Web Secure Login Design With Symetric Encription RC-6 Algorithm

Arkhan Subari
Faculty of Enggineering, Diponegoro University
Semarang, Indonesia
Email : arkhansubari@undip.ac.id

Kodrat Iman Satoto
Faculty of Engineering, Diponegoro University
Semarang, Indonesia
Email : kodrat@undip.ac.id

Abstract - **Authentication techniques that use at many web pages and easy to do is use user-id and password. However, these techniques are vulnerable to theft user-id and password when sent from client to server. For that given an alternative security by encrypting the user-id and password at client side before being sent to the server. The algorithm used is symmetric algorithm RC-6, designed with javascript on the client side and PHP on the server side. Based on RC-6 Symmetric encryption algorithm, the research done by creating a generating keys script for encryption and decryption, encryption RC-6 with javascript, decryption RC-6 with PHP and the design of a prototype web page with a login that already uses encryption. Using the program fidller and wireshark shows that a web page with login form that does not use encryption to send user-id and password in plaintext form so easily obtained by the sniffer. While in the web pages that use encryption, user-id and password is sent in the form of ciphertext. The addition of a web page access time is shown by firebug, where on the web pages that use encryption are adding an average access time of 64.67 ms.**

Keywords : web, login, encryption, decryption, RC-6, PHP, javascript, fidller, wireshark, firebug

I. INTRODUCTION

In web technology, authentication to access the web page that is confidential and restricted. One of the most widely used method is to use user-id and password are entered on the login form. In addition to cheap and require no additional devices, use of user-id and password is also convenient. Users only need to memorize user-id and password can then log in anywhere (Yang, 2009).

However, the use of user-id and password is not without drawbacks. Users often choose the user-id and password are short and weak, so easily stolen by brute-force technique (Yang, 2009). Besides the standard format of the login form will send the user-id and password from the client to the server in plaintext format or the original text. In this format, it is very easy for hackers to get the data user-id and password are valid and can be used on the login form in question (Chakrabarti dan Singhal, 2007).

To keep the user-id and passwords are not easily read by hackers required process to protect user-id and password. An alternative process to protect data is encrypt user-id dan password on the client side before the data is sent to the server via the internet. Thus that is sent through the Internet is the ciphertext. Ciphertext format can also protect user-ids and passwords from being stolen by brute-force technique (Halevi dan Krawczyk, 1998). On the server side perform decryption to get the original data.

One of the encryption algorithm is the algorithm RC-6. RC-6 is a block cipher algorithm that is registered to a NIST proposed by RSA Security Laboratories. RC-6 is included in the category of symmetric encryption that uses the same key in encryption and decryption. RC-6 using a 4 (four) working registers, and include integer multiplication as an additional primitive operation. Multiplication operations increase the spread for each rotation thereby increasing the safety factor, reducing the round, and improve performance outcomes. Level of security on this algorithm lies in the strength of rotation is based on the data, the exclusive use of the alternate OR, modulo functions and functions of the equation that uses a fixed rotation.

II. PROBLEM

Problems identified in the web-based login form is securing user-id and password sent from client to server that are not easily obtained by hackers. Proposed solution to overcome this problem is to do the encryption user-id and password using the symmetry algorithm RC-6 before being sent. Encryption is done using javascript on the client side while on the server side decryption performed by using php.

From the above, research is focused to answer the question whether the symmetric encryption algorithm RC-6 is able to secure the login process on web technologies?

III. BASIC CONCEPTS OF CRYPTOGRAPHY

Cryptography comes from the Greek Kryptos meaning "hidden" and graphein meaning "writing", so is the art and science of cryptography to maintain data security. And an expert called a cryptographer. Cryptanalst are people doing cryptanalysis, the art and science to open the ciphertext into plaintext without going through the way it should. Readable data is called plaintext and techniques to make such data can not be read to be called encryption. The result of encrypting data is called ciphertext, and the process to return the ciphertext into plaintext is called decryption. Branch of mathematics that includes cryptography and cryptanalysis is called cryptology and the culprit is called cryptologist.

Cryptographic system or cryptosystem is an algorithm plus all possible plaintext, ciphertext and key. In this system, a set of parameters that specify a particular encoding transformation is called a set of keys. Encryption and decryption process is governed by one or more cryptographic keys. In general, the keys used for encryption and decryption process does not need to be identical, depending on the system used. Each cryptographic algorithm comprises an encryption algorithm (E) and decryption algorithm (D). Mathematical basis underlying the process of encryption and decryption is a relation between two sets is the set that contains elements of the set which contains the plaintext and ciphertext element. Encryption and description of a transformation function between the two sets. Generally it can be described mathematically as follows:

Ek(P) = C (Encrypt)
Dk(C) = P (Decrypt)
Dk(E(P)) = P (Decrypt)

In the process, the plaintext P encrypted with a key K and the resulting message C. In the decryption process, C is described by using the key K to produce the same M as before.

A. RC-6 Encrypt Algorithm

RC-6 split 128-bit block into 4 block of 32 bits, then this algorithm works with 4 pieces of 32-bit registers A, B, C, D. The first byte of plaintext or ciphertext is placed in byte A, while the last byte is placed in bytes D. In the process will be obtained (A, B, C, D) = (B, C, D, A) which means that the value of which is located on the right side comes from the register on the left.

Algorithm RC-6 using 44 pieces of sub keys that are raised from the keys and called with S [0] to S [43]. Each sub key length is 32 bits. The process of encryption on the algorithm RC-6 begins and ends with a whitening process that aims to disguise the first iteration and the last of the encryption and decryption process. At the initial whitening process, the value of B will be summed with S [0], and D values are summed with S [1]. At each iteration of the RC-6 uses two pieces of sub keys. Sub-key on the first iteration using S [2] and S [3], while the iteration, the next iteration using the key sub-sequel. After the 20th iteration was completed, a final whitening process in which an A summed with S [42], and C values are summed with S [43].

Each iteration of the algorithm RC-6 follow the rules as follows, the value of B inserted into the function f, defined as f (x) = x (2x +1), then rotated left as far as lg-w or 5 bits. The results obtained in this process is exemplified as u. The value u then XORed with C and the result becomes the value of C. T values are also used as a reference for the C value is left to play. Similarly, the value of u, also used as a reference for the value of A to make the process of playing left. Then the sub key S [2i] at iteration summed with A, and sub key S [2i +1] are summed with C. The fourth part of the block will then be exchanged by following the rules, that an A ditempakan on D, the value of B is placed on A, the value of C is placed at B, and the (original) D pad placed C. Thus the iteration will continue until 20 times.

B. RC-6 Decrypt Algorithm

Ciphertext decryption process in the algorithm RC-6 is a reversal of the encryption process. In the whitening process, if the encryption process uses the addition operation, then the decryption process using a reduction operation. Sub keys used in the whitening process after the last iteration is applied before the first iteration, and vice versa subkeys are applied to the whitening process before the first iteration used in whitening after the last iteration. Consequently, to perform decryption, the thing to do is simply apply the same algorithm as encryption, with each iteration using the same sub-key used during encryption, it's just a sequence of sub keys used upside down.

C. Key generation

Users enter a key size of b bytes, where $0 \leq b \leq 255$. Key bytes are then placed in an array c w-bit words L[0] ... L [c-1]. The first byte of the key will be placed as in L [0], the second byte in L [1], and so on. (Note, if b = 0 then c = 1 and L [0] = 0). Each value of w-bit word will be raised at the round key addition 2r +4 and will be placed on the array S [0, ..., 2r +3]. The constant P32= B7E15163 and Q32 = 9E3779B9 (in hexadecimal) is the "magic constants" used in the key scheduling of the RC-6. P32 values obtained from the binary expansion of e-2, where e is a logarithmic function. While the Q32 value obtained from the binary expansion of -1, which is arguably the "golden ratio" (the golden ratio).

IV. PHP HYPERTEXT PREPROCESSOR (PHP)

PHP is a programming script that is executed together with HTML and is a server side language. So the execution of a PHP script done on the server. While sending data to the client only in the form HTML view. PHP is stored in files ending in. Php,. Php3 or. Phtml, it depends on the setting of PHP, but in general the PHP file extension is. Php. PHP code with the tags - HTML tags in one file. PHP several advantages compared with other programming languages, namely:

- PHP is easy to make and has a high-speed access
- PHP can run on different Web servers and in different operating systems. PHP can run on the system oprasi UNIX, Windows, Windows NT, and Macintosh
- PHP was published free of charge

- PHP can also run on a web server is Microsoft Personal Web Server, Apache, IIS, Xitami, and so on.
- PHP includes language that is embedded (can be placed or affixed to the HTML tag).

V. JAVASCRIPT

Javascript is a cross-platform language that was first introduced by Netscape. Javascript is a script language (scripting) object-oriented. JavaScript contains a core set of objects, such as Array, Date, and Math, and a core set of language elements such as operators, control structures, and statements.

Javascript provides a means for running applications over the Internet. Client applications running in browsers such as Netscape Navigator and server applications running on the server such as Netscape Enterprise Server. Javascript can be used to create dynamic HTML that processes user input and maintain data using special objects, files, and database relationships. Javascript was invented by Netscape and first used in Netscape browsers.

VI. METHODOLOGY

Authentication process begins by entering a user-id and password in the login form has been determined. User-id and password and then sent from client to server. After receiving the user-id and password server to authenticate the user-id and password with the data stored on the server. If the user-id and password is valid, then the server will fulfill client requests according to user-id privileges in question. If no valid will be given a message to the client that the user-id and password is not valid.

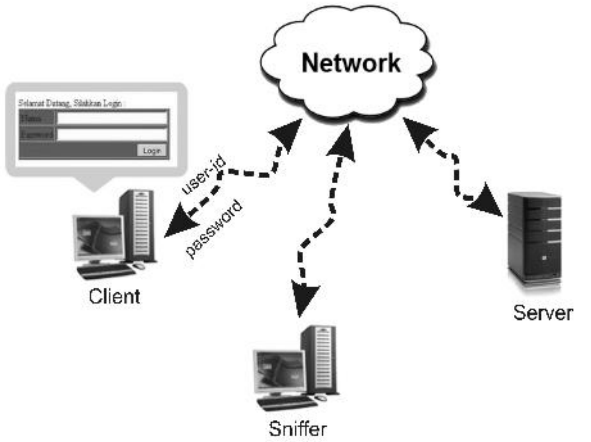


FIGURE 1. DESCRIPTION OF THE LOGIN FORM AUTHENTICATION IN WEB TECHNOLOGY

In standard format, the form will send plainttext login. Suppose the user-id is "abc" and password is "def", when pressing the "Login" then the data "abc" and "def" will be sent to the server. If during the delivery process there are sniffer or hacker that is able to obtain this data, then the sniffer or hacker could use the data to do is log on the web.

To prevent sniffer get plainttext of user-ids and passwords, encryption done user-id and password before being sent to the server so that the data transmitted is encrypted (ciphertext). Server will not decrypt the ciphertext before authentication.

For system design and analysis of the results required additional tools-tools as follows:

- *Browser*
- *Fiddler* v2.2.9.1
- *Wireshark* v1.2.1
- *Firebug v1.5.4*

Design done on the client side and server side. Picture of the system on the client side is shown in Figure 2 while the server side is presented in Figure 3.

Main page displays a login form to enter user-id and password. At the login button is pressed, the input user-id and password is encrypted using the RC-6 before being sent to the server. On the server side, the first step is to build a session. Furthermore, the data is sent from the client will be decrypted with the same algorithm. The results were compared with data stored on the server. If these data are then displayed according to the requested web page. The error message displayed when the data being compared are not appropriate.

VII. DESIGN

The research design of a secure web login using symmetry encryption RC-6 algorithm is done in several steps as follows:

- Key generation algorithm.
- Symmetric encryption RC-6 algorithm.
- Symmetric decryption RC-6 algorithm.
- Designing a web-based login page using encryption RC-6.
- Decryption process of designing user-id and password, and authentication with the data stored on the server.

A. Key generation algorithm

The key used for encryption and decryption of data on kriptography. In kriptography symmetry algorithm, the key used in encryption and decryption process is the same. Thus the key generation in this study is done once for each encryption process.

Key generation is done by creating a random string to every user to be logged. Through this process each user-id and passwords are encrypted using different keys. This random string will be placed on the array L which is a sequence of bytes of data generated key. Each character, will be encoded into 8 bits binary or 1 byte. Therefore, the amount of data on L equals the number of characters on the keys. The next step is the initialization key. Initialization is done so key table S contains pseudo-random bit pattern is fixed. At this stage, the resulting pattern does not depend on the key, but relies on two magic constants P = b7e15163H and Q = 9e3779b9H. Data is then performed mixing S and L to get the key that will be used for data encryption.

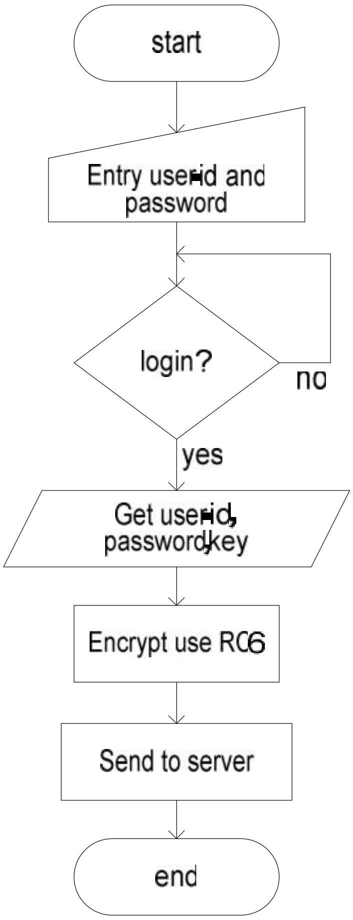


FIGURE 2. CLIENT SIDE

The entire process for encryption key generation algorithm using RC-6 can be described according to the flowchart in Figure 4.

B. Symmetric Encryption RC-6 Algorithm

Encryption function is made by using the javascript programming language. The use of the javascript programming language in the encryption process associated with the encryption process is performed on the client side. So used programming language that is executed on the client side.

User-id and password to be encrypted is divided into 4 blocks that will be placed on the 4 pieces registers A, B, C and D. The next four registers is encrypted using keys that have been raised on the key generation process. In the key generation, key data respectively were merged into one so that the encryption is done before the process of separation is the key array. The entire encryption process user-id and password using the symmetric encryption RC-6 algorithm as shown in Figure 5.

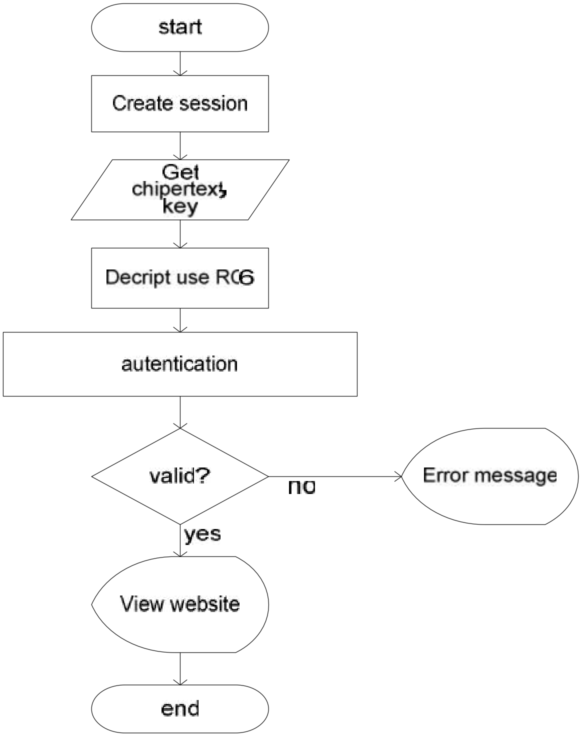


FIGURE 3. SERVER SIDE

C. Symmetric Decryption RC-6 Algorithm

Decryption process is needed to get back to user-id and password that has been encrypted. This process is performed on the server so that the language used is a language that supports server side programming. In this case use the PHP programming language. Decryption process uses the same key with the key that is used in the encryption process. Delivery of data user-id and password from the client to the server is done using a variable. Therefore the separation process is required to register each decryption process. Having obtained the data registers A, B, C and D, using the same key data decryption process is done. This decryption process can be described using a flowchart as shown in Figure 6.

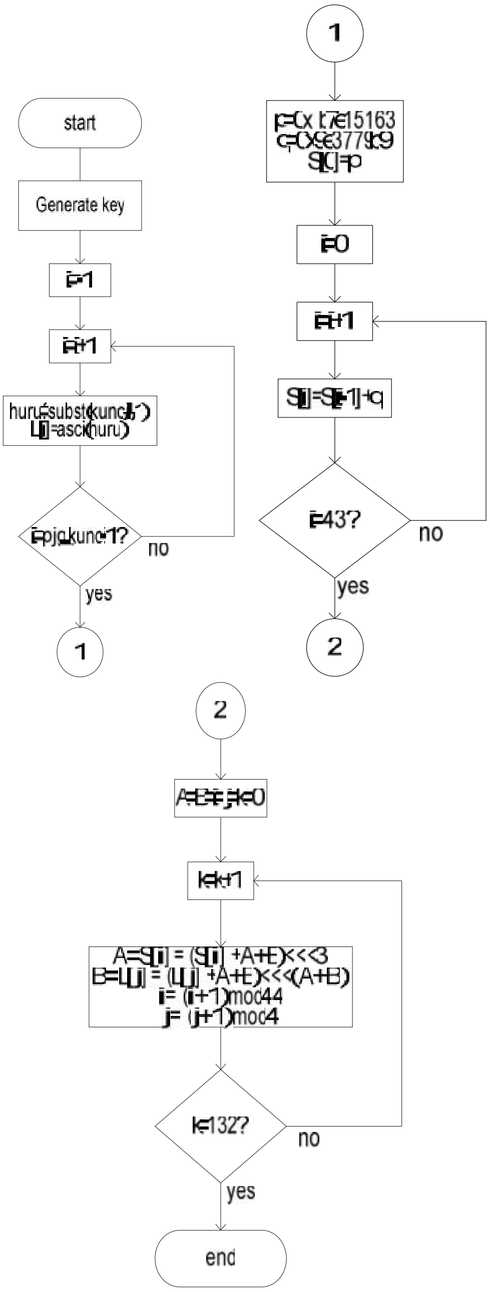


FIGURE 4. KEY GENERATION ALGORITHM

VIII. RESULTS

By using a browser, program design is shown. In this case use two browsers ie mozilla firefox and internet explorer. Display the main page in the study are shown in Figure 7.

Using fiddler, we can known what data transferred. This is done by running the program fiddler along with accessing web pages. At the time of logging into a standard form, in getting data on the fiddler is nm = arkhan & y = taruna as in Figure 8. These data indicate that the standard login form data transfer without performing any security precautions. Thus easy to note that the user-id used to login is arkhan with a password taruna.

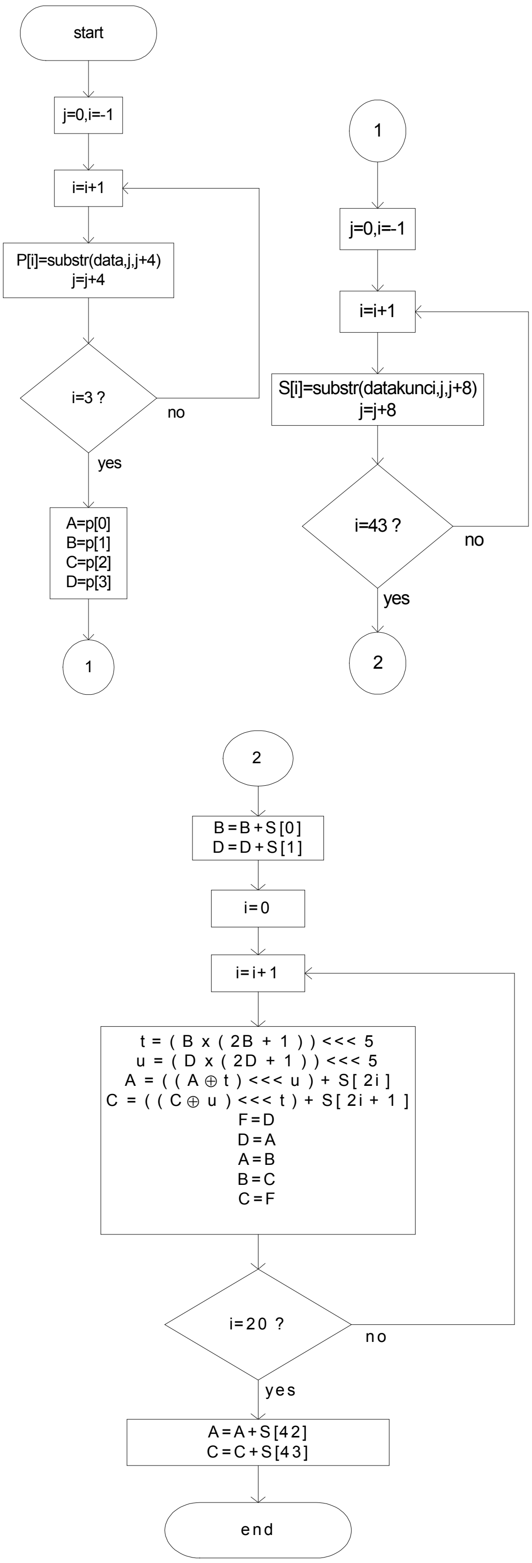


FIGURE 5. SYMMETRIC ENCRYPTION RC-6 ALGORITHM

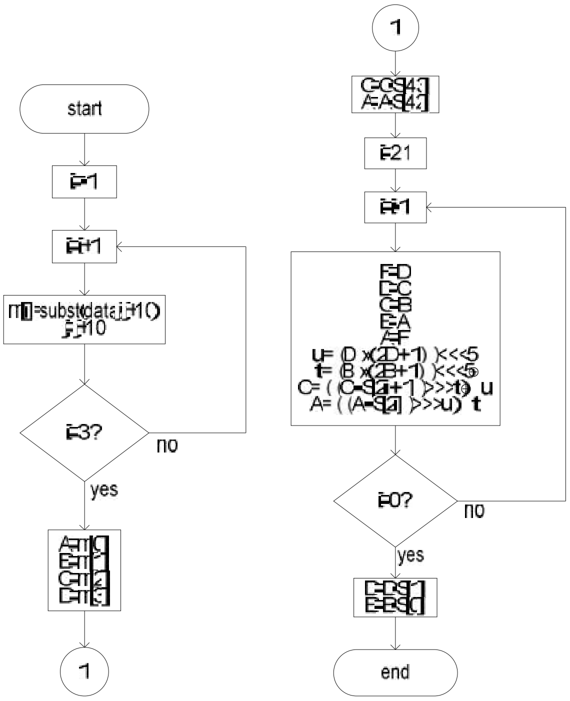


FIGURE 6. SYMMETRIC DECRYPTION RC-6 ALGORITHM

Different data obtained at login with a secure form. In this condition the data obtained is x=24cb4d28c6e60a306900c3500b1b7f48ad363a484f50f750f16bb07093866c6835a12768d7bbe47079d69d901bf15988be0c14886026d19002418ab0a45c46a8467701a8e891beb08aac77d02cc733c8cee1eec870fcabd0131764f0b53220e8574cdbe8f96798f09b8252103d9d0e08dfb7c90881d2861023ed3f30c607fb286822b6280a3d7330ac582c504e72e848f08da34892a8605034c31970d6ddd56878f890681b134d70bd2e06905f48c288&nm=00d5a3fbf00054fb7d58000d4d232a01324e6b9e6&y=00d5a3fbf00054fb7d58000d4d361901395b78916 as shown in Figure 9. This suggests that user-id and password used has been encrypted so it is unknown the data user-id and password is the truth.

A. *Testing With Wireshark* v1.2.1

Figure 10 shows the display when used wireshark to capture data on a standard login form.

From Figure 10, shown at the Line-based text data that the data captured is nm = arkhan & y = taruna. The data consists of two parameters nm with a value arkhan and y with value taruna who are separated by & or ampersand. arkhan and taruna are user-id and password are typed in the login form on a web page. Different results obtained at the time of arrest data on a secure login form. Figure 11 shows the view at the wireshark capture data that is sent from a secure login form.

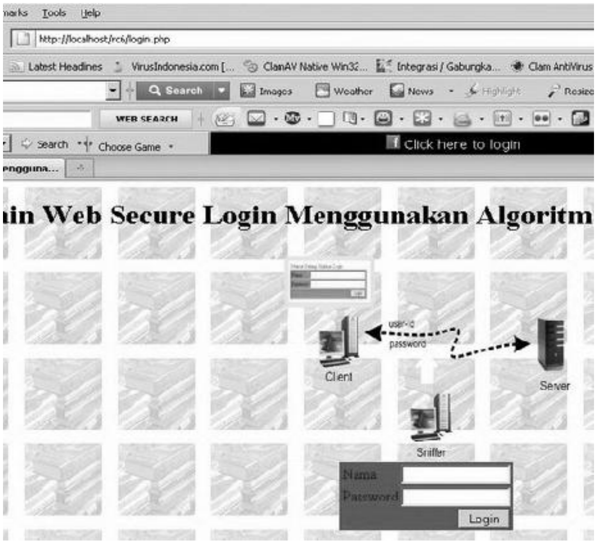
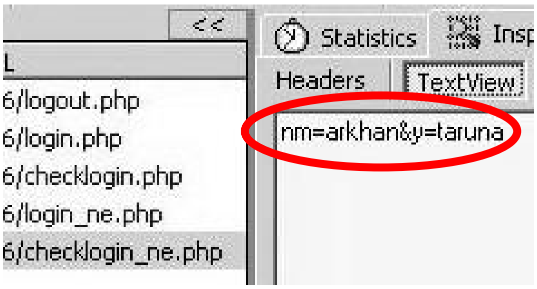


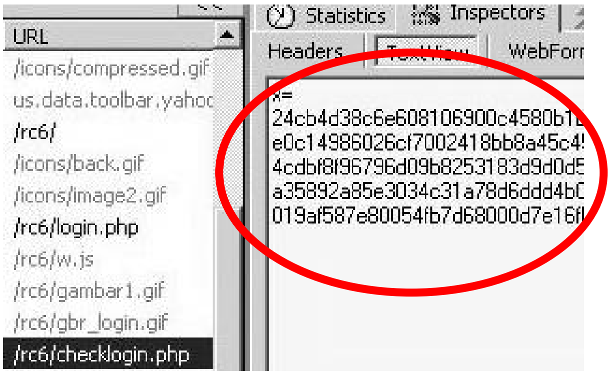
FIGURE 7. THE MAIN VIEW WEBSITE WITH A LOGIN IS ADDED TO THE ENCRYPTION



```
6/logout.php
6/login.php
6/checklogin.php
6/login_ne.php
6/checklogin_ne.php
```

nm=arkhan&y=taruna

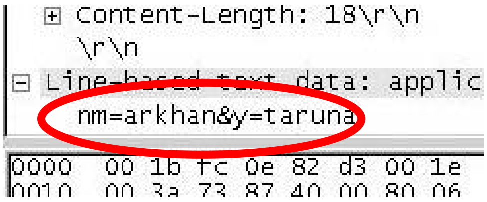
FIGURE 8. FIDDLER ON THE STANDARD LOGIN FORM



```
URL
/icons/compressed.gif
us.data.toolbar.yahoo
/rc6/
/icons/back.gif
/icons/image2.gif
/rc6/login.php
/rc6/w.js
/rc6/gambar1.gif
/rc6/gbr_login.gif
/rc6/checklogin.php
```

```
x=
24cb4d38c6e608106900c4580b1
e0c14986026cf7002418bb8a45c4
4cdbf8f96796d09b8253183d9d0d5
a35892a85e3034c31a78d6ddd4b0
019af587e80054fb7d68000d7e16f
```

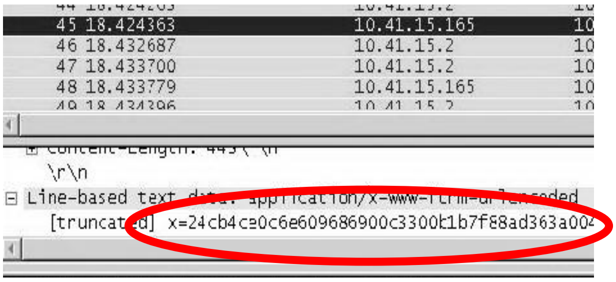
FIGURE 9. FIDDLER ON THE SECURE LOGIN FORM



```
⊞ Content-Length: 18\r\n
  \r\n
⊟ Line-based text data: applic
    nm=arkhan&y=taruna

0000  00 1b fc 0e 82 d3 00 1e
0010  00 3a 73 87 40 00 80 06
```

FIGURE 10. WIRESHARK ON THE STANDARD LOGIN FORM



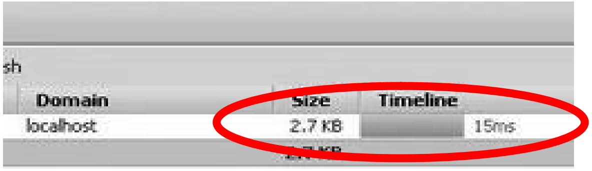
```
45 18.424363          10.41.15.165     10
46 18.432687          10.41.15.2       10
47 18.433700          10.41.15.2       10
48 18.433779          10.41.15.165     10
49 18.434396          10.41.15.2       10
  \r\n
⊟ Line-based text data: application/x-www-form-urlencoded
  [truncated] x=24cb4ce0c6e609686900c3300b1b7f88ad363a004
```

FIGURE 11. WIRESHARK ON THE SECURE LOGIN FORM

From the display can be seen that the data captured by wireshark is not a data user-id and password are entered on the login form but the data is already encrypted.

B. *Website Performance Testing*

Performance is measured by the speed of website access web pages in question. The shorter the time needed to access a web page, the better its performance. In this study of performance measurement is calculated from the speed of access to web pages but measure changes in speed of access to web pages due to the addition of the encryption process on the login process. By using add-on firefox firebug web page access time can be known. Figure 12 is a view of firebug.



Domain	Size	Timeline
localhost	2.7 KB	15ms
	2.7 KB	

FIGURE 12 F*IREBUG*

Table 1. shows the time taken to access a web page with variations user-id and password in the login form and the form of safe standards. The addition of encryption and decryption on a secure login form does not have an impact on increasing access time a website. This time accretion occurs naturally due to the increasing number of files that are called in the login process. In the standard login process, the number of files called is 2 while on a secure login process called 5 pieces of the file.

Additional 3 files needed for key generation, encryption and decryption. The addition of the average time in this experiment was 64.67 ms (0.06467 seconds (sec)). In addition the performance of the access time can be said to reduce the visual performance of the web but added time is not much of an effect. The addition of the access time is balanced with maintaining the security of data transmitted through the Internet.

IX. CONCLUSION

The conclusion that can be drawn from research on designing a secure login form using the encryption symmetry of the RC-6 is:

- By using the program monitors the session fiddler and a sniffer wireshark shown that a login page that does not use encryption facilities, the form sends the user-id and password entered in the form plainttext.
- With the same program is seen that the login form that uses encryption facility, the form sends the user-id and password that has been encrypted (ciphertext).
- For added security, each user session raised key used for encryption and decryption are different. Thus, each user will get a different key each user login.
- Use firebug shows that the addition process on the client side encryption and decryption on the server side add the website access time on average 64.67 ms (0.06467 seconds (sec)). Visually the addition does not affect the access time in the process of appearance of the website.

TABLE 1. ACCESS TIME REQUIRED TO FORM A STANDARD AND SECURE FORM

No	*User-id*	Password	Access Time		Time Gap
			Standard	Secure	
1	arkhan	taruna	73 ms	141 ms	68 ms
2	arkhans	tarunaboyolali	74 ms	141 ms	67 ms
3	arkhansubari	taruna	79 ms	140 ms	61 ms
4	agus	tembalang	74 ms	145 ms	71 ms
5	herlambang	234#@!	79 ms	141 ms	62 ms
6	suryo	123suryo#@!	79 ms	141 ms	62 ms
7	andi@yahoo.com	hebat	78 ms	140 ms	62 ms
8	sempurna	solusi	73 ms	140 ms	67 ms
9	super	duper	79 ms	141 ms	62 ms

REFERENCES

[1]. Anupam, V.; Mayer, A., 1998, “Secure Web Scripting”, IEEE Internet Computing, pp. 46-55.

[2]. Bellare, M.; Pointcheval, D.; and Rogaway, P., 2000, “Authenticated Key Exchange Secure Against Dictionary Attacks”, Advances in Cryptology - EUROCRYPT 2000, Proc. Int’l Conf. Theory and Application Cryptographic Techniques, LNCS 1807, Springer, pp. 139-155.

[3]. Bellovin, S.; Merritt, M., 1992, “Encrypted Key Exchange: Password-Based Protocols Secure Against Dictionary Attacks”. Proc. IEEE Symposium on Research in Security and Privacy, pp. 72-84.

[4]. Boyarsky, M., K., 1999, “Public-key Cryptography and Password Protocols: The Multi-User Case”. Proc. ACM. Computer and Communication Security, pp. 63-72.

[5]. Chakrabarti, S.; Singhal, M., 2007, “Password-Based Authentication: Preventing Dictionary Attacks”, IEEE Computer Society, pp. 68 – 74.

[6]. Halevi, S.; Krawczyk, H., 1998, “Public-key Cryptography and Password Protocols”. Proc. ACM. Computer and Communication Security, pp. 122-131.

[7]. Itani, M.; Diab, H., 2004, “Reconfigurable Computing for RC6 Cryptography”, 2004 IEEE/ACS International Conference on Pervasive Services (ICPS'04), pp. 121-127.

[8]. Prayudi, Y.; Halik, I., 2005, “Studi Dan Analisis Algoritma Rivest Code 6 (Rc6) Dalam Enkripsi/Dekripsi Data”, Seminar Nasional Teknologi Informasi 2005 (SNATI 2005), pp. 149 – 158.

[9]. Pressman, R.S., 2001, “Sofware Engineering : A Practitioner’s Aproach”, McGraw-Hill.

[10]. Rivest, R., L.; Robshaw, M.J.B; Sidney, R.; Yin, Y.L., 1998, “The RC6 Block Cipher”, RCA Laboratories.

[11]. Rudianto, ”Analisis Keamanan Algoritma Kriptografi RC6”, Jurusan Teknik Informatika ITB, Bandung

[12]. Stark, E.; Hamburg, M.; Boneh, D., 2009, “Symmetric Cryptography in Javascript”, 2009 Annual Computer Security Applications Conference, pp. 373-381,

[13]. Veglis, A., 2005, “PHP and SQL Made Simple”, IEEE Distributed Systems Online, pp. 4,

[14]. Yang, Y.; Zhou, J.; Weng, J.; Bao, F., 2009, A “New Approach for Anonymous Password Authentication”, 2009 Annual Computer Security Applications Conference, IEEE Computer Society, pp. 199 – 208.

[15]. Zhongying; Jiancheng, Q., 2009, “Webpage Encryption Based on Polymorphic Javascript Algorithm”, 2009 Fifth International Conference on Information Assurance and Security, pp. 327-330.