitate user performance based on the method applied.

B. *Design, Data Analysis and Testing Techniques*

The planning technique used is face-to-face planning of system applications. This includes home page planning, encryption process planning, description process planning and system application login planning. The process of data encryption itself uses the SEAL algorithm and for the description process uses the IDEA algorithm. As for the Blowfish algorithm is used for application login data security.

C. *Blowfish Algorithm Encyption*

- *Blowfish*

Is an algorithm consisting of 16 rounds. The key that is entered consists of 64bit. This key will be divided into 32bit of left block and 32bit of right block. For each spin, the 32bit of left block key will be XORed with the first element of the P-array (P1 through P18). The result is P', and will be subjected to an F function which will then be XORed with a 32-bit right block key, called F. After that, the 32-bit left block that has been XORed with P'is exchanged with the 32-bit of right block that has been XORed with P' which has been subjected to the F (F') function, this process will be carried out until the P-16 array. P16' will be XORed with P17 while P16' will be XORed with P18, then the results will be recombined to produce 64 bit of ciphertext.

The following is a flow chart of the Blowfish algorithm which is shown in Figure 1. below:

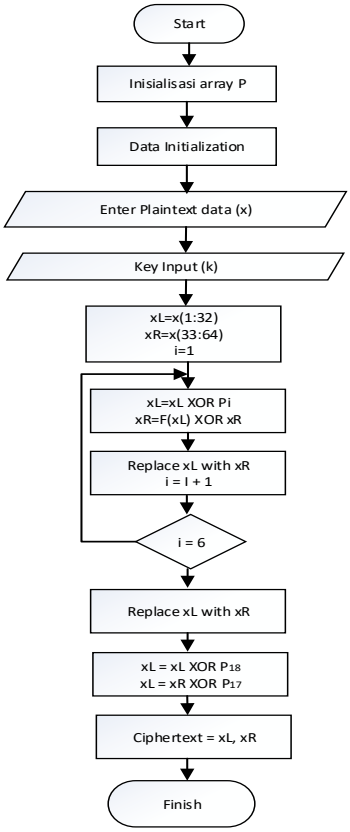

Figure 1. Blowfish Encryption Flow Chart

- *F Function*

Blowfish uses the F function, which is a function applied when calculating the XR value. In function F there are 4 S- boxes where each S-boxes has 256 inputs measuring 32 bits. How to calculate the function F using equations F (XL) = ((S1, a + S2, b mod 232) XOR S3, c) + S4, d mod 232 The values of a, b, c and d are obtained from XL where XL measuring 32bit is broken down into 8 bits. The flow diagram for function F is illustrated in Figure 2. below:

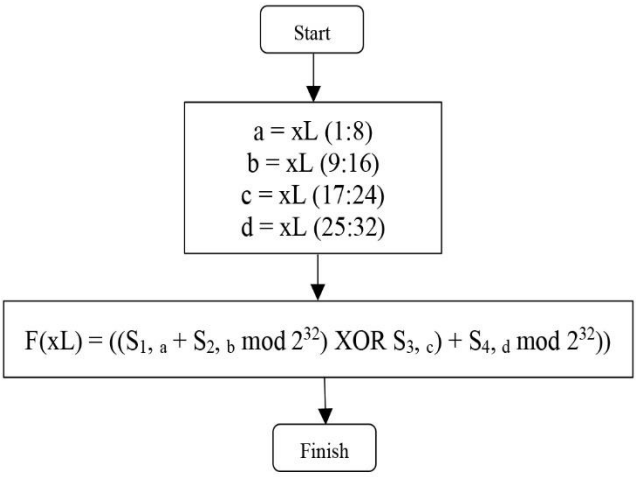

Figure 2. Flow Diagram of F Function

- *Key Variables*

http://dx.doi.org/10.31364/SCIRJ/v8.i12.2020.P1220830

Blowfish uses a key of type string up to 56 characters long which is stored in a key variable (K). The key variables are distributed into an array from K1 to K14. Each of these K is 32 bits of data. This key variable will then be used during the P-array initialization.

- *P-array Initialization*

The Blowfish algorithm uses P-array constants and S-boxes. The P-array constant is 18, each of which has 32 bits. Then there are 4 constant S-boxes consisting of 256 entries where each input is 32 bits in size. This P-array constant is used to strengthen the security of the data by means of XOR operations with keys.The p-array is initialized by means of 18 constants. The P-array is subject to XOR operation with 14 divided keys each.32 bit size. The XOR process will be carried out on the first 14 P-arrays with 14 keys. Starting from P1 is XORed with K1 and so on until P14 is XORed with K14 like the following algorithm:

$$P1 = P1 \text{ XOR } K1$$
$$P2 = P2 \text{ XOR } K2$$
$$P14 = P14 \text{ XOR } K14 \quad (1)$$

The next process is, the P-array from P15 is subject to XOR operation with K1 returning. This process can be seen in the algorithm below.

$$P15 = P15 \text{ XOR } K1$$
$$P18 = P18 \text{ XOR } K4 \quad (2)$$

- *Data Initialization*

At this stage, the P-array that has been operated with a key will be subject to operation with a data that is divided into two parts, namely XL and XR, each of which is zero so that a new P-array is obtained. Then the values of P1 and P2 are replaced by the values of P17 and P18 from the results of this XOR operation. This process will continue until all inputs from the P-array and all inputs from the four S-boxes fulfilled. This is done so that the output of the blowfish algorithm continues to change.

- *Encryption Cycle*

In Blowfish encryption, the data that has been entered, in this case is the data in a file, will be divided into blocks of 64 bits each. Furthermore, the block is divided into XL and XR. XL and XR will be processed where XL is XORed with P1 to produce XL1 and XR is XORed with XL1 which has been subjected to the F function and produces XR1. This step was carried out until the 16th XL and XR. Furthermore, the XL16 was XORed with the P18 and the XR16 was XORed with the P17.

for i = 1 to 16 do
XL[i] = XL[i] XOR P[i]
XR[i] = F(XL[i]) XOR XR[i]
XL[16} = XL[16] XOR P[18]
XR[16] = XR[16] XOR P[17] (3)

- *IDEA Algorithm*

This IDEA algorithm process has 8 iterations (rounds) plus one output transformation loop. For more details on how the IDEA encryption algorithm works, see the following example: Suppose we are going to encrypt a message, where the message is plaintext and key.

Key: KRIPTOGRAFI IDEA
Plaintext: ABDHANAN

The following is a display of the encryption flowchart of the IDEA algorithm. The following shows some examples of encryption generated using this application program in IDEA Encryption Theory.

Table 1. Examples Of Encryption.

No	Plain Text	Keywords	Ciphertext
1.	ubudiyah	students	ä Ï
2.	collegeIT	programmerdrsabang	4÷ýÈ@Æ •
3.	keylock	passwordandkey	Ó_ÒÓàc-C
4.	plaintex	crystaletekeydat	úÝö$r•¾
5.	protection	newkeydata	µu¿ð?«ï

The IDEA Encryption Flowchart is illustrated in Figure 3. bellow:

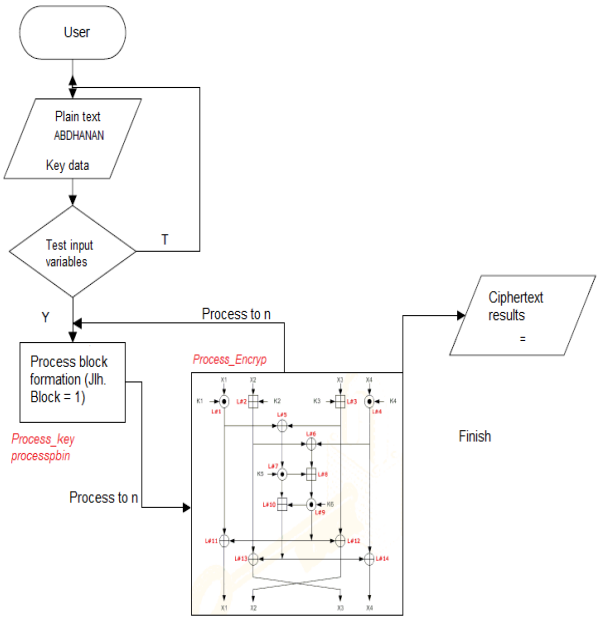

Figure 3. IDEA Encryption Flowchart

The form of encryption process design diagram and data description using IDEA cryptographic algorithm is illustrated in Figure 4. below:

http://dx.doi.org/10.31364/SCIRJ/v8.i12.2020.P1220830

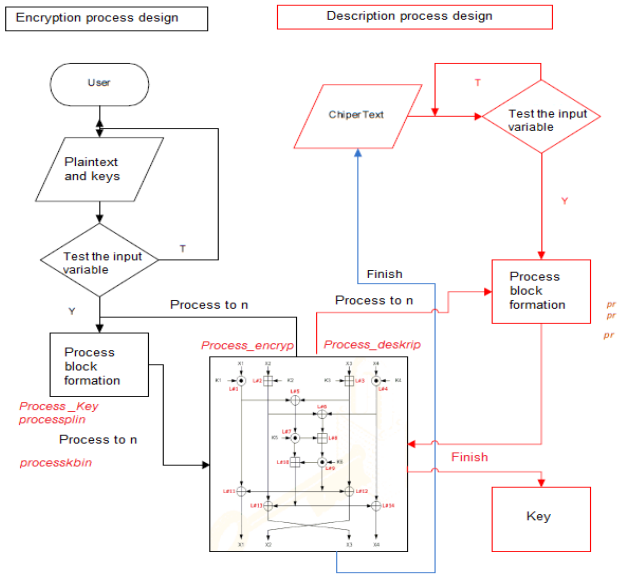

Figure 4. Diagram of Encryption Process Design and Data Description

- *Model Testing*

The three algorithm schemes/models will be combined to get test results regarding the algorithm. Then the best results in terms of data encryption between the two can be seen and are illustrated in Figure 5. below:

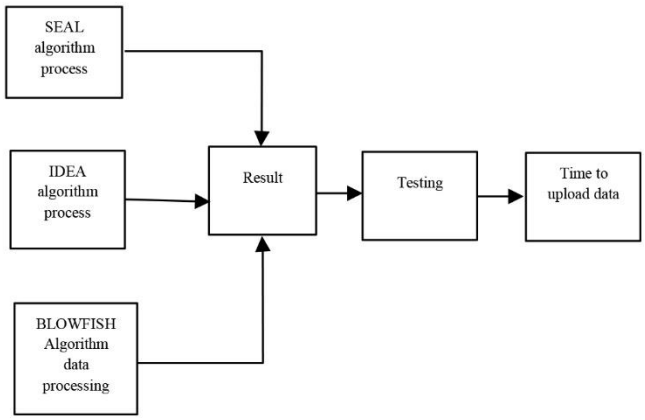

Figure 5. Process of testing model

- *Black Box Testing System*

According to (Akanksha Verma, 2019) Black box is a software testing technique that is widely used to determine the functionality of an interface system [1] depicted in Figure 6. below:

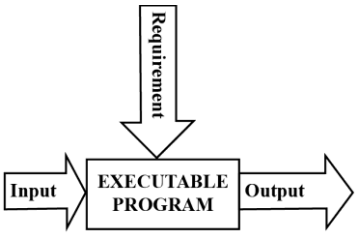

Figure 6. Black Box Testing Method (Verma, 2017)

- *Research Design*

Applications designed in this study were built using the PHP programming language. In this study, an application prototype was developed that applies the SEAL, IDEA and Blowfish algorithms. This prototype will display information on how long the data encryption process will take. For more details, it can be seen in Figure 7. below:

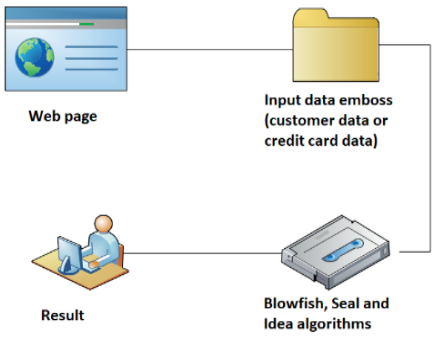

Figure 7. Application Workflow

III. Research And Discussion

A. Study Overview

There are several studies related to scheduling optimization using genetic algorithms. The research conducted by (Sihotang, 2017) uses the blowfish algorithm method, the huffan research result is that the huffman has the largest compression rate in the text compression process, the original size text file is 172012 bytes, using the half byte method the size is 171 124 bytes, using the run length method to be 171062 bytes [11]. Research conducted by (I Made Kartika, 2016) using the Seal algorithm method, the results of his research are the occurrence of large changes in file size and time after the encryption process because during the file encryption process, there are several processes, namely the formation of file hashes, data decomposition, data insertion with file hashes , and the process of reconstructing encrypted data files [7]. Research conducted by (Tri Ardriyanto, 2014) Pardede results of his research stated that the time required for the encryption and decryption process in text files using the IDEA algorithm is relatively the same as the processing time for encryption and decryption using the Blowfish algorithm. The processing time for encryption and decryption of document files between the IDEA algorithm and Blowfish only show slight differences [13]. Research conducted by (Manju Suresh, 2016) used Verilog HDL and found that the modified algorithm was more efficient than the original in terms of encryption time of 16.9% and throughput of 18.7% [10]. The research conducted (Sujacka Retno, 2018) using the Honey Encryption Algorithm and the Blowfish Algorithm. The results of the research are comparisons that have been carried out. The results show that if you review the encryption and decryption process, the Honey Encryption algorithm is much more effective and efficient than the Blowfish algorithm in terms of security and level, encryption and decryption complexity [12]. Research conducted (Dimas Aulia

http://dx.doi.org/10.31364/SCIRJ/v8.i12.2020.P1220830

Trianggana1, 2015) using cryptography, Blowfish Algorithm, Twofish Algorithm, the result is that the Blowfish algorithm has a faster execution time compared to the Twofish algorithm, and when viewed from the size of the file before and after the encryption and decryption process, the Blowfish algorithm and the algorithm Twofish has the same size [5]. Then there is research that comes from (Fresly Nandar Pabokory, 2015) using Cryptography, Advanced Encryption Standard (AES), the results of his research are encrypting files to documents compressed into images so that the security is thicker [6].

B. Implementation

This section will explain some of the screen displays available in the application and their functions.

1) Login Form Interface

The login menu is used to perform the login process by ordinary users, and the data entered is in the form of a user and a password. In this menu, the Blowfish algorithm decryption will be implemented in securing user password data following the Login screen display in Figure 8. below:

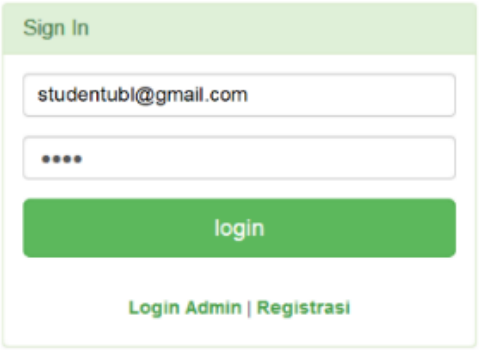

Figure 8. Login Menu Interface

2) Registration Form Interface

The registration menu is used to carry out the registration process by ordinary users who do not have login access, in this menu the registered user's password will be encrypted using the Blowfish algorithm, which can be seen in Figure 9. below:

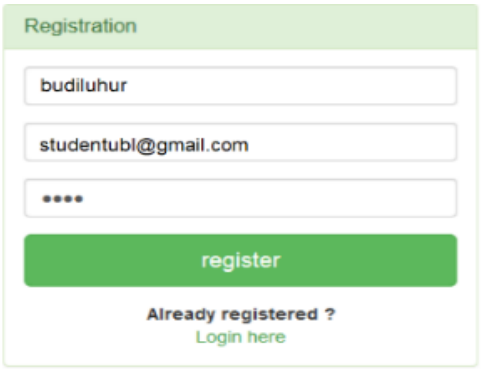

Figure 9. Registration Menu Interface

3) Home Form Interface

The home menu screen will appear after the login process is successful. The changes include the login button will change to a sign out button. Can be seen in Figure 10. below:

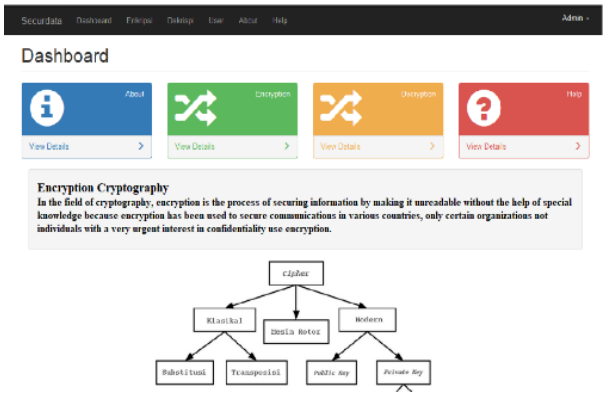

Figure 10. Home Interface

4) Form Encryption Interface

The enkrispi menu is used to perform the encryption process by users who have logged in to the application, in this menu the SEAL algorithm will be implemented to secure data in doc, txt and xlx formats. The user will upload the data so that the algorithm process will run can be seen in Figure 1. below:

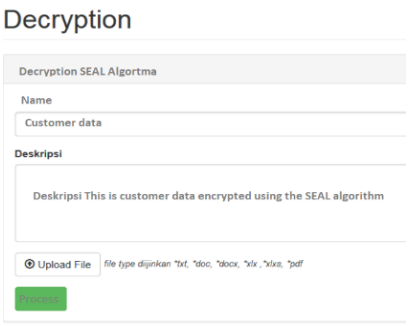

Figure 11. Form Encryption Interface

5) Decryption Form Interface

The decryption menu is used to perform the decryption process by users who are logged in to the application, this menu will implement the IDEA algorithm to encrypt data in doc, txt and xlx formats. The user will upload the encrypted data so that the algorithm process will run as shown in Figure 12. below:

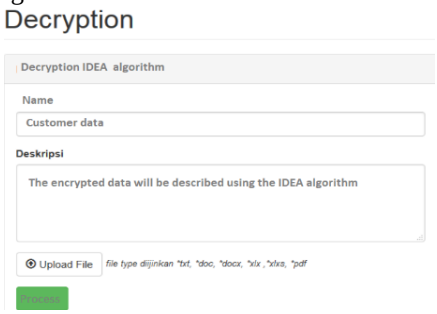

Figure 12. Decyrption Form Interface

6) About Menu Interface

The About Menu screen will appear after the login process is successful. The changes can be seen in Figure 13. below:

http://dx.doi.org/10.31364/SCIRJ/v8.i12.2020.P1220830

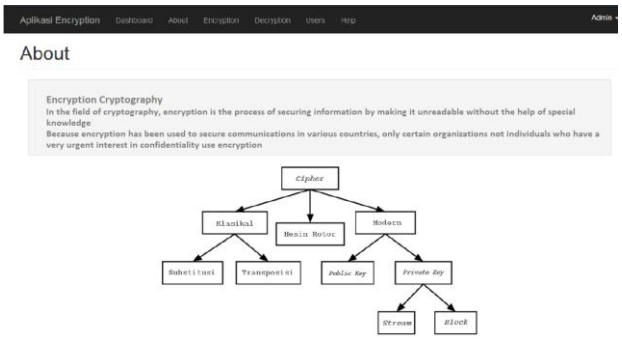

Figure 13. About Menu Interface

7) Users Menu Interface

The User Menu screen will appear after the login process is successful. This menu will display registered user data for more details, it can be seen in Figure 14. below:

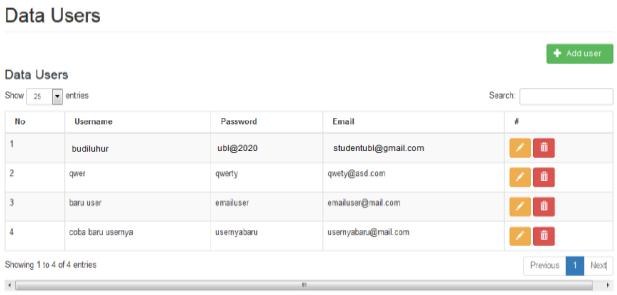

Figure 14. User Menu Interface

C. Testing

1) Black Box Testing

This algorithm is tested by measuring the level of success overcoming speed, memory, number of iterations, diversity of solutions, and the target fitness value and is achieved. Testing with black box in table 2. below:

Table 2. Black Box Testing

Interface	Which is tested	Input	Output	Status
Form Login	The Login button is clicked or entered	username: admin, password:Admin	The main menu opens	TRUE
		Email:Adminq, password: 12345	Blank error message appears and remains on the login form	TRUE
Form Register	Insert data user	username member, email: member@mail.com, password: sandi	User list page appears	TRUE
		username : ",eail",password is not filled	ShownPermanent error messages on the add user form	TRUE
Form enkripsi	Upload file encryption	Name:name file description: description file, Upload file:*pdf	A message has been successfully encrypted and a list of encrypted files appears	TRUE
		Name:name file description: description file, Upload file:*pptx	An error message appears and remains on the encryption file upload form	TRUE
Form deskripsi	Upload file description	Name:name file description: description file, Upload file:*idea	A successful decryption message appears and the page lists the decrypted files	TRUE
		Name:name file description: description file, Upload file:*pdf	An error message appers and remains on the decryption file upload form	TRUE

2) Blowfish Algorithm Encryption Testing

Testing Encryption of Blowfish Algorithm for size time, encryption speed can be seen in table 3 below:

Table 3. Blowfish Algorithm Encryption Testing

Trial	Size Plaintex (kb)	Decryption Time (Detik)	Decryption Speed (Byte/s)	Size Ciphertext (Kb)
Customer.doc	0,95	1,533	0,278	0,69
Card.xlx	1,74	4,75	0,099	1,89
Customer.txt	2,74	5,545	0,025	2,99
Customer.xlx	3,48	11,469	0,082	5,9

3) Testing The Blowfish Algorithm Decryption

Testing the Blowfish Algorithm decryption so that it can be concluded that the plaintext size can change the file size can be seen in table 4. below:

Table 4. Testing The Blowfish Algorithm Decryption

Trial	Size Ciphertext (Kb)	Decryption Time (Detik)	Decryption Speed (Byte/s)	Size Plaintex (kb)
Customer.doc	0,69	0,567	0,278	0,95
Card.xlx	1,89	2,76	0,099	1,74
Customer.txt	2,99	2,235	0,025	2,74
Customer.xlx	5,9	5,762	0,082	3,48

4) Testing The Seal Algorithm Encryption

Testing the size, time, encryption speed with the SEAL Algorithm can be seen in table 5. below:

Table 5. Testing The Seal Algorithm Encryption

Trial	Size Plaintex (kb)	Decryption Time (Detik)	Decryption Speed (Byte/s)	Size Ciphertext (Kb)
Customer.doc	0,95	2,533	0,245	3,69
Card.xlx	1,74	5,75	0,074	6,99
Customer.txt	2,74	10,545	0,065	10,9
Customer.xlx	3,48	11,469	0,039	13,9

5) Testing The Seal Algorithm Decryption

Testing the decryption so that it can be concluded that the plaintext size can change the file size as seen in table 6. below:

Table 6. Testing The Seal Algorithm Decryption

Trial	Size Plaintex (kb)	Decryption Time (Detik)	Decryption Speed (Byte/s)	Size Ciphertext (Kb)
Customer.doc	3,69	1,533	0,245	0,95
Card.xlx	6,99	3,75	0,074	1,74
Customer.txt	10,9	6,545	0.065	2,74
Customer.xlx	13,9	10,469	0,039	3,48

6) Testing The Idea Algorithm Encryption

The result of testing the size, time, encryption speed with the IDEA Algorithm can be seen in table 7. below:

Table 7. Testing The Idea Algorithm Encryption

Trial	Size Plaintex (kb)	Decryption Time (Detik)	Decryption Speed (Byte/s)	Size Ciphertext (Kb)
Customer.doc	0,95	1,533	0,415	2,69

http://dx.doi.org/10.31364/SCIRJ/v8.i12.2020.P1220830

Card.xlx	1,74	4,75	0,234	5,89
Customer.txt	2,74	5,545	0,045	8,99
Customer.xlx	3,48	11,469	0,072	11,9

7) Testing The Idea Algorithm Decryption

Decryption testing so it can be concluded that the plaintext size can change the file size, as seen in table 8. below:

Table 8. Testing The Idea Algorithm Decryption

Trial	Size Ciphertext (Kb)	Decryption Time (Detik)	Decryption Speed (Byte/s)	Size Plaintex (kb)
Customer.doc	2,69	1,003	0,415	0,95
Card.xlx	5,89	2,75	0,234	1,74
Customer.txt	8,99	3,234	0,045	2,74
Customer.xlx	11,9	9,352	0,072	3,48

8) White Box Testing

White box testing is a test based on checking the details of the design, using the control structure of the procedural design program to divide the test into several test cases. Testing is done based on how a software produces output from the input. This test is carried out based on the program code can be seen in table 9. below:

Table 9. Encryption Cource Code

Node	Source code
1	<form role="form" method="post" action="encrypt-process.php" enctype="multipart/form-data"> <fieldset> <label>Nama</label> <input class="form-control" placeholder="nama" name="name" type="text" autofocus> <label>Deskripsi</label> <textarea class="form-control" name="deskripsi" cols="30" rows="4" id="deskripsi" placeholder="deskripsi"></textarea> <input id="inputFile" placeholder="Input File" type="file" name="file" required> file type diijinkan *txt, *doc, *docx, *xlx ,*xlxs, *pdf
2	if (isset($_POST['proses'])) {
3	$start = (double)microtime()+time(); $name = $_POST["name"];
4	}
5	if($ext=="docx" || $ext=="doc" || $ext=="txt" || $ext=="pdf" || $ext=="xls" || $ext=="xlsx"){
6	

7	else{
	echo("<script language='javascript'>
	window.location.href='enkripsi.php';
	window.alert('Maaf, file yang bisa dienkrip hanya word, excel, text, ppt ataupun pdf.');
	</script>");
	exit();
	}

8	if($size2>3084){
	echo("<script language='javascript'>
	window.location.href='enkripsi.php';
	window.alert('Maaf, file tidak bisa lebih besar dari 3MB.');
	</script>");
	exit();
	}

9	if($ext=="pdf" || $ext=="xls" || $ext=="xlsx"){
10	$sql1 = "INSERT INTO file VALUES ('', '$name', '$final_file', '$finalfile.chpr', '', '$size2', now(), '1', '$deskripsi','$durasi','')"; $query1 = mysqli_query($connect,$sql1); }

11	function seal_encrypt($message, $key, $salt) {
	$seal = new SEAL ("$key\0$salt");
	$mask = pack("V*", $seal->r);
	while (strlen($mask) < strlen($message)) {

12	$seal->seal(); $mask .= pack("V*", $seal->r); }
13	return $message ^ substr($mask, 0, strlen($message)); }
14	if($mod==0){
15	$banyak = $size / 16; }

16	else{
	$banyak = ($size - $mod) / 16;
	$banyak = $banyak+1;
	}

17	*if(is_uploaded_file($file_tmpname)){*

18	move_uploaded_file($file_tmpname,"./file_decrypt/".$finalfile."~");
	ini_set('max_execution_time', -1);
	ini_set('memory_limit', -1);
	}

19	else{
	echo("<script language='javascript'>
	window.location.href='enkripsi.php';
	window.alert('Encrypt file mengalami masalah..');
	</script>");
	}

D. Cyclomatic Complexity

This is a software metric that provides a quantitative measurement of the logical complexity of a program. When used in the context of the flow-based test method, the value obtained will determine the number of independent paths in the path set, and will provide an upper limit value for the number of tests that must be performed, to ensure that all statements have been executed at least once can be seen in Figure 15. below:

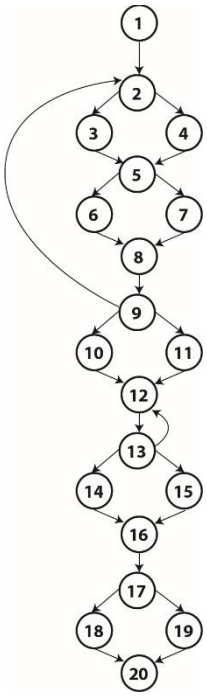

Figure 15. Cyclomatic complexcity

From Figure 15. above Cyclomatic Complexity can be determined as follows:

V(G) = E-N+2 = 25-19+2 = 8	E = The number of arcs in the flow graph is 25 N = The number of nodes in the flow graph is 19

E. Result of Cyclomatic Complexity

Metric software that provides a quantitative measure of the logical complexity of a program. By using the measurement or calculation results of the cyclomatic complexity metric, we can determine whether a program is a

http://dx.doi.org/10.31364/SCIRJ/v8.i12.2020.P1220830

simple or complex program based on the logic applied to the program. If associated with software testing, Can be see in table 10. below:

Table 10 : Result Cyclomatic Complexity

Basis Flow	Independent path
1 Path	1-2-3-5-6-5-7-8-9-10-11-13-14-16-17-18-19
2 Path	1-2-3-5-6-5-7-8-9-10-12-13-15-16-17-18-19
3 Path	1-2-4-5-6-5-7-8-9-10-12-13-15-16-17-19
4 Path	1-2-4-5-6-5-7-8-9-10-12-13-14-16-17-19
5 Path	1-2-3-5-6-5-7-8-9-10-12-13-15-8-16-17-18-19
6 Path	1-2-3-5-6-5-7-8-9-10-12-13-15-8-16-17-19
7 Path	1-2-4-5-6-5-7-8-9-10-12-13-15-8-16-17-19
8 Path	1-2-4-5-6-5-7-8-9-10-11-15-8-16-17-19

IV. Conslusion

Based on the results of the research that has been carried out, it can be concluded that the system can secure data using the SEAL and Blowfish algorithms and with the IDEA algorithm decryptions so that data storage and exchange becomes safer. In the cryptographic process using the SEAL and Blowfish methods, a symmetric key was used in the process. Encryption and decryption using the IDEA algorithm. The time obtained to perform encode and decode process is directly proportional to the size of the file being processed.

References

[1] Akanksha Verma, et al. (2019). A Comparative Study of Black Box Testing and White Box Testing International Journal of Computer Sciences and Engineering Open Access A Comparative Study of Black Box Testing and White Box Testing, (December 2017). https://doi.org/10.26438/ijcse/v5i12.301304

[2] Cnnindonesia. (2020). Search-91-million-data-leaked-tokopedia-for-sale-rp74-million.

[3] CnnIndonesia. (2016). Cyber Crime, the Most Crime Cases in 2016.

[4] Cyber-crime-Indonesia. (2016). 36.6 million incidents of cyber attacks.

[5] Dimas Aulia Trianggana1, et al. (2015). BLOWFISH AND TWOFISH ALGORITHM IN ENCRYPTION AND DECRIPSION PROCESSES, 37–44.

[6] Fresly Nandar Pabokory, et al. (2015). IMPLEMENTATION OF DATA SECURITY CRYPTOGRAPHY IN TEXT MESSAGES, DOCUMENT FILE CONTENTS, AND DOCUMENT FILES USING ADVANCED ENCRYPTION ALGORITHM, 10 (1).

[7] I Made Kartika, et al. (2016). IMPLEMENTATION OF SEAL ALGORITHM ON DATA SECURITY.

[8] itgid.org. (2017). five cases of cybersecurity.

[9] Kholidya Yuli Wardani, et al. (2017). IMPLEMENTATION OF IDEA CRYPTOGRAPHIC METHOD on PRIORITY DEALER for BOOKING SERVICES and WEB-BASED HAMDPHONE SALES REPORTS, 1–7.

[10] Manju Suresh, et al. (2016). Hardware implementation of blowfish algorithm for the secure data transmission in the Internet of Things. Procedia Technology, 25 (Raerest), 248–255. https://doi.org/10.1016/j.protcy.2016.08.104

[11] Sihotang, D. (2017). DESIGNING TEXT DATA SECURITY APPLICATIONS WITH IDEA METHODS AND USING COMPRESSION, 14–19.

[12] Sujacka Retno, et al. (2018). ENCRYPTION AND BLOWFISH ALGORITHM, 858 (1).

[13] Tri Ardriyanto, et al. (2014). STUDY AND COMPARISON OF IDEA ALGORITHM AND BLOWFISH ALGORITHM. Industry, Faculty of Technology.

[14] Yani Parti Astuti, et al. (2016). OPTIMIZING PASSWORD ENCRYPTION USING, 15 (1), 15–21.

http://dx.doi.org/10.31364/SCIRJ/v8.i12.2020.P1220830