Terbit online pada laman web jurnal : **http://seminar.iaii.or.id**

PROSIDING
SEMINAR NASIONAL SISFOTEK
(Sistem Informasi dan Teknologi)
Padang, 4 – 5 September 2018 ISSN Media Elektronik 2597-3584

Pengamanan Data User Login dengan Algoritma Kriptografi Tea dan Notifikasi SMS

Siswanto[a], M.Anif[b], Ulil Abshor[c]
[a]Prodi Teknik Informatika, Fakultas Teknologi Informasi,Universitas Budi Luhur, siswantobl@gmail.com
[b]Prodi Teknik Informatika, Fakultas Teknologi Informasi,Universitas Budi Luhur, m.anif91@gmail.com
[c]Prodi Teknik Informatika, Fakultas Teknologi Informasi,Universitas Budi Luhur, ulil.abshor93@gmail.com

Abstract

Application of user login data security is designed to secure user login user data at PT. TELKOM Indonesia TBK, HSI Division in Minitools application containing data from customer's internet number. The security of user logni data is very vulnerable to the theft of various irresponsible parties that will impact on the manipulation of customer data in the Minitools application. These problems can be encountered by adding applications to prevent irresponsible parties from being able to read passwords from user login data in the database. In addition, by adding SMS notification feature to prevent irresponsible parties are free to use user login data to access and change customer data on Minitools application. In this paper the algorithm used in cryptography, the cryptography algorithm Tiny Encryption Algorithm (TEA). For SMS notification itself, built using Gammu module as a special software aids SMS Gateway, PHP, and also Wavecom GSM M1306B modem. The result of this cryptographic testing, password data can be secured in the form of text encrypted (ciphertext). With the application of data security user cryptographic login and SMS notification for this login system will make the information system more secure because the password will be encrypted and the authentication code to login to the application Minitools sent to the user's mobile number. From the experimental results, the average duration of the encrypt process is 0.08361488 ms and the duration of the descrypt process is 0.166120556 ms. For the average sms the duration is not more than 10 second.

Keywords: TEA Cryptography Algorithm, Minitools Application, User Login Data, SMS Notification, PHP

Abstrak

Aplikasi pengamanan data user login ini dirancang untuk mengamankan data user login karyawan pada PT. TELKOM Indonesia TBK, Divisi HSI pada aplikasi Minitools yang berisi data dari nomor internet pelanggan. Keamanan data user logni sangat rentan terhadap pencurian dari berbagai pihak yang tidak bertanggung jawab yang akan berimbas pada manipulasi data pelanggan di aplikasi Minitools tersebut. Permasalahan tersebut dapat dihadapi dengan menambahkan aplikasi untuk mencegah pihak yang tidak bertanggung jawab dapat membaca password dari data user login di database. Selain itu dengan menambahkan fitur notifikasi SMS untuk mencegah pihak yang tidak bertanggung jawab bebas menggunakan data user login untuk mengakses dan merubah data pelanggan pada aplikasi Minitools. Dalam penulisan ini algoritma yang digunakan dalam kriptografi, yaitu algoritma kriptografi Tiny Encryption Algorithm (TEA). Untuk notifikasi SMS sendiri, dibangun menggunakan modul Gammu sebagai software bantu khusus SMS Gateway, PHP, dan juga modem Wavecom GSM M1306B. Hasil dari pengujian kriptografi ini, data password dapat diamankan berupa teks tersandi (ciphertext). Dengan adanya aplikasi pengamanan data user login kriptografi dan notifikasi SMS untuk sistem login ini maka akan membuat sistem informasi lebih aman karena password akan dienkrip dan kode otentikasi untuk login ke aplikasi Minitools dikirimkan ke nomor handphone user. Dari hasil percobaan didapatkan rata-rata durasi proses encrypt adalah 0.08361488 ms dan durasi proses descrypt adalah 0.166120556 ms. Untuk pengiriman sms rata-rata durasi adalah tidak lebih dari 10 second.

Kata kunci: Algoritma Kriptografi TEA, Aplikasi Minitools, Data User Login, Notifikasi SMS, PHP.

1. Pendahuluan

IndiHome merupakan layanan internet dari Telkom. Menggunakan teknologi Fiber Optik (FO) IndiHome mampu menyediakan koneksi internet yang lebih. Teknologi fiber merupakan media yang tidak diragukan untuk menyediakan *bandwidth* dengan jumlah besar. Ini karena tidak dipengaruhi interferensi gelombang elektromagnetik.

Divisi HSI sendiri memiliki pelanggan yang cukup banyak, dimana pada setiap jaringan memungkinkan akan terjadinya kesalahan. Dikarenakan adanya masalah tersebut, maka solusi yang tepat adalah dengan memonitor gangguan internet yang masuk dari pelanggan, lalu kemudian gangguan dilaporkan kepada para teknisi di lapangan untuk memperbaiki gangguan yang terjadi pada jaringan sisi pelanggan. Berdasarkan permasalahan yang ada, PT. TELKOM TBK, Divisi HSI membutuhkan aplikasi yang mampu memberikan hasil audit penanganan gangguan jaringan *High Speed Internet* yang cepat dan tepat serta bisa diakses oleh *user* di internal Telkom.

Minitools yang dikembangkan oleh Pihak PT. TELKOM Indonesia TBK, memiliki Fungsi umum yakni untuk mengetahui Data Pemakaian (*Usage*) pelanggan, melihat status Persiapan untuk Pasang Baru, mengetahui Status Nomor Internet Pelanggan dan melihat data IP pelanggan. Dengan adanya aplikasi Minitools ini mampu membantu pihak PT. TELKOM Indonesia TBK, dalam mengelola data dari nomor internet pelanggan dan menampilkannya dalam laporan pada aplikasi Minitools.

Karena banyaknya pihak yang kurang bertanggung jawab ingin bebas mengakses aplikasi Minitools, dan merubah data pada aplikasi Minitools. Maka keamanan data *user login* kru HSI pada aplikasi Minitools menjadi sangat rentan terhadap pencurian oleh pihak yang kurang bertanggung jawab. Permasalahan tersebut dapat diatasi dengan menambahkan aplikasi untuk mencegah pihak yang tidak bertanggung jawab dapat membaca *password* dari data *user login* di *database*. Selain itu dengan menambahkan pengiriman sms kode otentikasi pada saat melakukan *login* ke handphone user. Dengan itu, diharapkan tidak adanya lagi pencurian data user login kru HSI pada aplikasi Minitools dan pemakaian aplikasi Minitools untuk karyawan/kru PT. Telkom Indonesia sesuai dengan peran divisi masing-masing.

2. Tinjauan Pustaka

2.1 Pengertian *Tiny Encryption Algorithm*

Tiny Encryption Algorithm (TEA) adalah algoritma sandi yang diciptakan oleh David Wheeler dan Roger Needham dari Computer Laboratory, Cambridge University, England pada bulan November tahun 1994. Algoritma ini merupakan algoritma penyandian *block cipher* yang dirancang untuk penggunaan memori yang seminimal mungkin dengan kecepatan proses yang maksimal.[1]

Sistem penyandian TEA menambahkan fungsi matematik berupa penambahan dan pengurangan sebagai operator pembalik selain XOR. Pergeseran dua arah (ke kiri dan ke kanan) dimaksudkan agar semua bit kunci dan data bercampur secara berulang-ulang. Algotima TEA memproses 64-bit input sekali waktu pemrosesan dan menghasilkan 64-bit output. TEA menyimpan 64-bit input tersebut kedalam L0 dan R0 yang masing masing berjumlah 32-bit. Sedangkan 128-bit kunci disimpan kedalam k(0), k(1), k(2), dan k(3) yang masing masing berisi 32-bit. Teknik ini diharapkan cukup dapat mencegah penggunaan teknik *exshautive search* secara efektif. Hasil outputnya akan disimpan dalam L16 dan R16.[2].

2.2 Langkah- Langkah Penyandian Dengan Algoritma TEA Dalam Dua Ronde (Satu *Cycle)*

Berikut beberapa langkah penyandian dengan algoritma TEA dalam dua ronde (satu cycle) :[3]

a. Pergeseran (*shift*)

Blok teks terang yang masing masing sebanyak 32-bit pada kedua sisi yang akan digeser kekiri sebanyak 4 kali dan kemudian digeser ke kanan sebanyak 5 kali.

b. Penambahan

Setelah proses pergeseran kekiri dan kekanan, maka variabel Y dan Z akan ditambahkan dengan kunci k(0)-k(3). Sedangkan untuk variabel Y dan Z awal akan ditambahkan dengan sum (delta).

c. Peng-XOR-an

Selanjutnya adalah proses peng-XOR-an dengan rumus untuk satu round seperti rumus (1) dan (2).

y[i] = y + (((ROL4 z) + K0) ^ (z + sum) ^ ((ROL5 z) + K1))…….(1)
z[i] = z + (((ROL4 y) + K2) ^ (y + sum) ^ ((ROL5 y) + K3))……..(2)

Dalam hal ini sum= sum+delta. Hasil penyandian dalam satu *cycle* satu blok teks 64-bit menjadi 64-bit teks sandi adalah dengan cara menggabungkan variabel y dan variabel z. Untuk proses penyandian pada *cycle* selanjutnya, variabel y dan variabel z ditukar posisinya, sehingga y1 menjadi z1 dan z1 menjadi y1 lalu dilanjutkan proses seperti langkah-langkah di atas tadi sampai dengan 16 *cycle* (32 *round*).

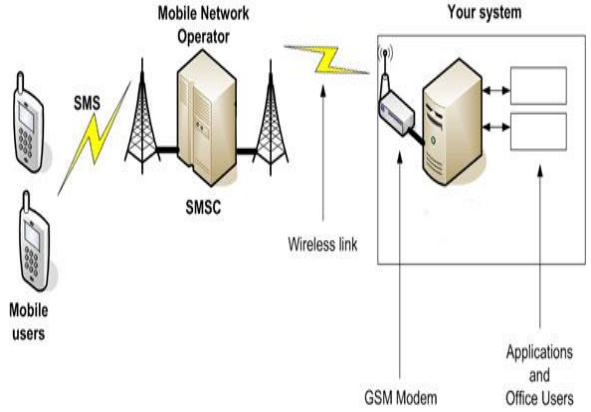
d. *Key Schedule*

Key Schedule pada algoritma TEA sangat sederhana. Untuk kunci k(0) dan k(1) konstan digunakan untuk

round ganjil saja, sedangkan untuk kunci k(2) dan k(3) konstan digunakan untuk round genap. [3][4]

2.3 *Cara kerja SMS gateway*

Cara kerja SMS *gateway* seperti gambar 1, pada dasarnya hampir sama dengan mengirimkan SMS melalui *handphone* pada umumnya. Hanya saja, bedanya adalah perangkat pengirimnya bukan lagi *handphone*, tetapi modem GSM. Dan moden inilah yang dikendalikan oleh PC menggunakan aplikasi SMS *gateway* yang akan dibuat.[5]



Gambar 1. Cara Kerja SMS Gateway

GAMMU (GNU *All Mobile Management Utilities*) merupakan *software* yang digunakan sebagai *tool* untuk mengembangkan aplikasi berbasis SMS *Gateway*, cukup mudah untuk diimplementasikan, dan juga tidak berbayar. Kelebihan GAMMU dari tool SMS *gateway* lainnya adalah :[5]

a. GAMMU dapat dijalankan di sistem operasi Linux maupun Windows.
b. Banyak *device* yang kompatibel di GAMMU.
c. GAMMU menggunakan *database* MySQL untuk menyimpan SMS yang ada pada kotak masuk (*inbox*) maupun untuk mengirim pesan, sehingga dapat dibuat *interface* yang berbasis web maupun desktop.
d. Baik kabel data USB maupun serial, semuanya kompatibel di GAMMU.

2.4 Penelitian Sebelumnya

Pada penelitian sebelumnya terdapat penelitian dimana algoritma yang digunakan adalah algoritma *Tiny Encryption Algorithm*. TEA merupakan algoritma jenis *stream cipher* yang memproses unit input data. algoritma *Tiny Encryption Algorithm* (TEA) juga merupakan bagian dari algoritma simetris, dimana proses enkripsi dan dekripsinya memiliki kunci yang sama. Pembuatan aplikasi ini menggunakan bahasa pemograman C#. Hasil yang akan dicapai dari penilitian ini adalah aplikasi kriptografi dokumen yang bisa melakukan enkripsi dan dekripsi dengan algoritma *Tiny Encryption Algorithm* (TEA) [6].

Pada penelitian lain, algoritma *Cryptographic* yang akan digunakan adalah Algoritma Enkripsi *Tiny Encryption Algorithm* (TEA), sedangkan algoritma steganografi yang akan digunakan adalah *Least Significant Bit* (LSB), data atau informasi yang pertama dienkripsi menjadi TEH, kemudian dimasukkan ke dalam gambar oleh algoritma LSB. Jadi hasil enkripsi dan steganografi tidak akan mencurigakan bagi yang lain, berdasarkan testing, perubahan gambar tidak terlihat. Oleh karena itu dapat disimpulkan dengan menggabungkan *Cryptography* TEA dan steganografi LSB, sehingga pengacakkan data akan lebih akurat dan kinerja program yang baik [6][7].

Penelitian lainnya membuat sistem yang berfokus pada implementasi FPGA ringan algoritma kriptografi enkripsi algoritma TEA untuk beradaptasi dengan banyak kendala *real time* seperti memori, kehilangan data dan biaya rendah. Skema yang diusulkan menggunakan *Linear Feedback Shift Register* untuk menghasilkan kunci acak, sehingga lebih aman untuk transfer informasi sensitif di banyak aplikasi *real time* [8][9]

Penelitian lain mengimplementasikan algoritma enkripsi yang digunakan untuk keamanan lebih komunikasi nirkabel, tetapi mengamankan data juga mengkonsumsi sumber daya. Faktor penting utama yang perlu dipertimbangkan ketika merancang sistem kriptografi adalah kinerja, kecepatan, ukuran, dan keamanan. *Tiny Encryption Algorithm* (TEA), dan *eXtended TEA* (XTEA) adalah contoh dari algoritma kriptografi.[9] *Tiny Encryption Algorithm* (TEA) adalah algoritma kriptografi yang dirancang untuk meminimalkan pemakaian memori dan memaksimalkan kecepatan. Ini adalah jenis *cipher feistel* yang menggunakan operasi dari campuran (*orthogonal*) kelompok aljabar [10][11].

3. Metodologi Penelitian

Dalam penyusunan laporan tulisan ilmiah ini telah dilakukan penelitian untuk memperoleh fakta dan juga data yang diperlukan. Adapun metode yang digunakan adalah metode waterfall dengan langkah–langkah, sebagai berikut :

3.1 Menganalisis masalah, kebutuhan, keperluan, dan penggunaan apa saja yang akan diperlukan untuk pengamanan data *user login* di PT. TELKOM Indonesia TBK, *Divisi High Speed Internet*.

3.2 Metode pengumpulan data yang digunakan, diantaranya yaitu :

1) Perencanaan, mengidentifikasi masalah-masalah keamanan data *user login* pada aplikasi Minitools di PT. TELKOM Indonesia TBK, Divisi High Speed Internet.

2) Penelitian lapangan, yaitu melakukan observasi atau praktek lapangan secara langsung di perusahaan terkait guna mendapatkan data yang akurat dan dapat dipertanggung jawabkan keabsahannya. Adapun teknik pengumpulan data yang digunakan yaitu:
   a) Studi lapangan, yaitu penelitian langsung di PT. TELKOM Indonesia TBK, Divisi *High Speed Internet* (HSI) untuk mendapatkan data serta informasi yang dibutuhkan.
   b) Pengamatan, yaitu teknik pengumpulan data dengan mengamati langsung cara kerja dari aplikasi Minitools PT. TELKOM Indonesia TBK, Divisi High Speed Internet.
   c) Metode wawancara, ialah proses tanya jawab langsung kepada orang yang memahami dan mengetahui secara langsung tentang permasalahan yang sedang diamati .

3.3 Studi Literatur, Mempelajari referensi atau sumber-sumber yang berkaitan dengan algoritma kriptografi TEA, SMS, SMS *Gateway, GAMMU.*

3.4 Desain Sistem, membuat desain system yang akan dibuat, dari desain awal hingga akhir agar memudahkan dalam merelisasikan Aplikasi SMS Gateway pada form *login* aplikasi Minitools.

3.5 Implementasi, mengimplementasikan rancangan yang telah dibuat pada tahap perancangan sistem ke dalam perangkat lunak komputer dengan menggunakan bahasa pemrograman PHP.

3.6 Ujicoba program, menguji kinerja program, apakah program berjalan dengan baik atau belum. Jika belum, maka akan dilakukan perbaikan pada tahap implementasi.

3.7 Melakukan Simulasi, kegiatan simulasi berupa pengujian program secara nyata yang melibatkan kru PT.TELKOM Indonesia TBK, Divisi High Speed Internet.

3.8 Dokumentasi, melakukan penulisan hasil sistem yang telah dibangun ke dalam sebuah laporan.

4. Hasil dan Pembahasan

4.1 *Pseudo Code* Proses *Encrypt Tiny Encryption Algorithm* (TEA)

TEA menggunakan 64 bits block size dan menggunakan 128-bits key dan melakukan 32 putaran proses yang sama. TEA adalah cipher yang menggunakan iterasi dengan variable i, tiap putaran mempunyai input y [i-1] dan z [i-1] yang didapat dari putaran sebelumnya. Untuk subkey K[i] didapatkan dari 128 bits key dan menggunakan delta (∂).Delta ini didapat dari rasio emas (*golden number ratio*) untuk memastikan *subkey* sulit diketahui.

Nilai dari delta (rasio emas) didapat dari fungsi berikut ini :

$\partial = (\sqrt{5} - 1) * 231 = 9E3779B9$ (dalam bentuk hexadecimal)

Pseudo code proses *encrypt* algoritma TEA adalah sebagai berikut:

```
1   START
2     INSERT plaintext
3     INSERT secret key (16 chr)
4     DO key schedule   //split key menjadi 4 subkey [K0 –K3]
5       i = 1, str = panjang dari plaintext
6      SPLIT (plaintext/8 chr ) ← block//text dikelompokan per 8 chr
7       IF ( i ≤ str )THEN
8       SPLIT (block / 4 chr ) ← P
9           P = y,z
10          delta = 9E3779B9, n = 1, sum  = delta
            IF ( n ≤ 32 ) THEN
11          y+(((ROL4 z)+K0) XOR (z+sum) XOR ((ROR5 z) + K1))
            ← y
12          z+(((ROL4 y)+K2) XOR (y+sum) XOR ((ROR5 y) + K3))
            ← z
13          n = n + 1, sum = sum + delta
14      ELSE
15              i = i + 8
16              JOIN all cipher ← ciphertext
17          ENDIF
18      ELSE
19          PRINT ciphertext
20      ENDIF
21    END
22    Return
```

Sedangkan untuk *pseudo code decrypt TEA*, sebagai berikut :

```
1   START
2     INSERT ciphertext
3     INSERT secret key (16 chr)
4     DO key schedule   //split key menjadi 4 subkey [K0 –K3]
5       i = 1, str = ciphertext length
6     SPLIT ciphertext/8 chr ← block   //text dikelompokan per 8 chr
7     IF ( i ≤ str ) THEN
8           SPLIT block / 4 chr ← C
9           c = y,z
10          delta = 9E3779B9, n = 1, sum = C6EF3720
11          IF ( n ≤ 32 ) THEN
12              z-(((ROL4 y)+K2) XOR (y+sum) XOR ((ROR5 y) +
                K3)) ← z
13              y-(((ROL4 z)+K0) XOR (z+sum) XOR ((ROR5 z) +
                K1)) ← y
14              n = n + 1, sum = sum - delta
15          ELSE
16              i = i + 8
17              JOIN all plain ← plaintext
18          ENDIF
19      ELSE
20          PRINT plaintext
21      ENDIF
22  END
23   Return
```

Contoh perhitungan proses *encrypt TEA* satu putaran dengan :

Plaintext = uL1l4bSh

Secret key = T3LK0M1ND0N3S1@!

Proses subtitusi key :

T	3	L	K	0	M	1	N	D	0	N	3	S	1	@	!
a		b		c		d		e		f		g		h	

⇓

@	!	T	3	S	1	L	K	N	3	0	M	D	0	1	N
h		a		g		b		f		c		e		d	

Proses *subkey* :

@	!	T	3	S	1	L	K	N	3	0	M	D	0	1	N
K0				K1				K2				K3			
Bentuk ACII *(hexadecimal)* :															
40215433				53314C4B				4E33304D				4430314E			

Split *plaintext* menjadi y dan z :

u	L	1	l	4	b	S	h
75	4C	31	6C	34	62	53	68
y				z			

=> y = 754C316C z = 34625368

y= 754C316C (11101010100110000110001011011 00)
z= 34625368 (10100011000100101001101101000)
K0=40215433(10000000010000101010100000110011)
K1=53314C4B(10100110011000101001100010 0101)
K2=4E33304D(10011100011001100110000010 0110)
K3=4430314E(10001000011000000110001010011 10)

Proses penghitungan encrypt TEA :
y[1] = y + (((ROL4 z) + K0) ^ (z + sum) ^ ((ROR5 z) + K1))
y[1]= 754C316C + (((ROL4 34625368) + 40215433) XOR (34625368 + 9E3779B9) XOR ((ROL5 34625368) + 53314C4B))
y[1]= 11101010100110000110001011011 00 +
(((ROL411101010100110000110001011011 00) +
10000000010000101010100000110011)
XOR(10100011000100101001101101000+
10011110001101110111100110111001)XOR ((ROL5
11010001100010010100110110100 0) +
10100110011000101001100010010 11))
y[1]= 11101010100110000110001011011 00 +
((10101001100001100010111011001110 +
10000000010000101010100000110011)XOR
(11010010100110011100110100100001) XOR
((01000110100011000100101001101 1) +
10100110011000101001100010010 11))
y[1]= 11101010100110000110001011011 00 +
(10010100111001000110101100000001 XOR
11010010100110011100110100100001 XOR
11001001101010001011110111001 10)
y[1]= 11101010100110000110001011011 00+
10001010101001111110001100 0110
y[1]= 10010111111101100010101000110010
y[1]= 97F62A32 // hexadecimal
z[1] = z + (((ROL4 y1) + K2) ^ (y1 + sum) ^ ((ROR5 y1) + K3))
z[1]= 34625368 + (((ROL4 97F62A32) + 4E33304D) XOR (97F62A32 + 9E3779B9) XOR ((ROR5 97F62A32) + 4E444949))
z[1]= 11010001100010010100110110100 0 + (((ROL4
10010111111101100010101000110010) +
10011100011001100110000010011 01) XOR
(11010001100010010100110110100 0 +
10011110001101110111100110111001) XOR ((ROR5
10010111111101100010101000110010) +
10001000011000000110001010011 10))
z[1]= 11010001100010010100110110100 0 +
((01111111011000101010001100101001 +
10011100011001100110000010011 01) XOR
(11010010100110011100110100100001) XOR
(10010100101111111011000101010001 +
10001000011000000110001010011 10))
z[1]= 11010001100010010100110110100 0 +
(11001101100101011101001101110110 XOR
11010010100110011100110100100001 XOR
11011000111011111110001010011111)
z[1]= 11010001100010010100110110100 0 +
11000111111000111111110011001000
z[1]= 11111100010001100101000000110000
z[1]= FC465030 // hexadecimal

Jadi untuk hasil *encrypt* 1 putaran TEA dengan *Plaintext* = uL1l4bSh dan *Secret key* = T3LK0M1ND0N3S1@! adalah 97F62A32FC465030 (dalam bentuk *hexadecimal*).

Pada bagian ini akan dijelaskan langkah-langkah dalam proses pengujian mulai dari tahap pengujian *register* , proses *encrypt password*, lalu pengujian *login* dengan notifikasi sms kedalam aplikasi yang telah dibuat. Pengujian aplikasi pengamanan data *user login* diawali dengan melakukan *register* di form *register* yang telah disediakan, seperti gambar 3.

Gambar 3. Tampilan proses daftar

Munculnya *alert* notifikasi pada sisi atas halaman web yang memberikan informasi bahwa *password* telah berhasil dienkrip dan hasil dari proses *encrypt* seperti pada gambar 4.

Gambar 4. Tampilan notifikasi hasil proses encrypt

4.2 Hasil Pengujian

Berikut adalah hasil pengujian dari beberapa proses seperti tabel 1.

Tabel 1. Tabel hasil uji coba proses encrypt

Pengujian ke-	Nama User	Tipe	Panjang *Password as Plaintext (character)*	Durasi (ms)
1	ARIE NALA CANDRA	huruf (A-Z, a-z), Angka (0-9)	14	0.145001984
2	MAOLANA SWARGOASTO	huruf (A-Z, a-z)	14	0.143002129
3	RIZKY TRI ANUGRAH	huruf (A-Z, a-z), Angka (0-9)	16	0.149901867
4	BAYU SEPTI K	huruf (A-Z, a-z), Angka (0-9)	9	0.0330019
5	MUADZIN ARZI	huruf (A-Z, a-z), Angka (0-9)	10	0.050003052
6	SURYO PRASETYO	huruf (A-Z, a-z)	11	0.057003021
7	ULIL ABSHOR	huruf (A-Z, a-z), Angka (0-9)	12	0.049003124
8	BUDI SANTOSO	huruf (A-Z, a-z), Angka (0-9)	12	0.042001963
Rata-rata durasi proses encrypt				0.08361488

Bahwa dengan jumlah karakter yang berbeda proses enkripsi tetap bisa dilakukan dengan waktu rata-rata: 0,08361488 ms. Sehingga dapat dikatakan bahwa proses enkripsi password ke database bekerja dengan baik. Dengan waktu tersebut maka user tidak membutuhkan waktu yang lama pada proses enkripsi password.

Tabel 2. Tabel hasil uji coba proses pengiriman sms

Pengujian ke-	Nama User	No. Handphone	Durasi pengiriman sms dr profider TELKOMSEL ke- (s)		
			XL	INDOSAT	TELKOMSEL
1	ARIE NALA CANDRA	0813-8856-7825			5.107293
2	MAOLANA SWARGOASTO	0851-0268-8602			6.510487
3	RIZKY TRI ANUGRAH	0877-7731-4044	8.43513		
4	BAYU SEPTI K	0812-9662-0077			9.182526
5	MUADZIN ARZI	0877-8177-3659	9.312533		
6	SURYO PRASETYO	0815-8615-2001		8.390249	
7	ULIL ABSHOR	0812-4141-0915			5.178296
8	BUDI SANTOSO	0856-9106-4858		8.613642	
Rata-rata durasi pengiriman sms ke user			8.873832	8.501945	6.49465

Seperti Tabel 2 diketahui bahwa, meskipun *profider* yang di gunakan oleh user berbeda-beda, proses pengiriman tetap bisa dilakukan dengan waktu rata-rata 6.49465 - 8.873832 detik. Sehingga dapat dikatakan bahwa proses pengiriman sms kode otentikasi ke *user* bekerja dengan baik. Dengan waktu tersebut maka *user* tidak membutuhkan waktu yang lama untuk mendapatkan kode otentikasi dan menyelesaikan proses login.

Tabel 3. Tabel hasil uji coba proses decrypt

Pengujian ke-	Nama User	Tipe	Panjang *Ciphertext (character)*	Durasi (ms)
1	ARIE NALA CANDRA	Kode ASCII (A-Z, a-z, 0-9, symbols)	14	0.157003975
2	MAOLANA SWARGOASTO	Kode ASCII (A-Z, a-z, 0-9, symbols)	14	0.197011948
3	BUDI SANTOSO	Kode ASCII (A-Z, a-z, 0-9, symbols)	12	0.166008949
4	RIZKY TRI ANUGRAH	Kode ASCII (A-Z, a-z, 0-9, symbols)	16	0.160889728
5	BAYU SEPTI K	Kode ASCII (A-Z, a-z, 0-9, symbols)	9	0.143020887
6	MUADZIN ARZI	Kode ASCII (A-Z, a-z, 0-9, symbols)	10	0.157008886
7	SURYO PRASETYO	Kode ASCII (A-Z, a-z, 0-9, symbols)	11	0.158009052
8	ULIL ABSHOR	Kode ASCII (A-Z, a-z, 0-9, symbols)	12	0.190011024
Rata-rata durasi proses decrypt				0.166120556

Proses dekripsi seperti tabel 3 tetap bisa dilakukan dengan waktu rata-rata 0,166120556 ms. Sehingga dapat dikatakan bahwa proses enkripsi password ke *database* bekerja dengan baik.

5. Kesimpulan Dan Saran

Simpulan dan saran yang dapat diambil dari penelitian ini:

5.1 Simpulan

Simpulan yang dapat diambil dari hasil penelitian ini:

a. Pengamanan password dapat diamankan dengan algoritma kriptografi *Tea.*
b. Program sistem keamanan data user login pada aplikasi Minitools dengan sistem kriptografi algoritma *Tea* dan notifikasi sms telah diuji coba, sehingga program dinyatakan sudah sesuai.
c. Rata-rata durasi proses *encrypt* adalah 0.08361488 ms
d. Rata-rata durasi proses *descrypt* adalah 0.166120556 ms
e. Rata-rata durasi proses pengiriman sms dari *profider* TELKOMSEL ke sesama TELKOMSEL adalah 6.494650483 *second*
f. Rata-rata durasi proses pengiriman sms dari *profider* TELKOMSEL ke *profider* INDOSAT adalah 8.501945496 *second*
g. Rata-rata durasi proses pengiriman sms dari profider TELKOMSEL ke *profider* XL adalah 8.873831511 *second*
h. Proses pengiriman sms kode otentikasi tergantung dengan sinyal *profider* yang digunakan, sehingga proses pengiriman sms kode otentikasi bisa cepat, lama atau bahkan sms tidak diterima oleh *user*.

5.2 Saran

Berdasarkan dari pengalaman yang telah dilakukan dalam penelitian ini, terdapat beberapa saran untuk pengembangan sistem selanjutnya, diantaranya :

a. Pengamanan password dapat diamankan dengan algoritma kriptografi stream cipher atau digital signature.
b. Proses pengiriman kode otentikasi melalui whatsapps dan twitter yang tidak tergantung dengan sinyal *profider* yang digunakan, sehingga proses pengiriman kode otentikasi bisa cepat diterima oleh *user*.

6. Daftar Rujukan

[1] Siswanto, M. Anif, dan Windu Gata, 2018. *Penerapan Algoritma Kriptografi TEA Dan Base64 Untuk Mengamankan Email Data Policy Asuransi* Jurnal ELTIKOM, ISSN 2598-3245(Print)ISSN 598-3288 (Online), Vol. 2 No. 1, Juni 2018, pp.31-46.

[2] Nugroho, Sandromedo C. 2013, *Algoritma Tea (Tiny Encryption Algorithm)*, Available at: https://kriptologi.wordpress.com/2008/10/03/algoritma-tea-tiny-encryption-algorithm/. [Accessed 16 November 2017].
[3] Kumar, Kiran V. G, et al. 2015, *Design And Implementation Of Tiny Encryption Algorithm. International Journal of Engineering Research and Applications*, ISSN : 2248-9622 Vol. 5, Issue 6, pp.94-97
[4] Qamal, Mukti, 2014. *Kriptografi File Citra Menggunakan Algoritma Tea (Tiny Encryption Algorithm)*, Jurnal Techsi Vol. 5 No. 2 Oktober 2014. pp. 11-33.
[5] Irmayani, 2012. *Implementasi Sms Gateway Untuk Layanan Informasi Absensi Pegawai*, Available at: http://repository.usu.ac.id/handle/123456789/33822. [Accessed 14 November 2017].
[6] Nurdin,2013. *Implementasi Algoritma TEA Dan Fungsi HASH MD4 Untu Enkripsi Dan Dekripsi Data*, Journal TECHSI, (e-ISSN:2614-6029, p-ISSN:2302-4836). DOI: https://doi.org/10.29103/techsi.v5i1.143Vol 5, No 1, 2013, pp. 97-112.
[7] Maharani, Helen S. 2014. *Implementasi Kombinasi Tiny Encryption Algorithm (TEA) Dan Algoritma Least Significant Bit (LSB) Untuk Keamanan File Tex*t, Medan : Universitas Sumatera Utara.
[8] M. Shoeb and V. K. Gupta, 2013. *A Crypt Analysis Of The Tiny Encryption Algorithm In Key Generation*, International Journal of Communication and Computer Technologies, ISSN: 2278-9723, Vol. 01, No. 38, Issue 05, pp. 123-128.
[9] Setiawan, Iwan, 2017. *Aplikasi Kriptografi Dengan Algoritma Tiny Encryption Algorithm Menggunakan Microsoft Visual Basic*, Jakarta: Universitas Mercu Buana,.
[10] Setyawan, Ryan Ari, Sulistyo, Selo, dan Hantono, Bimo Sunafri, 2014. *Algoritma Kriptografi Untuk Pengembangan Aplikasi Telepon Anti Sadap di Android*, CITEE 2014, ISSN:2085-6350/ISBN:978-602-71396-1-9, Yogyakarta, 7-8 Oktober 2014, pp.53-58.
[11] R. Khoirianti, N. Hidayah, and V. Widyaningsih, 2014. *Implementasi Algoritma Tea Untuk Enkripsi Dan Dekripsi Menggunakan Bahasa Pemrograman Visual Basic*, Academia, 2014.