MODIFIKASI METODE NIHILIST CIPHER DENGAN PENDEKATAN KEYSTREAM GENERATOR YANG DITERAPKAN PADA PENYANDIAN SISTEM LOGIN

SKRIPSI

Oleh:

HARIS MUNANDAR
NIM. 1410000358

JENJANG PENDIDIKAN STRATA-1
PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNIK DAN ILMU KOMPUTER
UNIVERSITAS POTENSI UTAMA
MEDAN
2018

LEMBAR PENGESAHAN

MODIFIKASI METODE NIHILIST CIPHER DENGAN PENDEKATAN KEYSTREAM GENERATOR YANG DITERAPKAN PADA PENYANDIAN SISTEM LOGIN

SKRIPSI

Diajukan untuk Melengkapi Persyaratan Guna
Mendapatkan Gelar Strata Satu
Program Studi Teknik Informatika

HARIS MUNANDAR
NIM. 1410000358

Disetujui Oleh :

Pembimbing I	Pembimbing II
(Budi Triandi, M.Kom)	(Yustriza, M.Kom)
Penguji I	**Penguji II**
(Iwan Fitrianto Rahmad, M.Kom)	(Hardianto, M.Kom)

Medan, 03 Oktober 2018
Diketahui dan Disahkan Oleh :

Dekan Fakultas Teknik dan Ilmu Komputer	Ketua Program Studi
(Ratih Puspasari, M.Kom)	(Budi Triandi, M.Kom)

LEMBAR PERSETUJUAN SIDANG SKRIPSI II

MODIFIKASI METODE NIHILIST CIPHER DENGAN PENDEKATAN KEYSTREAM GENERATOR YANG DITERAPKAN PADA PENYANDIAN SISTEM LOGIN

Yang Dipersiapkan Dan Disusun Oleh :

HARIS MUNANDAR
NIM. 1410000358

Telah Memenuhi Persyaratan Untuk Dipertuhankan
Didepan Dewan Penguji Pada Ujian Sidang Skripsi

Disetujui Oleh :

Pembimbing I	Pembimbing II
(Budi Triandi, M.Kom)	(Yustrizal, M.Kom)

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNIK DAN ILMU KOMPUTER
UNIVERSITAS POTENSI UTAMA
MEDAN
2018

	DOKUMEN LEVEL FORM	NO. DOKUMEN F-FTIK-18-09
	JUDUL JADWAL BIMBINGAN SKRIPSI	Tanggal Terbit : 05 Desember 2016 Tanggal Efektif : 10 Desember 2016
		Halaman : 1 dari 2
	AREA PROGRAM STUDI	NO.REVISI 02

JADWAL BIMBINGAN SKRIPSI

Nama Mahasiswa : Huris Munandar
NIM : 1410000358
Program Studi : Teknik Informatika
Judul : Modifikasi Metode Nihilist Cipher Dengan Pendekatan Keystream Generator Yang Diterapakan Pada Penyandian Sistem Login

NO	TANGGAL	MATERI BIMBINGAN	T. TANGAN PEMBIMBING
1	23/1/2018	Revisi Proposal	
2	30/1/2018	Revisi Proposal	
3	6/2/2018	Acc Proposal	
4	6/2/2018	Revisi Bab I	
5	12/2/2018	Acc Bab I	
6	21/2/2018	Revisi Bab II	
7	22/2/2018	Revisi Bab II	
8	23/2/2018	Acc Bab II	
9	28/2/2018	Revisi Bab III	
10	6/3/2018	Revisi Bab III	
11	21/3/2018	Acc Bab III	
12	25/7/2018	Revisi Bab IV	
13	14/8/2018	Revisi Bab IV	
14	16/8/2018	Revisi Bab IV	
15	23/8/2018	Acc Bab IV	

Ketua Program Studi

(Budi Triandi, M.Kom)

Dosen Pembimbing I

(Budi Triandi, M.Kom)

	DOKUMEN LEVEL FORM	NO. DOKUMEN F-FTIK-18-09
JUDUL JADWAL BIMBINGAN SKRIPSI		Tanggal Terbit : 05 Desember 2016 Tanggal Efektif : 10 Desember 2016
AREA PROGRAM STUDI		Halaman : 2 dari 3 NO.REVISI 02

JADWAL BIMBINGAN SKRIPSI

Nama Mahasiswa : Haris Munandar
NIM : 1410000358
Program Studi : Teknik Informatika
Judul : Modifikasi Metode Nihilist Cipher Dengan Pendekatan Keystream Generator Yang Diterapakan Pada Penyandian Sistem Login

NO	TANGGAL	MATERI BIMBINGAN	T. TANGAN PEMBIMBING
1	23/9/2018	Revisi Bab V	
2	30/8/2018	Acc Bab V	
3	31/8/2018	Acc kelengkapan.	
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			

Ketua Program Studi

(Budi Triandi, M.Kom)

Dosen Pembimbing I

(Budi Triandi, M.Kom)

	DOKUMEN LEVEL FORM	NO. DOKUMEN F-FTIK-18-09
	JUDUL JADWAL BIMBINGAN SKRIPSI	Tanggal Terbit : 05 Desember 2016 Tanggal Efektif : 10 Desember 2016
	AREA PROGRAM STUDI	Halaman : 1 dari 1 NO.REVISI 02

JADWAL BIMBINGAN SKRIPSI

Nama Mahasiswa : Haris Munandar

NIM : 1410000358

Program Studi : Teknik Informatika

Judul Skripsi : Modifikasi Metode Nihilist Cipher Dengan Pendekatan Keystream Generator Yang Diterapkan Pada Penyandian Sistem Login

NO	TANGGAL	MATERI BIMBINGAN	T. TANGAN PEMBIMBING
1	5/2-2018	Revisi Proposal	
2	7/2-2018	ACC Proposal	
3	7/2-2018	Revisi BAB I	
4	14/2-2018	ACC Perbaikan BAB I	
5	20/2-2018	Perbaikan BAB II	
6	27/2-2018	ACC Perbaikan BAB II	
7	28/2-2018	Revisi BAB III	
8	22/3-2018	ACC Perbaikan BAB III	
9	6/8-2018	ACC BAB IV	
10	27/8-2018	ACC BAB V	
11	31/8-2018	ACC Keseluruhan	
12			
13			
14			
15			

Ketua Program Studi

(Budi Triandi, M.Kom)

Dosen Pembimbing II

(Yusfrizal, M.Kom)

SKRIPSI

Diajukan untuk Memenuhi Salah Satu Syarat

Memperoleh Gelar Sarjana Komputer

LEMBAR PENGAKUAN

"Saya akui karya ini adalah hasil kerja keras saya dan usaha saya sendiri kecuali kutipan dan ringkasan yang masing-masing telah saya jelaskan sumbernya"

Tanda tangan	:	
Nim	:	1410000358
Nama Penulis	:	Haris Munandar
Tanggal	:	28 Februari 2018

Alhamdulillah, atas rahmat dan hidayah-Nya, saya dapat menyelesaikan skripsi ini dengan baik. Karya sederhana ini ku persembahkan untuk:

Kedua orang tua ku, ayah dan ibu Tercinta yang tak pernah lelah membesarkan ku dengan penuh kasih sayang, serta memberi dukungan, perjuangan, motivasi dan pengorbanan dalam hidup ini.

Teman seperjuangan (TIF-A, TIF-B, TIF-C Pagi) yang selalu memberi semangat dan dukungan serta canda tawa yang sangat mengesankan selama masa perkuliahan, susah senang dirasakan bersama dan sahabat-sahabat seperjuanganku yang lain yang tidak bisa disebutkan satu-persatu. Terima kasih buat kalian semua.

"Kesalahan bukan kegagalan tapi bukti bahwa seseorang sudah melakukan sesuatu"

ABSTRAK

Pada sebuah sistem biasanya ditemukan adanya sistem login untuk mencegah orang-orang yang tidak memiliki hak akses masuk dan mencuri informasi dari sebuah sistem tersebut. Sistem komputer dapat diserang oleh pihak ketiga dengan menggunakan cara-cara yang sangat berbahaya. Jenis-jenis serangan komputer antara lain virus, exploit, worm, spyware, adware, malware, trojan horse, rootkit, spam, hoax, key logging, phishing, Denial of Service dan Man-in-The-Middle. Oleh karena itu dibutuhkan sebuah teknik yang dapat mengatasi kecurian informasi melalui sistem login. Dengan mengamankan isi dari database sistem login, maka pencuri informasi tidak dapat masuk ke dalam sistem. Sistem yang peneliti usulkan yaitu Modifikasi Metode Nihilist Cipher Dengan Pendekatan Keystream Generator Yang Diterapkan Pada Penyandian Sistem Login. Dengan adanya sistem tersebut maka, masalah keamanan sistem login dapat teratasi.

***Kata Kunci** : Sistem Login, Keystream Generator, Nihilist Cipher.*

ABSTRACT

In a system usually found a login system to prevent people who do not have access rights and steal information from a system. Computer systems can be attacked by third parties using very dangerous methods. Types of computer attacks include viruses, exploits, worms, spyware, adware, malware, Trojan horses, rootkits, spam, hoaxes, key logging, phishing, Denial of Service and Man-in-The-Middle. Therefore we need a technique that can overcome the theft of information through a login system. By securing the contents of the login system database, information thieves cannot enter the system. The system that the researchers propose is the Modification of the Nihilist Cipher Method with the Generator Keystream Approach Applied to the Login System Encryption. Using this system, the login system security problem can be resolved.

Key Word : *Login System, Keystream Generator, Nihilist Cipher.*

KATA PENGANTAR

Assalamu'alaikum Warahmatullahi Wabarakatuh.

Alhamdulillah penulis ucapkan puji syukur atas kehadirat Allah SWT yang telah memberikan kesehatan dan kesempatan kepada penulis sehingga penulis dapat melaksanakan dan menyelesaikan skripsi ini. Adapun judul penulisan skripsi yang penulis buat ini adalah **"Modifikasi Metode *Nihilist Cipher* Dengan Pendekatan Keystream Generator Yang Diterapkan Pada Penyandian Sistem Login".**

Penulisan skripsi ini merupakan syarat untuk menyelesaikan Pendidikan Strata Satu (S1) program studi Teknik Informatika pada Universitas Potensi Utama. Namun demikian penulisan skripsi ini bukan hanya sekedar "syarat" belaka, tetapi juga merupakan suatu aplikasi nyata terhadap ilmu pengetahuan yang telah penulis dapat selama mengikuti perkuliahan. Selain itu, penulisan skripsi ini juga sebagai bahan pembelajaran bagi penulis, khususnya dalam hal penulisan karya ilmiah.

Puji dan syukur, akhirnya penulis mampu menyelesaikan penulisan skripsi ini. Penulis akhirnya menyampaikan terima kasih kepada berbagai pihak yang turut membantu penyelesaian skripsi ini baik langsung maupun tidak langsung. Ucapan terima kasih ini penulis sampaikan kepada :

1. Bapak Budi Triandi, M.Kom, selaku Dosen Pembimbing I sekaligus Ketua program Studi Teknik Informatika Universitas Potensi Utama Medan yang

telah begitu banyak memberikan bimbingan, arahan dan masukan serta meluangkan waktunya selama penyusunan skripsi ini.

2. Bapak Yusfrizal, M.Kom, Selaku Dosen Pembimbing II yang telah mengajarkan banyak ilmu dan tata cara penulisan skripsi yang baik dan benar.
3. Ibu Hj. Nuriandy, B.A, selaku Pembina Yayasan Universitas Potensi Utama Medan.
4. Bapak H. Bob Subhan Riza, ST, M.Kom, selaku Ketua Yayasan Universitas Potensi Utama Medan.
5. Ibu Dr. Rika Rosnelly, S.Kom, M.kom, selaku Rektor Universitas Potensi Utama Medan.
6. Ibu Lili Tanti, M.Kom, selaku Wakil Rektor I Universitas Potensi Utama Medan.
7. Ibu Ratih Puspasari, M.Kom, selaku Dekan Fakultas Teknik dan Ilmu Komputer Potensi Utama Medan.
8. Seluruh Dosen di Universitas Potensi Utama Medan yang telah memberikan ilmu dan nasihatnya kepada penulis.
9. Teristimewa buat Orang tua tercinta Ibu dan Ayah, yang telah membimbing dan telah memberikan dorongan dan bantuan baik do'a maupun material sehingga penulis dapat menyelesaikan tugas akhir ini.
10. Kepada Aruna Syifa Almira yang slalu bisa diandalkan dalam suka duka, memberikan dukungan dan motivasi kepada penulis untuk tetap semangat dalam menyelesaikan penulisan skripsi ini.

11. Buat saudara - saudara penulis yang telah memberikan dukungan dan motivasi kepada penulis untuk tetap semangat dalam menyelesaikan penulisan skripsi Ini.
12. Kepada teman-teman penulis kelas TIF-B Pagi dan TIF-E Pagi Angkatan 2014 yang sama-sama dengan penulis berjuang untuk menyelesaikan skripsi ini dan banyak membantu penulis.

Penulis menyadari masih banyak kekurangan di dalam skripsi ini. Untuk itu penulis mengharapkan kritik dan saran agar nantinya skripsi ini dapat lebih sempurna lagi dan bermanfaat bagi para pembaca ataupun yang membutuhkan, terutama bagi para mahasiswa Universitas Potensi Utama.

Medan, 31 Maret 2018
Penulis

(Haris Munandar)
1410000357

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR LAMPIRAN

BAB I

PENDAHULUAN

BAB I

PENDAHULUAN

I.1. Latar Belakang

Keamanan pada sebuah data dan informasi sangatlah penting. Oleh karena itu keamanan harus diterapkan pada sebuah data dan informasi. Di dalam penyimpanan data dan informasi, keamanan dalam sebuah data dan informasi tidak terjamin dari adanya pencuri informasi. Data dapat didefenisikan sebagai kenyataan yang digambarkan oleh nilai, bilangan-bilangan, untaian karakter atau simbol-simbol yang membawa arti tertentu. Informasi sendiri dapat didefenisikan sebagai hasil dari pengolahan data dalam bentuk yang lebih berguna bagi penerimaanya, yang digunakan sebagai alat bantu dalam pengambilan. (Sitohang, 2013 : 2). Masalah keamanan merupakan salah satu aspek penting dari sebuah sistem informasi. Sayang sekali masalah keamanan ini sering kali kurang mendapat perhatian dari para pemilik dan pengelola sistem informasi. Seringkali masalah keamanan berada di urutan kedua, atau bahkan di urutan terakhir dalam daftar hal-hal yang dianggap penting. Apabila menggangu performansi dari sistem, seringkali keamanan dikurangi atau ditiadakan. (Sholeh, dkk, 2013 : 2). Pada sebuah sistem biasanya ditemukan adanya sistem *login* untuk mencegah orang-orang yang tidak memiliki hak akses masuk dan mencuri informasi dari sebuah sistem tersebut. Sistem komputer dapat diserang oleh pihak ketiga dengan menggunakan cara-cara yang sangat berbahaya. Jenis-jenis serangan komputer antara lain *virus*, *exploit*, *worm*, *spyware*, *adware*, *malware*, *trojan horse*, *rootkit*,

spam, *hoax*, *key logging*, *phishing*, *Denial of Service* dan *Man-in-The-Middle*. Oleh karena itu dibutuhkan sebuah teknik yang dapat mengatasi kecurian informasi melalui sistem *login*. Dengan mengamankan isi dari *database* sistem *login*, maka pencuri informasi tidak dapat masuk ke dalam sistem.

Teknik yang peneliti usulkan yaitu kriptografi. Kriptografi merupakan suatu bidang ilmu yang mempelajari tentang bagaimana merahasiakan suatu informasi penting ke dalam suatu bentuk yang tidak dapat dibaca oleh siapapun serta mengembalikannya kembali menjadi informasi semula dengan menggunakan berbagai macam teknik yang telah ada sehingga informasi tersebut tidak dapat diketahui oleh pihak manapun yang bukan pemilik atau yang tidak berkepentingan. Sisi lain dari kriptografi ialah kriptanalisis (*Cryptanalysis*) yang merupakan studi tentang bagaimana memecahkan mekanisme kriptografi. (Sitohang, 2013 : 3). Kriptografi merupakan langkah-langkah logis bagaimana menyembunyikan pesan dari orang-orang yang tidak berhak atas pesan tersebut dengan melakukan pembangkitan kunci, enkripsi dan dekripsi. Kriptografi bertujuan untuk memberi layanan keamanan (yang juga dinamakan sebagai aspek-aspek keamanan). (Sholeh, dkk, 2013 : 2). Namun untuk dapat menggunakan teknik kriptografi, maka dibutuhkan metode yang tepat untuk mendapatkan hasil yang baik. Peneliti mengusulkan metode *Nihilist cipher*, *Nihilist cipher* pertama kali dikembangkan oleh para *Russian Nihilist*, yaitu orang-orang Rusia yang mendukung cara kekerasan untuk mencapai perubahan politik yang diinginkan, dalam hal ini menggulingkan kekuasaan Tsar Alexander II di Rusia. Mereka memanfaatkan algoritma *Nihilist* untuk berkomunikasi dan mengorganisasikan para teroris untuk

melawan para pendukung Tsar pada tahun 1880-an. Selain itu, algoritma ini juga banyak digunakan oleh *First Chief Directorate*, sebuah divisi dari KGB (badan intelejen Rusia) untuk berkomunikasi para calon mata-mata mereka. Serta digunakan pula untuk berkomunikasi dengan para sekutu mereka. Dengan diterapkan cara tersebut maka kecurian data dan informasi dapat di atasi. (Mukhlis, 2013 : 2). Dengan latar belakang tersebut maka penulis menyimpulkan judul **"Modifikasi Metode Nihilist Cipher Dengan Pendekatan Keystream Generator Yang Diterapkan Pada Penyandian Sistem Login".**

I.2. Ruang Lingkup Permasalahan

Ruang lingkup permasalahan yang terdapat pada penelitian ini berdasarkan latar belakang adalah sebagai berikut :

I.2.1. Identifikasi Masalah

Identifikasi masalah dari penulis untuk penelitian ini yaitu :

1. Sistem *login* tidak aman dari pencuri data dan informasi.
2. Belum ada penyandian metode *Nihilist Cipher* terhadap sistem *login*.
3. Belum ada penyandian metode *Nihilist Cipher* dengan pendekatan *keystream generator* terhadap sistem *login.*
4. Belum ada aplikasi modifikasi metode *Nihilist Cipher* dengan pendekatan *Keystream Generator* yang diterapkan pada penyandian sistem *login.*

I.2.2. Perumusan Masalah

Perumusan masalah yang terdapat pada penelitian ini yaitu :

1. Bagaimana mengamankan sistem *login* dari pencuri data dan informasi ?

2. Bagaimana metode *Nihilist Cipher* dapat mengamankan sistem *login* dari pencuri data dan informasi ?
3. Bagaimana modifikasi metode *Nihilist Cipher* dengan pendekatan *Keystream Generator* yang diterapkan pada penyandian sistem *login* ?
4. Bagaimana menghasilkan aplikasi modifikasi metode *Nihilist Cipher* dengan pendekatan *Keystream Generator* yang diterapkan pada penyandian sistem *login* ?

I.2.3. Batasan Masalah

Agar pembahasan masalah tidak melebar penulis membatasi masalah sebagai berikut :

1. Aplikasi untuk menyandikan sistem *login*.
2. *Input* aplikasi ini pesan teks sistem *login*.
3. *Output* aplikasi ini berupa teks sistem *login* terenkripsi.
4. Pembuatan aplikasi ini menggunakan bahasa pemrograman PHP, HTML, CSS, *Javascript* dan menggunakan *database* MySQL.
5. Perancangan aplikasi ini menggunakan pemodelan UML.
6. Metode *Nihilist Cipher* hanya menggunakan huruf besar untuk pesan dan kunci.

I.3. Tujuan Dan Manfaat

I.3.1. Tujuan

Tujuan dari penelitian ini yaitu :

1. Mengamankan sistem *login* dari pencuri data dan informasi.

2. Metode *Nihilist Cipher* dapat mengamankan sistem *login* dari pencuri data dan informasi.
3. Memodifikasi metode *Nihilist Cipher* dengan pendekatan *Keystream Generator* yang diterapkan pada penyandian sistem *login***.**
4. Menghasilkan aplikasi modifikasi metode *Nihilist Cipher* dengan pendekatan *Keystream Generator* yang diterapkan pada penyandian sistem *login***.**

I.3.2. Manfaat

Manfaat dari penelitian ini yaitu :

1. Penggunaan aplikasi sistem *login* menjadi lebih aman.
2. Memahami penggunaan metode *Nihilist Cpher* dalam mengamankan sistem *login*.
3. Mengetahui dan memahami hasil modifikasi metode *Nihilist Cipher* dengan pendekatan *Keystream Generator* yang diterapkan pada penyandian sistem *login*.
4. Mendapat wawasan dalam pembuatan perangkat lunak kriptografi.

I.4. Metodologi Penelitian

Metode merupakan suatu cara yang sistematik untuk mengerjakan suatu permasalahan. Berikut ini adalah tahapan-tahapan penelitian yang peneliti lakukan untuk menyelesaikan penelitian.

I.4.1. Pengumpulan Data

Pengumpulan data yang peneliti lakukan menggunakan beberapa teknik ataupun cara sebagai berikut :

1. Angket

   Peneliti menulis dan menyusun daftar pertanyaan yang akan diajukan kepada beberapa responden untuk mendapatkan informasi mengenai penelitian.

2. Tanya Jawab

   Peneliti melakukan tanya jawab kepada responden ahli kriptografi mengenai penelitian ini untuk mendapatkan data-data yang sesuai.

3. Sampel

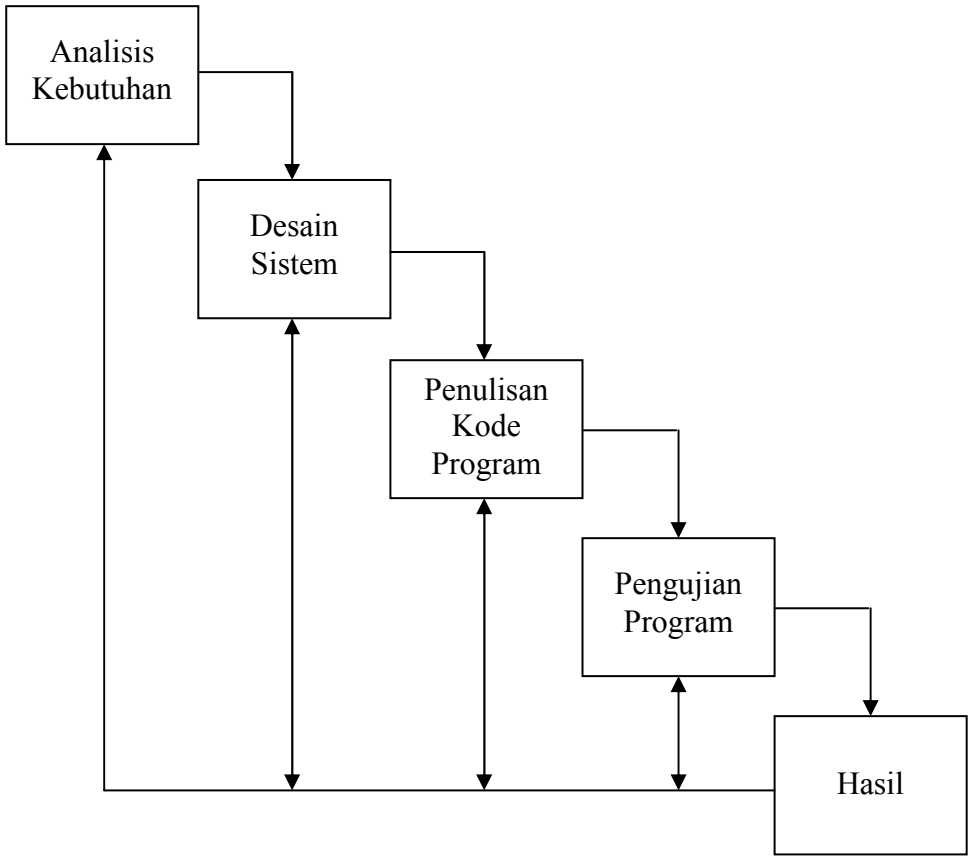
   Peneliti mengumpulkan contoh-contoh ataupun sampel-sampel untuk dijadikan bahan untuk penelitian.

4. Penelitian Kepustakaan

   Peneliti menggunakan referensi untuk teori-teori yang berkaitan dengan penelitian. Referensi tersebut berupa buku, jurnal, karya ilmiah dan lain sebagainya.

I.4.2. *Waterfall* Metode Penelitian

Metode merupakan suatu cara yang sistematik untuk mengerjakan suatu permasalahan. Penelitian ini akan melalui beberapa tahapan. Tahapan dalam penelitian ini dapat di modelkan pada diagram *waterfall*. Adapun beberapa tahapan yang digunakan dalam penelitian ini adalah sebagai berikut :



Gambar I.1. Diagram *Waterfall* Metodologi Penelitian

Keterangan :

1. Analisa Kebutuhan

Peneliti menganalisa kebutuhan yang diperlukan untuk mencapai tujuan penelitian yang akan dilakukan. Pada tahap ini dilakukan pengumpulan data-data tentang kriptografi.

Berikut ini adalah kebutuhan *hardware* untuk penelitian ini :

a. *Laptop* minimal spesifikasi core 2

b. *Hardisk* minimal 150Gb

c. RAM minimal 2Gb

Berikut ini adalah kebutuhan *software* untuk penelitian ini :

a. *Notepad* ++

b. XAMPP

Berikut ini adalah kebutuhan referensi untuk penelitian ini :

a. Jurnal

b. Buku

2. Desain Sistem

Pada tahap ini dilakukan desain sistem menggunakan pemodelan UML yaitu *use case diagram*, *class diagram*, *activity diagram* dan *sequence diagram*.

3. Penulisan Kode Program

Penulisan kode program diterapkan pada beberapa bahasa pemrograman antara lain HTML, PHP, MySQL.

4. Pengujian Program

Pengujian program dilakukan untuk mengetahui hasil dari perancangan sistem yang telah dibuat dan untuk mengetahui kekurangan sistem. Apabila terdapat kekurangan sistem atau program tidak berjalan dengan baik, maka akan dilakukan perbaikan sampai seluruh program berjalan dengan baik. Pengujian secara teori menggunakan *blackbox testing* dan pengujian secara praktek menggunakan *web browser.*

5. Hasil

Pada tahapan ini penelitian sudah memiliki sistem yang sesuai dengan perencanaan awal yaitu penelitian ini menghasilkan aplikasi yang dapat mengamankan sistem *login* menggunakan metode *Nihilist Cipher* dan

menghasilkan Metode *Nihilist Cipher* Dengan Pendekatan *Keystream Generator* yang diterapkan pada *database* MySQL menggunakan pemrograman PHP.

I.5. Kontribusi Penelitian

Kontribusi penelitian mengenai penelitian yang penulis buat, dapat dilihat dan dibandingkan dari beberapa jurnal yang terdapat pada tabel I.1. kontribusi penelitian.

Tabel I.1. Kontribusi Penelitian

No	Nama/ Tahun	Referensi	Judul	Hasil Penelitian
1.	Mukhlis (2013)	Jurnal	Modifikasi Nihilist Chiper	Algoritma ini cukup kuat pada beberapa serangan seperti ciphertext-only attack,plaintext-only attack, chosen-plaintext attack. Algorima ini lebih kompleks karena menggunakan bilangan M.
2.	Sholeh, dkk (2013)	Jurnal	Mengamankan Skrip Pada Bahasa Pemrograman PHP Dengan Menggunakan Kriptografi Base64	Dengan adanya cara pengamanan ini, pengembang aplikasi yang menggunakan bahasa pemograman PHP dapat menyembunyikan skrip php supaya tidak mudah disalin, diubah sebagian/ seluruhnya oleh orang yang tidak berhak.

Berdasarkan tabel I.1. kontribusi penelitian tidak ditemukan adanya kesamaan judul dan sistem dengan penelitian ini. Tabel I.1. kontribusi penelitian dapat digunakan untuk tambahan referensi untuk penelitian ini.

I.6. Sistematika Penulisan

Adapun sistematika penulisan yang diajukan dalam skripsi ini adalah sebagai berikut :

BAB I : PENDAHULUAN

Pada bab ini menerangkan tentang latar belakang, ruang lingkup permasalahan, tujuan dan manfaat, metode penelitian dan sistematika penulisan.

BAB II : TINJAUAN PUSTAKA

Pada bab ini menerangkan teori dasar yang berhubungan dengan program yang dirancang serta bahasa pemrograman yang digunakan.

BAB III : ANALISA DAN DESAIN SISTEM

Pada bab ini mengemukakan analisa masalah program yang akan dirancang dan rancangan program yang digunakan pada penulisan skripsi ini.

BAB IV : HASIL DAN PEMBAHASAN

Pada bab ini mengemukakan tentang hasil implementasi sistem yang dirancang mencakup uji coba sistem, tampilan serta perangkat yang dibutuhkan. Analisa sistem dirancang untuk mengetahui kelebihan dan kekurangan sistem yang dibuat.

BAB V : KESIMPULAN DAN SARAN

Dalam bab ini berisikan berbagai kesimpulan dan saran yang dapat dibuat berdasarkan uraian yang telah disimpulkan.

BAB II

TINJAUAN PUSTAKA

BAB II

TINJAUAN PUSTAKA

II.1. Penelitian Terdahulu

Penelitian yang dilakukan oleh Sholeh, dkk (2013) mengenai Mengamankan Skrip Pada Bahasa Pemograman PHP Dengan Menggunakan Kriptografi Base64, Sholeh, dkk (2013) menyimpulkan bahwa dengan adanya cara pengamanan ini, pengembang aplikasi yang menggunakan bahasa pemograman PHP dapat menyembunyikan skrip PHP supaya tidak mudah disalin, diubah sebagian/ seluruhnya oleh orang yang tidak berhak.

Penelitian yang dilakukan oleh Mukhlis (2013) mengenai Modifikasi *Nihilist Cipher*, Mukhlis menyimpulkan bahwa Algoritma ini cukup kuat pada beberapaserangan seperti *ciphertext-only attack*,*plaintext-only attack*, *chosen-plaintext attack*. Algorima ini lebih kompleks karenamenggunakan bilangan *M*.

Berdasarkan kedua penelitian di atas maka tidak ditemukan adanya kesamaan judul dan sistem pada penelitian ini, oleh karena itu referensi dari kedua penelitian di atas dapat digunakan sebagai referensi untuk penelitian ini.

II.2. Landasan Teori

II.2.1. Aplikasi

Aplikasi adalah penerapan dari rancang sistem untuk mengolah data yang menggunakan aturan atau ketentuan bahasa pemrograman tertentu. Aplikasi adalah Program yang dibuat oleh manusia yang berfungsi untuk menyelesaikan permasalahan-permasalahan masalah yang akan dihadapi. (Zulfauzi, 2015 : 57).

II.2.2. Keamanan Jaringan

Untuk mewujudkan layanan keamanan jaringan pengembang sistem dapat menggunakan mekanisme keamanan jaringan. Rekomendasi ITU-T(X.800) juga mendefinisikan beberapa mekanisme keamanan jaringan. Berikut ini adalah beberapa jenis mekanisme keamanan jaringan :

1. *Encipherment*

Encipherment merupakan mekanisme keamanan jaringan yang digunakan untuk menyembunyikan data. Mekanisme *Encipherment* dapat menyediakan layanan kerahasiaan data (*confidentiality)* meskipun dapat juga digunakan untuk layanan lainnya. Untuk mewujudkan mekanisme *Encipherment* teknik kriptografi dan steganografi dapat digunakan. Kriptografi merupakan kumpulan teknik untuk menyembunyikan pesan dengan mengubah pesan ini menjadi pesan tersembunyi. Sedangkan steganografi merupakan kumpulan teknik untuk menyembunyikan pesan pada media lain misalnya gambar, suara, atau video.

2. Keutuhan Data

Mekanisme keutuhan data digunakan untuk memastikan keutuhan data pada unit data atau pada suatu aliran (*stream)* data unit. Cara yang digunakan adalah dengan menambahkan nilai penguji (*check value)* pada data asli. Jadi jika sebuah data akan dikirim nilai penguji dihitung terlebih dahulu dan kemudian data dan penguji dikirim bersamaan. Penerima dapat menguji apakah ada perubahan data atau tidak dengan cara menghitung nilai penguji data yang dikirim dan membandingkan nilai penguji yang dihitung dengan nilai penguji yang dikirim bersamaan data asli. Bila sama penerima dapat menyimpulkan data tidak berubah.

3. *Digital Signature*

Digital Signature merupakan mekanisme keamanan jaringan yang menyediakan cara bagi pengirim data untuk "menandatangani" secara elektronik sebuah data dan penerima dapat memverifikasi "tanda tangan" itu secara elektronik. *Digital Signature* ditambahkan pada data unit dan digunakan sebagai bukti pengirim dan menghindari pemalsuan (*forgery)* tanda tangan.

4. *Authentication Exchange*

Mekanisme ini memberikan cara agar dua entitas dapat saling meng-otentikasi dengan cara bertukar pesan untuk saling membuktikan identitas.

5. *Traffic Padding*

Traffic Padding menyediakan cara untuk pencegahan analisis lalu lintas data pada jaringan yaitu dengan menambah data palsu pada lalu lintas data.

6. *Routing Control*

Routing Control menyediakan cara untuk memilih dan secara terus menerus mengubah alur (*rote)* pada jaringan komputer antara pengirim dan penerima. Mekanisme ini menghindarkan komunikasi dari penguping (*eavedropper).*

7. Notarisasi

Notarisasi (*notarizatio)* menyediakan cara untuk memilih pihak ketiga yang terpercaya sebagai pengendali komunikasi antar pengirim dan penerima.

8. Mekanisme Kendali Akses

Mekanisme kendali akses memberikan cara bagi penggna untuk memperoleh hak akses sebuah data. Misalnya dengan tabel relasi pengguna dan otoritasinya (kemampuan aksesnya).

Hubungan antar mekanisme dan layanan jaringan menjelaskan bahwa untuk mewujudkan sebuah layanan keamanan jaringan dibutuhkan mekanisme yang tepat dan tidak semua mekanisme keamanan jarinagn digunakan untuk mewujudkan sebuah layanan keamanan jaringan. Misalnya untuk otentikasi diperlukan beberapa mekanisme keamanan jaringan yaitu *encipherment, digital signature, dan authentication exchanges*. Ketika melakukan analisis kebutuhan terhadap keamanan jaringan, pengembang harus cermat memilih layanan keamanan jaringan yang tepat untuk memenuhi kebutuhan itu. (Sadikin, 2017 : 5).

II.2.2.1. Serangan Keamanan Jaringan

Sistem keamanan jaringan yang dioperasionalkan pada jaringan publik rentan terhadap serangan oleh siapapun. Orang yang berusaha meruntuhkan keamanan jaringan disebut sebagai penyerang (penyerang). Penyerang menyerang sistem keamanan jaringan untuk mengalahkan tujuan layanan keamanan jaringan. Misalnya penyerang pada layanan kerahaisaan data ingin mengungkap isi teks asli sehingga iadapat mengungkap teks sandi lainnya. Secara umum serangan pada sistem keamanan jaringan dapat dikatagorikan menjadi 2 jenis : serangan pasif (*passive attack*) dan serangan aktif (*active attack*).

1. Serangan Pasif

Pada serangan pasif, penyerang hanya mengumpulkan data yang melintas pada jaringan publik (jaringan yang bisa diakses oleh penyerang). Serangan pasif tidak melakukan modifikasi data yang melintas atau merusak sistem, penyerang hanya punya keamanan membaca saja (*read only*). Lalu berdasarkan data yang dikumpulkan, penyerang melakukan analisis untuk mengagalkan tujuan layanan

keamanan jaringan. Karena tidak melakukan perubahan data dan menganggu sistem, serangan pasif susah untuk dideteksi namun serangan pasif dapat dicegah dengancra misalnya selalu menggunakan sandi (*encryption)* ketika pengirim pesan. Oleh karena itu, penekanan untuk mengatasi serangan pasif lebih pada pencegahan daripada pendeteksian. Berikut ini beberapa jenis serangan yang digolongkan sebagai serangan pasif .

a. *Snooping*

Snooping merujuk pada kegiatan yang bermasksud mendapatkan data yang tengah terkirim pada jaringan biasanya melalui akses yang tak berwenang. Contoh aktivitas *Snooping* misalnya sebuah email disadap oleh penyerang. Untuk mengalahkan penyerang sehingga aktivitas *Snooping* tidak bermakna data yang dikirim dibuat tidak kaset mata(*monintelligible*)dengan menggunakan mekanisme penyandian (*encipherment*).

b. *Traffic Analysis*

*Traffic Analysis*merupakan kegiatan serangan pasif dengan melakukan *monitoring* terhadap lalu lintas data pada jaringan. Data-data lalu lintas jaringan dikumpulkan dan kemudian dianalisis sehingga penyerang dapat mengetahui maksud data-data itu. (Sadikin, 2017 : 7).

2. Serangan Aktif

Sebuah serangan aktif (*active attack*) dapat mengakibatkan perubahan data yang terkirim dan jalannya sistem terganggu. Pada serangan aktif seakan-akan penyerang memperoleh kemampuanan untuk mengubah data pada lalu lintas data selain kemampuan baca. Jens-jenis serangan aktif adalah sebagai berikut:

a. *Masquerade*

Masquerade adalah seranagn aktif yang dilakukan oleh penyerang dengan cara penyerang mengambil alih (menirukan) perilaku pengirim atau penerima. Misalnya pada saat Alice ingin membuat kunci bersama dengan Bob, Eve mengambil alih peran Bob sehingga Alice tidak sadar bahwa ia mengirim psean ke Eve bukan pada Bob.

b. *Modification*

Modification adalah serangan aktif yang dilakukan oleh penyerang dengan cara penyerang mengambil alih jalur komunikasi untuk mengubah atau menghapus atau menunda pesan yang sedang dikirim untuk keuntungan penyerang. Contohnya sebuah pesan "Kirim 1000 ke Akun Alice" diubah oleh Eve menjadi "Kirim 10000 ke Akun Eve".

c. *Replay*

Replay adalah serangan aktif yang terdiri atas pencatatan secara pasif data unit dan transmisi ulang untuk menimbulkan efek yang diinginkan penyerang. Contohnya Eve pernah meminta Bob mengirim 10000 ke Eve, lalu Bob mengirim pesan "Kirim 10000 ke Eve" ke Bank, Eve mencatat pesan "Kirim 10000 ke Eve" dan mengirim ulang ke Bank.

d. *Denial Of Service*

Denial Of Service adalah serangan aktif yang bertujuan agar sistem menjadi collapse sehingga tidak mampu memberikan respon atau layan yang semestinya kepada pengguna. Serangan ini biasanya dilakukan dengan membuat *server* menjadi *overload* dengan permintaan bodong (*dummy*). Untuk mengembangkan

sistem keaman jarinagn yang aman, perancang keamanan jarinagn harus menganalisis kemungkinan serangan-serangan atas layanan keaman jaringan. Biasanya sebuah sistem keamanan jaringan dikatakan aman bila sistem itu mampu bertahan terhadap serangan aktif. (Sadikin, 2017 : 8).

II.2.3. Kriptografi

Kriptografi pada awalnya dijabarkan sebagai ilmu yang mempelajari bagaimana menyembunyikan pesan. Namun pada pengertian modern kriptografi adalah ilmu yang bersandarkan pada teknik matematika untuk berurusan dengan keamanan informasi seperti kerahasian, keutuhan data dan otrntikasi entitas. Jadi pengertian kriptografi modern adalah tidak saja berurusan hanya dengan penyembunyian keamanan informasi. Berikut adalah beberapa rangkuman yang berkembang pada kriptografi modern.

1. Fungsi *Hash.* Fungsi *Hash* adalah fungsi yang melakukan pemetaan pesan dengan panjang sembarang ke sebuah teks khusus yang sisebut *message digest* degan panjang tetap. Fungsi *Hash* umumnya dipakai sebagai nilai uji *check value*) pada mekanisme keutuhan data.
2. Penyandian dengan kunci simetrik (*symmetric key encipherment*). Penyandian kunci dengan simetrik adalah penyandian yang kunci enkripsi dan kunci deskripsi bernilai sama. Kunci pada penyandian simetrik diasumsikan bersifat rahasia hanya piahak yang melakukan enkripsi dan deskripsi yang mengetahui nilainya. Oleh karena itu penyadian dengan kunci simetrik disebut juga penyandian dengan kunci rahasia *secret key encipherment.*

Penyandian dengan kunci asimetrik (A*symmetric key encipherment*). Penyandian dengan kunci asimetrik atau sering juga disebut kunci publik (*public key*) adalah Penyandian dengan enkripsi dan deskripsi berbeda nilai. Kunci enkripsi disebut dengan kunci publik (*public key*) bersifat terbuka. Sedangkan, kunci deskripsi disebut privat (*private key*) bersifat tertutup/rahasia. (Sadikin, 2017 : 9).

II.2.3.1. Jenis-JenisKriptografi

Berikut ini adalah pembagian kriptografi menurut Sadikin (2017 : 9) :

1. Kriptografi Klasik

Kriptografi klasik merupakan kriptografi yang digunakan pada zaman dahulu sebelum komputer ditemukan atau sudah ditemukan namun belum secanggih sekarang. Kriptografi ini melakukan pengacakan huruf pada kata terang / *plaintext.* Kriptografi ini hanya melakukan pengacakan pada huruf A - Z, dan sangatlah tidak disarankan untuk mengamankan informasi-informasi penting karena dapat dipecahkan dalam waktu singkat. Biarpun telah ditinggalkan, kriptografi klasik tetap dapat ditemui disetiap pelajaran kriptografi sebagai pengantar kriptografi modern.Semenjak ditemukannya komputer digital, metode kriptografi klasik yang bekerja dengan mengacak huruf semakin kehilangan posisinya dan digantikan dengan metode yang lebih baru, dimana yang diacak adalah bit dari huruf bersangkutan. Era kriptografi modern pun dimulai.

Berdasarkan teknik pengenkripsian, kriptografi klasik terbagi menjadi 2 yaitu:

a. Metode substitusi, yang dibagi lagi menjadi 2 yaitu:
    1. *Monoalphabetic*, setiap huruf pesan disubstitusi oleh satu huruf kunci

2. *Polyalphabetic*, setiap huruf pesan disubstitusi oleh beberapa huruf kunci dengan pola tertentu.

Metode substitusi adalah metode enkripsi dengan mengganti tiap-tiap huruf pesan dengan kunci tertentu menjadi huruf lain.

b. Metode transposisi

Metode transposisi adalah metode enkripsi dengan memindahkan posisi tiap-tiap huruf pesan dengan pola tertentu. Contohnya adalah *Blocking Cipher* dan *Permutation*.

2. Kriptografi Modern

Kriptografi modern menggunakan gagasan dasar yang sama seperti kriptografi klasik (permutasi dan transposisi) tetapi penekanannya berbeda. Pada kriptografi klasik, kriptografer menggunakan algoritma yang sederhana, yang memungkinkan cipherteks dapat dipecahkan dangan mudah (melalui penggunaan statistik, terkaan, intuisi, dan sebagainya). Algoritma kriptografi modern dibuat sedemikian kompleks sedemikian sehingga kriptanalis sangat sulit memecahkan cipherteks tanpa mengetahui kunci.

Algoritma kriptografi modern umumnya beroperasi dalam mode bit ketimbang mode karakter. Operasi dalam mode *bit* berarti semua data dan informasi (baik kunci, plainteks, maupun cipherteks) dinyatakan dalam rangkaian (string) bit biner, 0 dan 1. Algoritma enkripsi dan dekripsi memproses semua data dan informasi dalam bentuk rangkaian *bit*. Rangkaian *bit* yang menyatakan plainteks dienkripsi menjadi cipherteks dalam bentuk rangkaian *bit*, demikian sebaliknya. Berikut ini adalah jenis-jenis kriptografi modern :

a. Fungsi *Hash*

   Fungsi *hash* adalah fungsi yang melakukan pemetaan npesan dengan panjang sembarang ke sebuah teks khusus yang disebut *message digest* dengan panjang tetap. Fungsi *hash* umumnya dipakai sebagai nilai uji (*check value*) pada mekanisme keutuhan data.

b. Penyandian dengan kunci simetrik (*Symmetric Key Encipherment*)

   Penyandian dengan kunci simetrik adalah penyandian yang kunci enkripsi dan kunci simetrik adalah penyandian yang kunci enkripsi dan kunci dekripsi bernilai sama. Kunci pada penyandian simetrik diasumsikan bersifat rahasia hanya pihak yang melakukan enkripsi dan dekripsi yang mengetahui nilainya. Oleh karena itu penyandian dengan kunci simetrik disebut juga penyandian dengan kunci rahasia *secret key encipherment*.

II.2.4. Metode *Nihilist Cipher*

Nihilist cipher pertama kali dikembangkan oleh para*Russian Nihilist*, yaitu orang-orang Rusia yangmendukung cara kekerasan untuk mencapaiperubahan politik yang diinginkan, dalam hal inimenggulingkan kekuasaan Tsar Alexander II diRusia.

Mereka memanfaatkan algoritma *Nihilist*untuk berkomunikasi dan mengorganisasikan parateroris untuk melawan para pendukung Tsar pada tahun 1880-an.Selain itu, algoritma ini juga banyak digunakan oleh*First Chief Directorate*, sebuah divisi dari KGB(badan intelejen Rusia) untuk berkomunikasi paracalon mata-mata mereka. Serta digunakan pulauntuk berkomunikasi dengan para sekutu mereka. Dengan diterapkan cara tersebut maka kecurian pesan dapat

di atasi. (Mukhlis, 2013 :2). Berikut ini adalah langkah-langkah metode *Nihilist Cipher*.

a. Langkah I:

Persiapkan 2 kata kunci, dengan syarat:

a. Kata Kunci I : ≤ 25 huruf

b. Kata Kunci II : ≤ plainteks

b. Langkah II:

Misalkan, kata kunci I adalah KUNCI, masukkankata ini ke dalam baris I *Polybius Square*, kemudiandiikuti dengan huruf lainnya yang belum ada dalamkata kunci :

Tabel II.1. Tabel kunci

	1	**2**	**3**	**4**	**5**
1	K	U	N	C	I
2	A	B	D	E	F
3	G	H	L	M	O
4	P	Q	R	S	T
5	V	W	X	Y	Z

c. Langkah III:

Lalu, misalkan kata kunci II adalah KRIPTO,kemudian berdasarkan tabel kunci diatas maka,koordinat yang berkoresponden dengan kata kunci :

K	R	I	P	T	O
11	43	15	41	45	35

Gambar II.1. Koordinat Kata Kunci II

d. Langkah IV:

Misalkan plainteksnya adalah MATA KULIAH,kemudian lakukan langkah III pada plainteks, sehingga :

M	A	T	A	K	U	L	I	A	H
34	21	45	21	11	12	33	15	21	32

Gambar II.2. Koordinat Plainteks

e. Langkah V:

Lakukan operasi pertambahan antara koordinatplainteks dengan kata kunci II, sehingga akan didapat *cipherteks* :

kt	11	43	15	41	45	35	11	43	15	41
pt	34	21	45	21	11	12	33	15	21	32
ct	45	64	60	62	56	47	44	58	36	73

Gambar II.3. Hasil Chiperteks dengan *Nihilist*

3. Penyandian dengan kunci asimetrik (A*symmetric key encipherment*). Penyandian dengan kunci asimetrik atau sering juga disebut kunci publik (*public key*) adalah Penyandian dengan enkripsi dan deskripsi berbeda nilai. Kunci enkripsi disebut dengan kunci publik (*public key*) bersifat terbuka. Sedangkan, kunci deskripsi disebut privat (*private key*) bersifat tertutup/rahasia. (Sadikin, 2017 : 9).
4. Penyandian dengan kunci asimetrik (*Asymmetric Key Encipherment*).

   Penyandian dengan kunci asimetrik atau sering juga disebut dengan penyandian kunci publik (*public key*) adalah penyandian dengan kunci enkripsi dan dekripsi berbeda nilai. Kunci enkripsi yang juga disebut dengan kunci publik (*public key*) bersifat terbuka. Sedangkan, kunci dekripsi yang juga disebut kunci privat (*private key*) bersifat tertutup/rahasia. (Sadikin, 2017 : 10).

II.2.5. *Keystream Generator*

Keystream merupakan *bit-bit* kunci yang digunakan untuk enkripsi/dekripsi. *Keystream* umumnya dikenal pada *cipher*aliran, yang termasuk ke dalam algoritma kriptografi modern. *Keystream* tersebut dibangkitkan oleh *Keystream generator*. *Keystream generator* menerima masukan kunci U dan akan menghasilkan kunci (*keystream*) yang digunakan untuk enkripsi/dekripsi. Pengirim dan penerima pesan harus memiliki kunci U yang sama. Kunci U tersebut harus dijaga kerahasiaannya. Dengan menggunakan *keystream generator*, kunci U semula akan menghasilkan kunci (*keystream*) yang akan digunakan untuk enkripsi/dekripsi. Pendekatan terhadap prinsip tersebutlah yang akan digunakan untuk memodifikasi *Vigenere Cipher*. Penerapan pendekatan tersebut pada *Vigenere Cipher* dilakukan pada kunci U semula yang panjangnnya lebih pendek dari pada panjang plainteks. (Abhirama, 2014 : 2).

II.2.6. *Hypertext Preprocessor* (PHP)

PHP adalah singkatan dari PHP *Hypertext Preprocessor* yang digunakan sebagai bahasa *script server-side* dalam pengembangan *web* yang disisipkan pada dokumen HTML.PHP adalah bahasa *scripting* yang menyatu dengan HTML dan dijalankan pada *server side*. Artinya semua sintaks yang kita berikan akan sepenuhnya dijalankan pada *server* sedangkan yang dikirimkan ke *browser* hanya hasilnya saja. (Warnman dan Zahni, 2013 : 31).

II.2.7. *Hypertext Markup Language* (HTML)

Hypertext Markup Language (HTML) adalah suatu bahasa yang dikenali oleh *web browser* untuk menampilkan informasi dengan lebih menarik dibandingkan dengan tulisan teks biasa (*plaint text*). Sedangkan *web browser* adalah bahasa program komputer yang digunakan untuk membaca HTML, kemudian menerjemahkan dan menampilkan hasilnya secara *visual* ke layar komputer. (Nugraha, dkk, 2014 : 175).

II.2.8. MySQL

MySQL adalah *Relation Database Management System* (RDBMS) yang didistribusikan secara gratis di bawah lisensiGPL (*General Public License).* MySQL merupakan turunan dari salah satu konsep utama dalam *database* sejak lama, yaitu SQL (*Structure Query Language)*. SQL merupakan salah satu konsep pengoperasian *database,* terutama sebagai seleksi dan pemasukan data,yang memungkinkan pengoperasian datanya dikerjakan dengan mudah secara otomatis. (Inayah, dkk, 2015 : 5).

II.2.9. *Unified Modeling Language* (UML)

Menurut Windu Gata (2013) Hasil pemodelan pada OOAD terdokumentasikan dalam bentuk *Unified Modeling Language* (UML). UML adalah bahasa spesifikasi standar yang dipergunakan untuk mendokumentasikan, menspesifikasikan dan membangun perangkat lunak.

UML merupakan metodologi dalam mengembangkan sistem berorientasi objek dan juga merupakan alat untuk mendukung pengembangan sistem. UML

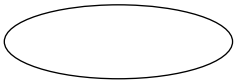
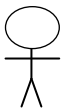
saat ini sangat banyak dipergunakan dalam dunia industri yang merupakan standar bahasa pemodelan umum dalam industri perangkat lunak dan pengembangan sistem. (Urva dan Siregar, 2015 : 93).

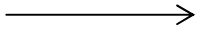
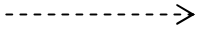
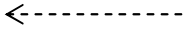
Alat bantu yang digunakan dalam perancangan berorientasi objek berbasiskan UML adalah sebagai berikut:

1. *Use Case* Diagram

Use case diagram merupakan pemodelan untuk kelakukan (*behavior*) sistem informasi yang akan dibuat. *Use case* mendeskripsikan sebuah interaksi antara satu atau lebih aktor dengan sistem informasi yang akan dibuat. Dapat dikatakan *use case* digunakan untuk mengetahui fungsi apa saja yang ada di dalam sistem informasi dan siapa saja yang berhak menggunakan fungsi-fungsi tersebut. Simbol-simbol yang digunakan dalam *use case* diagram dapat dilihat pada tabel II.4 dibawah ini:

Tabel II.2. Simbol *Use Case*

Gambar	Keterangan
	*Use case* menggambarkan fungsionalitas yang disediakan sistem sebagai unit-unit yang bertukar pesan antar unit dengan aktor, dan dinyatakan dengan menggunakan kata kerja di awal nama *use case*.
	Aktor adalah *abstraction* dari orang atau sistem yang lain yang mengaktifkan fungsi dari target sistem. Untuk mengidentifikasikan aktor, harus ditentukan pembagian tenaga kerja dan tugas-tugas yang berkaitan dengan peran pada konteks target sistem. Orang atau sistem bisa muncul dalam beberapa peran. Perlu dicatat bahwa aktor berinteraksi dengan *use case*, tetapi tidak memiliki *control* terhadap *use case*.
	Asosiasi antara aktor dan *use case*, digambarkan dengan garis tanpa panah yang mengindikasikan siapa atau apa yang meminta interaksi secara

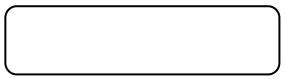
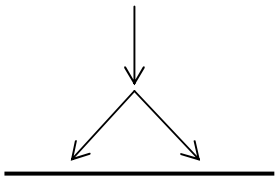
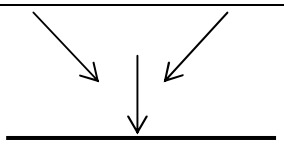
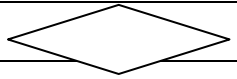
	langsung dan bukannya mengidikasikan aliran data.
	Asosiasi antara aktor dan *use case* yang menggunakan panah terbuka untuk mengidinkasikan bila aktor berinteraksi secara pasif dengan sistem.
	*Include,* merupakan di dalam *use case* lain (*required*) atau pemanggilan *use case* oleh *use case* lain, contohnya adalah pemanggilan sebuah fungsi program.
	*Extend,* merupakan perluasan dari *use case* lain jika kondisi atau syarat terpenuhi.

(Sumber:Urva dan Siregar, 2015 : 94)

2. Diagram Aktivitas (*Activity Diagram*)

Activity Diagram menggambarkan *workflow* (aliran kerja) atau aktivitas dari sebuah sistem atau proses bisnis. Simbol-simbol yang digunakan dalam *activity diagram* dapat dilihat pada tabel II.5 dibawah ini:

Tabel II.3. Simbol *Activity Diagram*

Gambar	Keterangan
	*Start point*, diletakkan pada pojok kiri atas dan merupakan awal aktifitas.
	*End point*, akhir aktifitas.
	*Activites*, menggambarkan suatu proses/kegiatan bisnis.
	*Fork* (Percabangan), digunakan untuk menunjukkan kegiatan yang dilakukan secara parallel atau untuk menggabungkan dua kegiatan pararel menjadi satu.
	*Join* (penggabungan) atau rake, digunakan untuk menunjukkan adanya dekomposisi.
	*Decision Points,* menggambarkan pilihan untuk

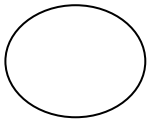
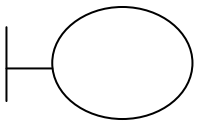
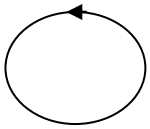
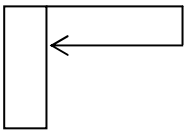
	pengambilan keputusan, *true, false.*
New Swimline	*Swimlane*, untuk menunjukkan siapa melakukan apa.

(Sumber : Urva dan Siregar, 2015 : 94)

3. Diagram Urutan (*Sequence Diagram*)

Sequence diagram menggambarkan kelakuan objek pada *use case* dengan mendeskripsikan waktu hidup objek dan pesan yang dikirimkan dan diterima antar objek. Simbol-simbol yang digunakan dalam *sequence diagram* dapat dilihat pada tabel II.6 dibawah ini :

Tabel II.4. Simbol *Sequence Diagram*

Gambar	Keterangan
	*EntityClass,* merupakan bagian dari sistem yang berisi kumpulan kelas berupa entitas-entitas yang membentuk gambaran awal sistem dan menjadi landasan untuk menyusun basis data.
	*Boundary Class,* berisi kumpulan kelas yang menjadi *interface* atau interaksi antara satu atau lebih aktor dengan sistem, seperti tampilan formentry dan *form* cetak.
	*Control class,* suatu objek yang berisi logika aplikasi yang tidak memiliki tanggung jawab kepada entitas, contohnya adalah kalkulasi dan aturan bisnis yang melibatkan berbagai objek.
	*Message*, simbol mengirim pesan antar *class*.
	*Recursive,* menggambarkan pengiriman pesan yang dikirim untuk dirinya sendiri.
	*Activation, activation* mewakili sebuah eksekusi operasi dari objek, panjang kotak ini berbanding lurus dengan durasi aktivitas sebuah operasi.
	Lifeline, garis titik-titik yang terhubung dengan objek, sepanjang *lifeline* terdapat *activation*.

(Sumber : Urva dan Siregar, 2015 : 95)

4. *Class Diagram* (Diagram Kelas)

Merupakan hubungan antar kelas dan penjelasan detail tiap-tiap kelas di dalam model desain dari suatu sistem, juga memperlihatkan aturan-aturan dan tanggng jawab entitas yang menentukan perilaku sistem.*Class diagram* juga menunjukkan atribut-atribut dan operasi-operasi dari sebuah kelas dan *constraint* yang berhubungan dengan objek yang dikoneksikan. *Class diagram* secara khas meliputi: Kelas (*Class*), Relasi, *Associations*, *Generalization* dan *Aggregation*, Atribut (*Attributes*), Operasi (*Operations/Method*), *Visibility,* tingkat akses objek eksternal kepada suatu operasi atau atribut. Hubungan antar kelas mempunyai keterangan yang disebut dengan *multiplicity* atau kardinaliti yang dapat dilihat pada tabel II.7 dibawah ini:

Tabel II.5. *Multiplicity Class Diagram*

Multiplicity	Penjelasan
1	Satu dan hanya satu
0..*	Boleh tidak ada atau 1 atau lebih
1..*	1 atau lebih
0..1	Boleh tidak ada, maksimal 1
n..n	Batasan antara. Contoh 2..4 mempunyai arti minimal 2 maksimum 4

(Sumber : Urva dan Siregar, 2015 : 95)

II.2.10. Sistem *Login*

Log masuk (bahasa Inggris: *login*, juga biasa disebut sebagai *log in*, *log on*, *logon*, *signon*, (*sign on*, *signin*, *sign in*) adalah proses untuk mengakses komputer dengan memasukkan identitas dari akun pengguna dan kata sandi guna

mendapatkan hak akses menggunakan sumber daya komputer tujuan.Pada saat melakukan *login* untuk masuk ke dalam sistem, *user* akan diminta memasukkan identitas *user* seperti identitas *user id* dan *password* sebagai antisipasi dalam hal pengamanan sistem (Agus, 2014 : 173).

BAB III

ANALISIS DAN DESAIN SISTEM

BAB III

ANALISA DAN DESAIN SISTEM

III.1. Analisis Masalah

Keamanan pada sebuah data dan informasi sangatlah penting. Oleh karena itu keamanan harus diterapkan pada sebuah data dan informasi. Di dalam penyimpanan data dan informasi, keamanan dalam sebuah data dan informasi tidak terjamin dari adanya pencuri informasi. Pada sebuah sistem biasanya ditemukan adanya sistem *login* untuk mencegah orang-orang yang tidak memiliki hak akses masuk dan mencuri informasi dari sebuah sistem tersebut. Oleh karena itu dibutuhkan sebuah teknik yang dapat mengatasi kecurian informasi melalui sistem *login*. Dengan mengamankan isi dari *database* sistem *login*, maka pencuri informasi tidak dapat masuk ke dalam sistem. Teknik yang peneliti usulkan yaitu kriptografi. Namun untuk dapat menggunakan teknik kriptografi, maka dibutuhkan metode yang tepat untuk mendapatkan hasil yang baik. Peneliti mengusulkan metode *Nihilist Cipher.*

III.2. Penerapan Metode

Pada penelitian ini peneliti menggunakan metode *Nihilist Cipher* untuk keamanan sistem *login*. Langkah-langkah metode *Nihilist Cipher* adalah sebagai berikut :

III.2.1. Enkrip Metode *Nihilist Cipher*

Berikut ini adalah langkah-langkah dalam enkrip pesan pada metode *Nihilist Cipher* :

1. Algoritma ini menggunakan *Polybius Square* yaitu sebuah kotak 5x5, dengan huruf Latin secara acak dan misalkan huruf J dihilangkan. Setiap elemen berisi huruf yang berbeda dengan 2 digit koordinat. Penempatan setiap huruf dapat diacak. Untuk kata TIGA dapat direpresentasikan sebagai koordinat (44 24 22 11).

Tabel III.1. Tabel Polybius Square

	1	**2**	**3**	**4**	**5**
1	A	B	C	D	E
2	F	G	H	I	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

2. Selanjutnya tentukan Kata Kunci misalnya NASUTION maka hasil substitusinya adalah (33 11 43 45 44 24 34 33). Lakukan pengulangan bila panjang pesan lebih besar dari pada panjang kunci dan jika panjang kunci lebih besar dari panjang pesan, maka digunakan *keystream generator* untuk mengulang pesan sehingga panjang pesan sama dengan panjang kunci. Jadi pesan asli menjadi TIGATIGA.
3. Lakukan perulangan pada kata yang lebih pendek dari kunci. Lakukan operasi penjumlahan antara koordinat kata kunci dengan *plaintext*. KK untuk Kata Kunci, PT untuk *plaintext* dan CT untuk *ciphertext*.

Tabel III.2. Tabel Hasil Enkripsi Dengan *Nihilist*

PT	44	24	22	11	44	24	22	11
KK	33	11	43	45	44	24	34	33
CT	**77**	**35**	**65**	**56**	**88**	**48**	**56**	**44**

III.2.2. Dekrip Metode *Nihilist Cipher*

Berikut ini adalah langkah-langkah dalam mendekripsi sebuah pesan pada algoritma *Nihilist Cipher* :

1. Untuk mendekripsi *Nihilist* kita harus mengetahui kata kunci dan memiliki *ciphertext*-nya. Misalkan kita memiliki "77 35 65 56 88 48 56 44" sebagai *ciphertext* dan "NASUTION" menjadi kata kuncinya.
2. Mengacu pada Tabel III.3 kata "TIGA" bila disubstitusi akan menghasilkan himpunan koordinat "44 24 22 11".

Tabel III.3. Tabel Polybius Square

	1	**2**	**3**	**4**	**5**
1	A	B	C	D	E
2	F	G	H	I	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

3. Lakukan operasi pengurangan antara koordinat *ciphertext* dengan kata kunci.

Tabel III.4. Tabel Hasil Dekripsi Dengan *Nihilist*

CT	77	35	65	56	88	48	56	44
KK	33	11	43	45	44	24	34	33
PT	**44**	**24**	**22**	**11**	**44**	**24**	**22**	**11**

4. Langkah terakhir adalah mencari padanan karakter untuk setiap koordinat yang didapatkan di atas dengan tabel *Polybius Square* seperti pada Tabel III.5, maka didapati kata *plaintext* "TIGATIGA". Apabila terdapat perulangan kalimat, maka kalimat awal sebagai *plaintext*. Berarti *plaintext*nya adalah "TIGA".

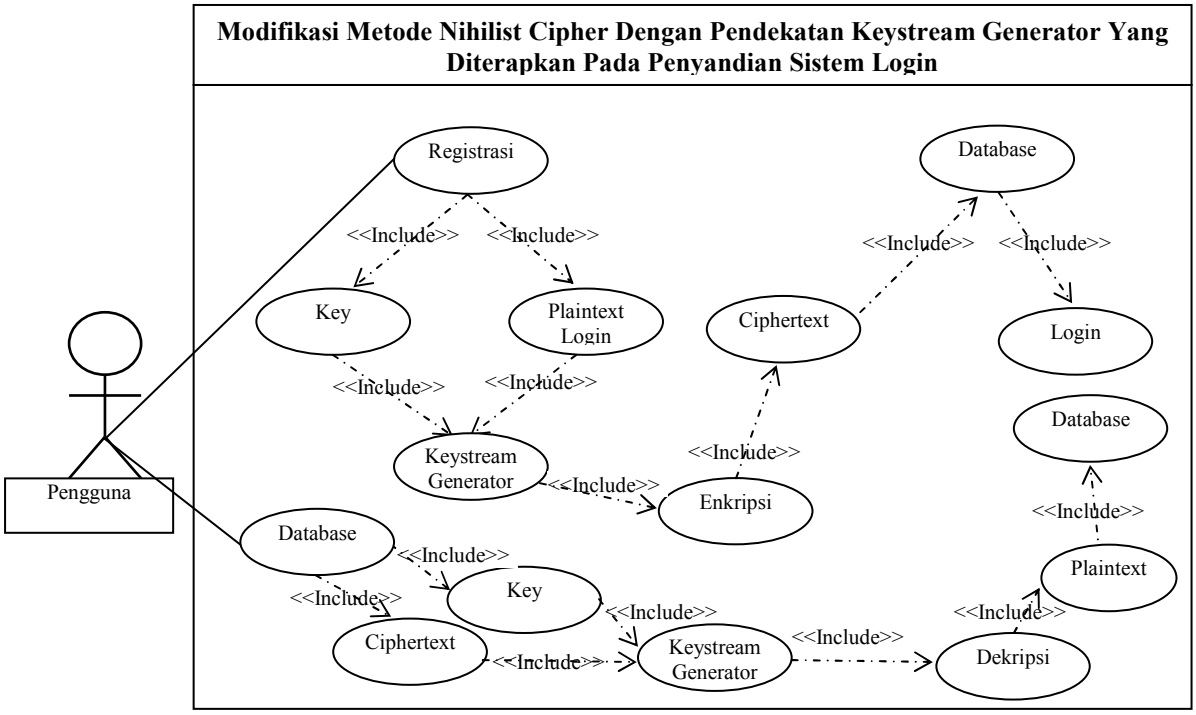
III.3. Desain Sistem

III.3.1. Desain Sistem Pemodelan UML

Pada penelitian ini peneliti menggunakan perancangan dengan diagram dari *Unified Modeling Language* (UML) yaitu *Use Cace Diagram*, *Sequence Diagram* dan *Activity Diagram*.

III.3.1.1. *Use Case Diagram*

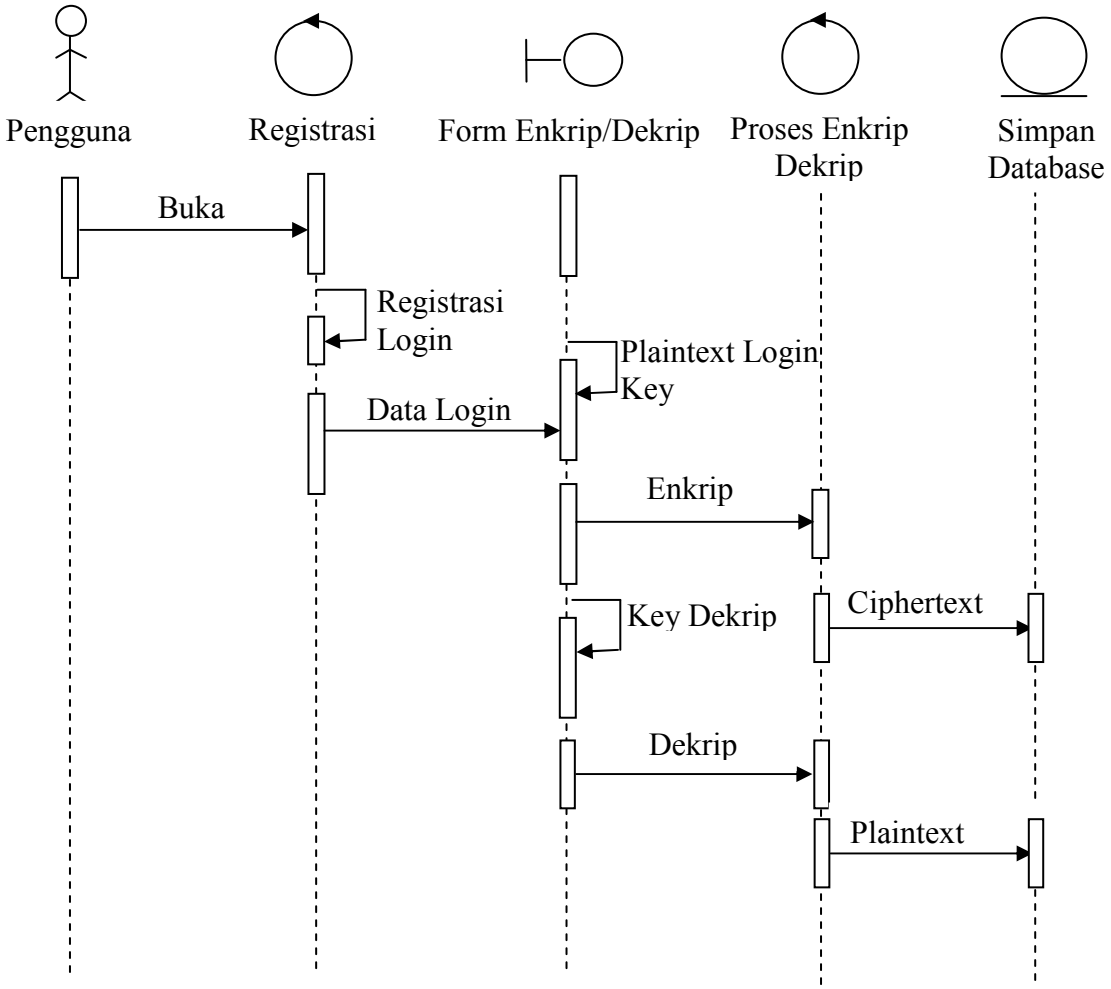
Perancangan dimulai dari identifikasi aktor dan bagaimana hubungan antara aktor dan *use case* di dalam sistem. Perancangan *Use Case* Diagram dapat dilihat pada gambar III.1.



Gambar III.1. *Use Case* Modifikasi Metode Nihilist Cipher Dengan Pendekatan *Keystream generator* Yang Diterapkan Pada Penyandian Sistem *Login*

III.3.1.2. *Sequence Diagram* Enkrip/Dekrip

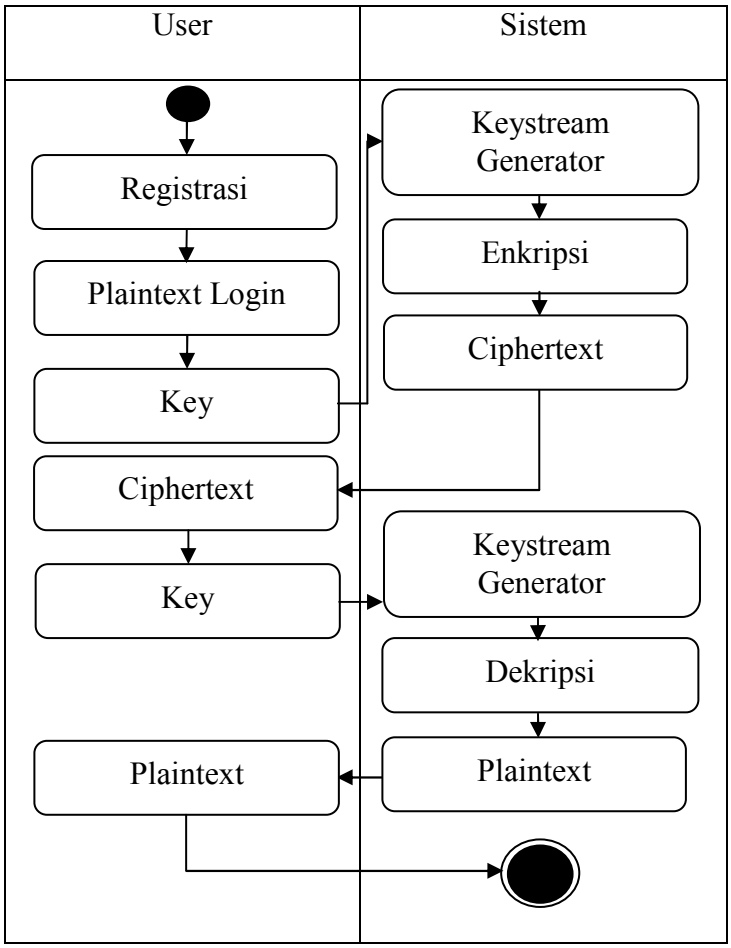
Gambar III.2 adalah *sequence diagram* enkrip/dekrip dari Aplikasi Modifikasi Metode *Nihilist Cipher* Dengan Pendekatan *Keystream generator* Yang Diterapkan Pada Penyandian Sistem *Login*.



Gambar III.2. *Sequence Diagram* Enkrip/Dekrip

III.3.1.3. *Activity Diagram* Enkrip/Dekrip

Gambar III.3 adalah *sequence* diagram enkrip/dekrip dari Aplikasi Aplikasi Modifikasi Metode *Nihilist Cipher* Dengan Pendekatan *Keystream generator.*



Gambar III.3. *Activity Diagram* Enkrip/Dekrip

III.3.2. Desain Sistem Aplikasi

Desain sistem aplikasi modifikasi metode *Nihilist Cipher* dengan pendekatan *keystream generator* yang diterapkan pada penyandian sistem *login* dapat dilihat pada gambar sebagai berikut.

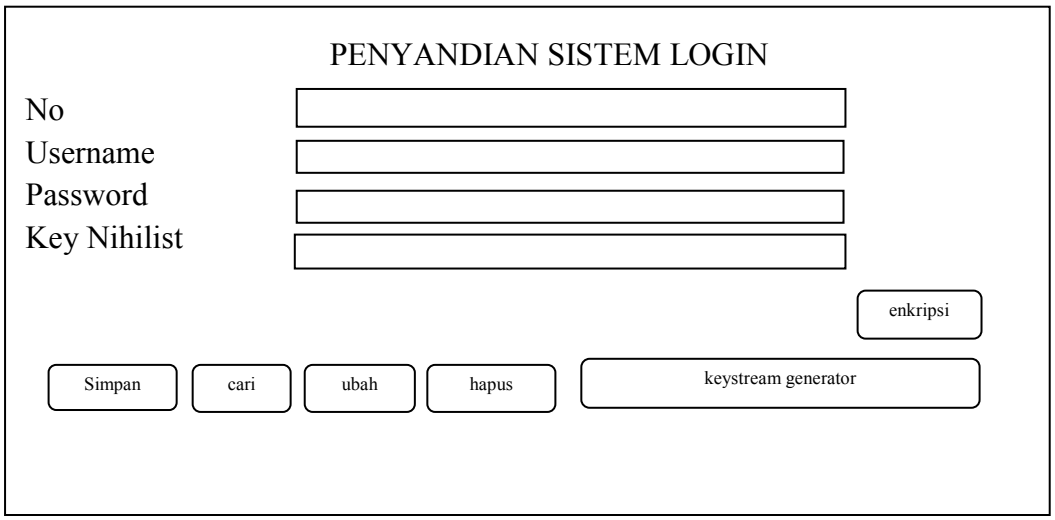
1. Desain *Form* Menu Utama

Gambar III.4 menunjukkan rancangan *form* menu utama dari aplikasi modifikasi metode *Nihilist Cipher* dengan pendekatan *keystream generator* pada penyandian sistem *login*.

Gambar III.4. Rancangan *Form* Desain Sistem Menu

2. Desain *Form* Enkripsi

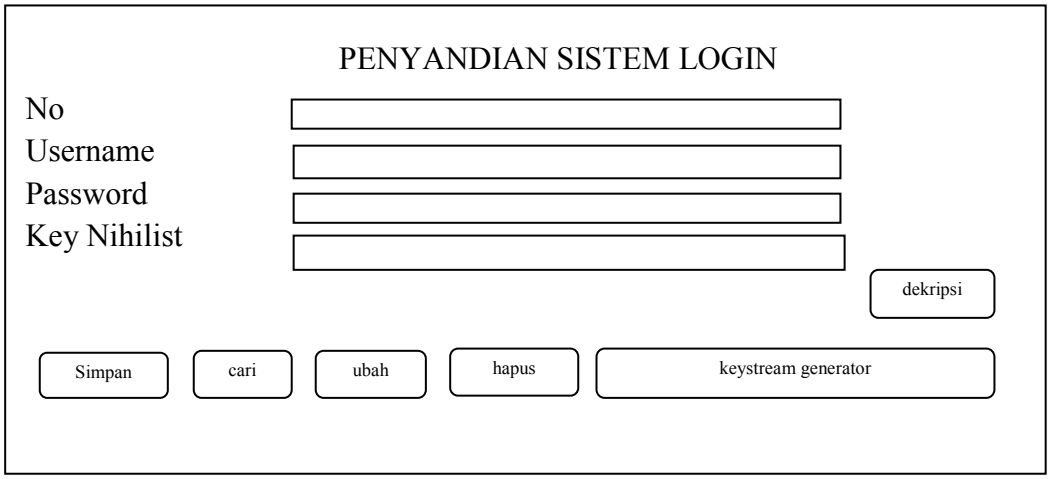
Gambar III.5 menunjukkan rancangan *form* enkripsi dari aplikasi modifikasi metode *Nihilist Cipher* dengan pendekatan *keystream generator* pada penyandian sistem *login*.



Gambar III.5. Rancangan *Form* Desain Sistem Enkripsi

3. Desain *Form* Dekripsi

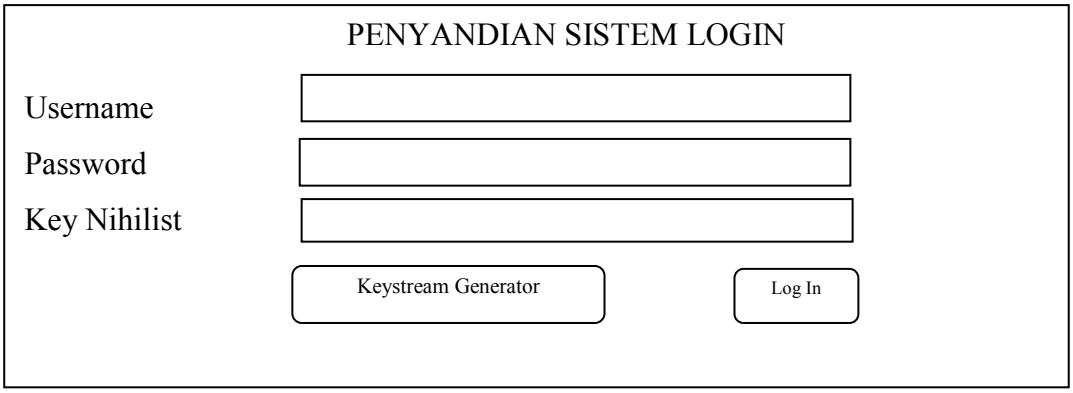
Gambar III.6 menunjukkan rancangan *form* dekripsi dari aplikasi modifikasi metode *Nihilist Cipher* dengan pendekatan *keystream generator* pada penyandian sistem *login*.



Gambar III.6. Rancangan *Form* Desain Sistem Dekripsi

4. Desain *Form* Tes *Login*

Gambar III.7 menunjukkan rancangan *form* enkripsi dari aplikasi modifikasi metode *Nihilist Cipher* dengan pendekatan *keystream generator* pada penyandian sistem *login*.



Gambar III.7. Rancangan *Form* Desain Sistem Tes *Login*

BAB IV

HASIL DAN PEMBAHASAN

BAB IV

HASIL DAN PEMBAHASAN

IV.1. Tampilan Hasil

Aplikasi modifikasi Metode *Nihilist Cipher* dengan pendekatan *Keystream generator* yang diterapkan pada penyandian sistem *login* menggunakan bahasa pemrograman HTML, PHP dan menggunakan *database* MySQL. HTML digunakan untuk membentuk tampilan, PHP digunakan untuk mengontrol aplikasi dan *database* MySQL sebagai penyimpanan data *login*. Berikut ini adalah tampilan hasil dari aplikasi modifikasi Metode *Nihilist Cipher* dengan pendekatan *keystream generator* yang diterapkan pada penyandian sistem *login* :

1. Tampilan *Form* Menu

Tampilan yang disajikan oleh sistem untuk menampilkan *form* menu dapat dilihat pada gambar IV.1.

Gambar IV.1. Tampilan *Form* Menu

Keterangan :

Gambar IV.1 adalah *form* menu dari aplikasi yang telah dibuat, pada *form* menu terdapat tiga buah tombol yang digunakan untuk membuka *form* yang lain. Apabila pengguna mengklik tombol dekripsi maka aplikasi akan menampilkan *form* dekripsi, apabila pengguna mengklik tombol dekripsi maka aplikasi akan menampilkan *form* dekripsi dan apabila pengguna mengklik tombol tes *login* maka aplikasi akan menampilkan *form* tes *login*.

2. Tampilan *Form* Enkripsi

Tampilan yang disajikan oleh sistem untuk menampilkan *form* enkripsi dapat dilihat pada gambar IV.2.

Gambar IV.2. Tampilan *Form* Enkripsi

Keterangan :

Gambar IV.2 adalah *form* enkripsi dari aplikasi yang telah dibuat, pada *form* enkripsi pengguna dapat menyandikan data *login* dengan cara mengisi seluruh kotak teks yang tersedia kemudian klik tombol enkrip. Pengguna dapat mengelola

database login dari *form* ini, pengguna dapat menambah, menyimpan, mengubah, menghapus dan mencari data yang dimasukkan.

3. Tampilan *Form* Dekripsi

Tampilan yang disajikan oleh sistem untuk menampilkan *form* dekripsi dapat dilihat pada gambar IV.3.

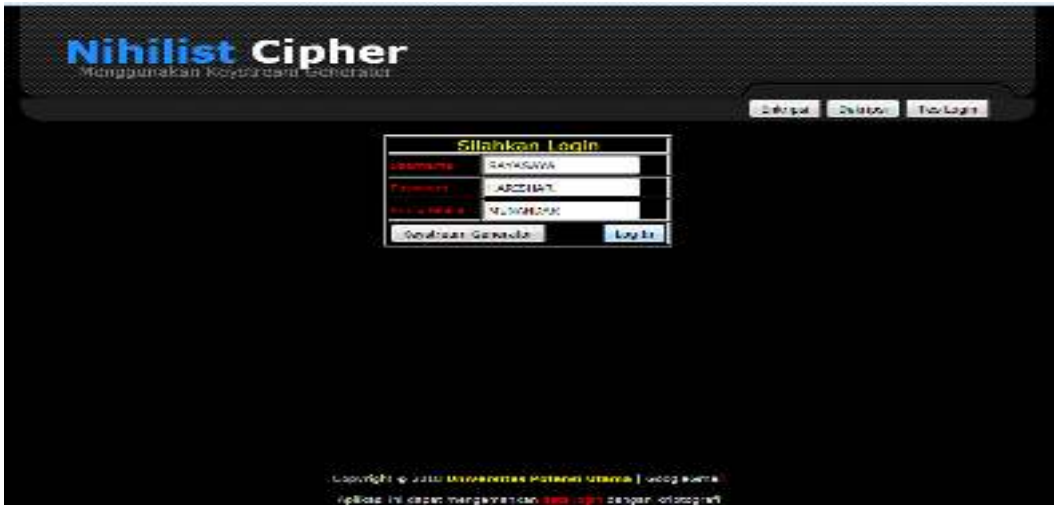
Gambar IV.3. Tampilan *Form* Dekripsi

Keterangan :

Gambar IV.3 adalah *form* dekripsi dari aplikasi yang telah dibuat, pada *form* dekripsi pengguna dapat membaca data *login* yang tersandi dengan cara membuka data *login* pada seluruh kotak teks yang tersedia kemudian klik tombol dekrip. Pengguna dapat mengelola *database login* dari *form* ini, pengguna dapat menambah, menyimpan, mengubah, menghapus dan mencari data yang dimasukkan.

4. Tampilan *Form* Tes *Login*

Tampilan yang disajikan oleh sistem untuk menampilkan *form* tes *login* dapat dilihat pada gambar IV.4.



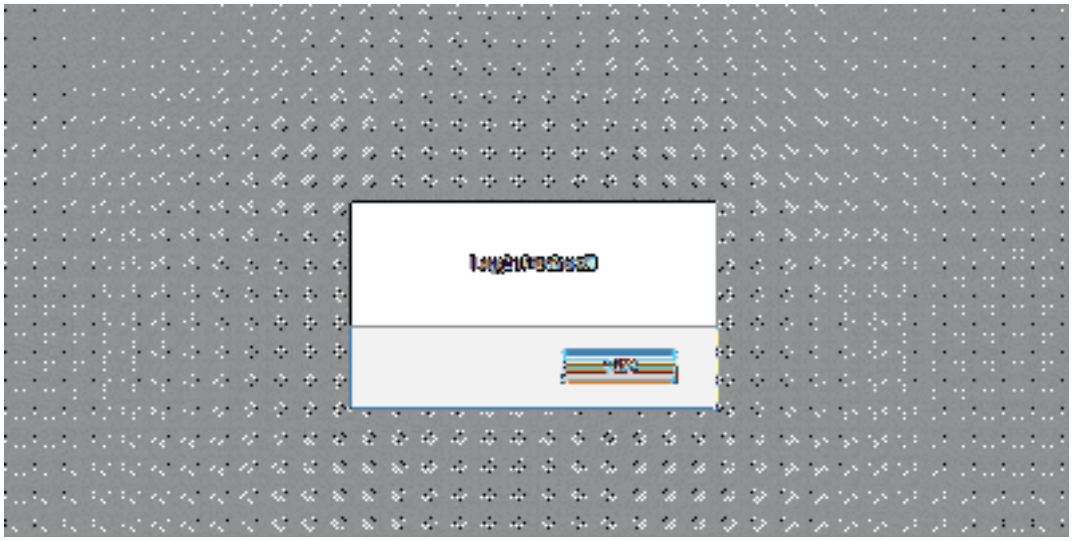
Gambar IV.4. Tampilan *Form* Tes *Login*

Keterangan :

Gambar IV.4 adalah *form login* dari aplikasi yang telah dibuat, pada *form* tes *login* apabila pengguna mengisi seluruh kotak teks, kemudian mengklik tombol *log in* jika data masukan benar, maka akan muncul pesan sukses dan apabila data masukan salah akan muncul pesan gagal.

5. Tampilan Notifikasi *Form Login*

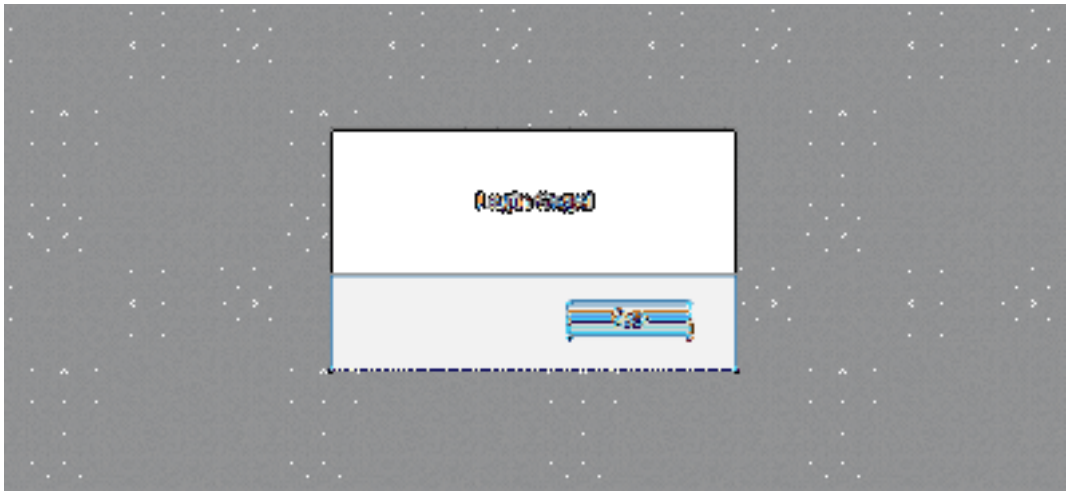
Tampilan yang disajikan oleh sistem untuk menampilkan notifikasi *form* tes *login* apabila berhasil dapat dilihat pada gambar IV.5. Dan apabila gagal dapat dilihat pada gambar IV.6.



Gambar IV.5. Tampilan Notifikasi *Form Login* Berhasil

Keterangan :

Gambar IV.5 adalah *form login* dari aplikasi yang telah dibuat, pada *form* tes *login* apabila pengguna mengisi seluruh kotak teks, kemudian mengklik tombol *log in* jika data masukan benar, maka muncul notifikasi "*Login* Berhasil".



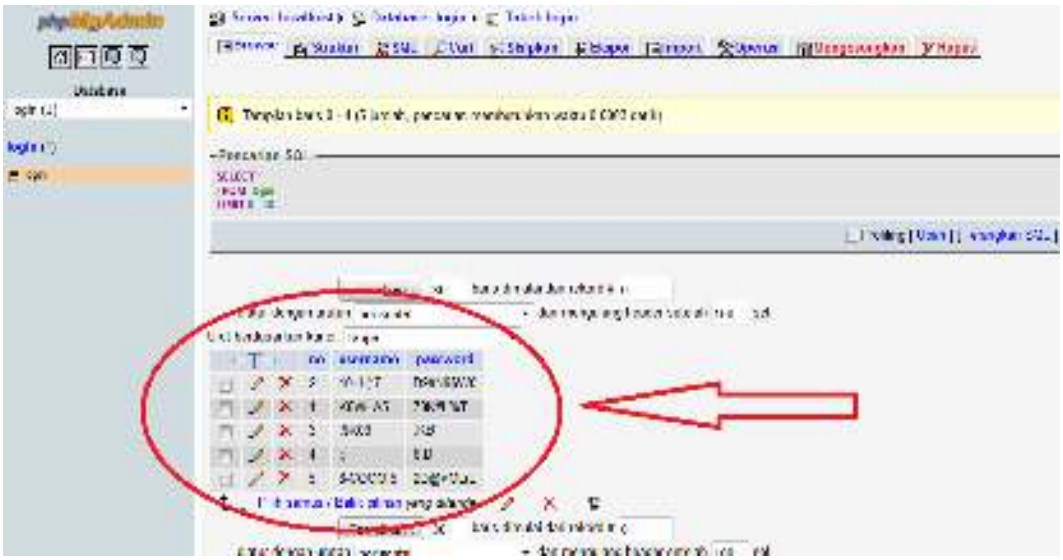
Gambar IV.6. Tampilan Notifikasi *Form Login* Gagal

Keterangan :

Gambar IV.6 adalah *form login* dari aplikasi yang telah dibuat, pada *form* tes *login* apabila pengguna mengisi seluruh kotak teks, kemudian mengklik tombol *log in* jika data masukan salah, maka muncul notifikasi "*Login* Gagal".

6. Tampilan *Form Database*

Tampilan yang disajikan oleh sistem untuk menampilkan *form database* dapat dilihat pada gambar IV.7.



Gambar IV.7. Tampilan *Form Database*

Keterangan :

Gambar IV.7 adalah *form database* dari aplikasi yang telah dibuat, pada *form database* apabila pengguna menyimpan isi teks registrasi pada *form* enkripsi dan dekripsi, kemudian mengklik tombol simpan, maka teks akan tersimpan ke dalam *database* MySQL.

IV.2. Uji Coba Program

Uji coba terhadap sistem bertujuan untuk memastikan bahwa sistem sudah berada pada kondisi siap pakai. Instrumen yang digunakan untuk melakukan pengujian ini yaitu dengan menggunakan *Blackbox Testing* :

Tabel. IV.1. *Blackbox Testing Form* Menu

No	Form Menu	Uji Coba Pengguna	Keterangan	Hasil
1	Tombol Enkripsi	Surya Atmaja, S.T M. Zulfadly Simatupang M. Hanif Aulianda Nova Andriani, M.Hum Sri Banun Eka Sukma, SH	Sistem akan menampilkan form enkripsi	Dari 5 orang yang menguji, 5 orang mengatakan sesuai (valid)
2	Tombol Dekripsi	Surya Atmaja, S.T M. Zulfadly Simatupang M. Hanif Aulianda Nova Andriani, M.Hum Sri Banun Eka Sukma, SH	Sistem akan menampilkan form dekripsi	Dari 5 orang yang menguji, 5 orang mengatakan sesuai (valid)

Tabel. IV.2. *Blackbox Testing Form* Enkripsi

No.	Form Enkripsi	Uji Coba Pengguna	Keterangan	Hasil
1.	Isi seluruh *textbox* dan Klik Tombol Enkrip	Surya Atmaja, S.T M. Zulfadly Simatupang M. Hanif Aulianda Nova Andriani, M.Hum Sri Banun Eka Sukma, SH	Sistem akan menyandikan isi teks pada seluruh textbox	Dari 5 orang yang menguji, 5 orang mengatakan sesuai (valid)
2.	Klik Tombol Simpan	Surya Atmaja, S.T M. Zulfadly Simatupang M. Hanif Aulianda Nova Andriani, M.Hum Sri Banun Eka Sukma, SH	Sistem akan menyimpan seluruh isi *text* ke dalam *database*	Dari 5 orang yang menguji, 5 orang mengatakan sesuai (valid)

3.	Klik Tombol Ubah	Surya Atmaja, S.T M. Zulfadly Simatupang M. Hanif Aulianda Nova Andriani, M.Hum Sri Banun Eka Sukma, SH	Sistem akan merubah isi *database* sesuai dengan kode pencarian	Dari 5 orang yang menguji, 5 orang mengatakan sesuai (valid)
4.	Klik Tombol Cari	Surya Atmaja, S.T M. Zulfadly Simatupang M. Hanif Aulianda Nova Andriani, M.Hum Sri Banun Eka Sukma, SH	Sistem akan menampilkan isi database sesuai dengan kode pencarian	Dari 5 orang yang menguji, 5 orang mengatakan sesuai (valid)
5.	Klik Tombol Hapus	Surya Atmaja, S.T M. Zulfadly Simatupang M. Hanif Aulianda Nova Andriani, M.Hum Sri Banun Eka Sukma, SH	Sistem akan menghapus isi *database* sesuai dengan kode pencarian	Dari 5 orang yang menguji, 5 orang mengatakan sesuai (valid)

Tabel. IV.3. *Blackbox Testing Form* Dekripsi

No.	Form Dekripsi	Uji Coba Pengguna	Keterangan	Hasil
1.	Isi seluruh *textbox* dan Klik Tombol Dekrip	Surya Atmaja, S.T M. Zulfadly Simatupang M. Hanif Aulianda Nova Andriani, M.Hum Sri Banun Eka Sukma, SH	Sistem akan membuka isi teks tersandi pada seluruh textbox	Dari 5 orang yang menguji, 5 orang mengataka n sesuai (valid)
2.	Klik Tombol Simpan	Surya Atmaja, S.T M. Zulfadly Simatupang M. Hanif Aulianda Nova Andriani, M.Hum Sri Banun Eka Sukma, SH	Sistem akan menyimpan seluruh isi *text* ke dalam *database*	Dari 5 orang yang menguji, 5 orang mengataka n sesuai (valid)
3.	Klik Tombol Ubah	Surya Atmaja, S.T M. Zulfadly Simatupang	Sistem akan merubah isi *database*	Dari 5 orang yang

		M. Hanif Aulianda Nova Andriani, M.Hum Sri Banun Eka Sukma, SH	sesuai dengan kode pencarian	menguji, 5 orang mengataka n sesuai (valid)
4.	Klik Tombol Cari	Surya Atmaja, S.T M. Zulfadly Simatupang M. Hanif Aulianda Nova Andriani, M.Hum Sri Banun Eka Sukma, SH	Sistem akan menampilkan isi database sesuai dengan kode pencarian	Dari 5 orang yang menguji, 5 orang mengataka n sesuai (valid)
5.	Klik Tombol Hapus	Surya Atmaja, S.T M. Zulfadly Simatupang M. Hanif Aulianda Nova Andriani, M.Hum Sri Banun Eka Sukma, SH	Sistem akan menghapus isi *database* sesuai dengan kode pencarian	Dari 5 orang yang menguji, 5 orang mengataka n sesuai (valid)

Tabel. IV.4. *Blackbox Testing Form* Tes *Login*

No	Form Tes *Login*	Uji Coba Pengguna	Keterangan	Hasil
1	Seluruh kotak teks di isi, kemudian klik tombol *log in*	Surya Atmaja, S.T M. Zulfadly Simatupang M. Hanif Aulianda Nova Andriani, M.Hum Sri Banun Eka Sukma, SH	Jika data masukan benar, maka akan muncul pesan sukses. Apabila data masukan salah akan muncul pesan gagal.	Dari 5 orang yang menguji, 5 orang mengataka n sesuai (valid)

IV.2.1 Hasil Uji Coba

Setelah melakukan uji coba terhadap sistem, maka dapat disimpulkan hasil yang didapatkan yaitu :

1. Metode *Nihilist Cipher* telah berhasil diterapkan ke dalam aplikasi.

2. Penerapan *Keystream generator* telah berhasil diterapkan ke dalam aplikasi.
3. Hasil enkripsi dan dekripsi berjalan dengan baik.
4. Hasil pengelolaan *database* berjalan dengan baik.
5. *Interface* bersifat *userfriendly* sehingga siapa saja dapat memahami penggunaan aplikasi.

IV.3. Kelebihan dan Kekurangan Sistem

Setiap sistem memiliki kelebihan dan kekurangan, berikut ini adalah kelebihan dan kekurangan sistem yang telah dibuat.

IV.3.1. Kelebihan Sistem

Adapun kelebihan sistem yang telah dibuat diantaranya yaitu :

1. Dapat menyandikan data sistem *login*.
2. Metode *Nihilist Cipher* dapat diterapkan pada sistem *login* berbasis *web*.
3. Memberikan hasil keamanan yang baik.

IV.3.2. Kekurangan Sistem

Adapun kekurangan sistem yang telah dibuat diantaranya yaitu :

1. Sistem yang telah dirancang menggunakan metode klasik.
2. *Interface* antar muka tidak terlalu menarik.
3. Sistem ini belum diterapkan pada perangkat *mobile*.

BAB V

HASIL DAN PEMBAHASAN

BAB V

KESIMPULAN DAN SARAN

V.1. Kesimpulan

Berdasarkan pembahasan dari bab-bab sebelumnya yang telah dilakukan maka dapat diambil beberapa kesimpulan sebagai berikut :

1. Dengan menyandikan isi dari data *login* maka para pencuri data dan informasi *login* tidak dapat membaca isi data *login* pada *database*.
2. Sebuah pesan dan kunci diubah kedalam bentuk kode ASCII dan kemudian menerapkan metode *Nihilist Cipher* yang menggunakan rumus dan langkah *Nihilist Cipher*. Setelah hasil metode didapatkan kemudian hasil penjumlahan diubah kembali dalam bentuk karakter.
3. Apabila panjang kunci melebihi panjang pesan, maka *keystream generator* menambahkan jumlah karakter pesan sesuai dengan panjang kunci.
4. Dengan menggunakan pemrograman *web* dan menggunakan *database* MySQL kemudian menerapkan metode *Nihilist Cipher* maka dapat menghasilkan aplikasi modifikasi metode *Nihilist Cipher* dengan pendekatan *Keystream Generator* yang diterapkan pada penyandian sistem *login*.

V.2. Saran

Untuk pengembangan lebih lanjut pada aplikasi modifikasi metode *Nihilist Cipher* dengan pendekatan *Keystream Generator* yang diterapkan pada

penyandian sistem *login* dapat bekerja dengan baik, maka dapat diberikan beberapa saran sebagai berikut :

1. Diharapkan aplikasi yang telah dibuat dapat menggunakan metode kriptografi modern.
2. Diharapkan aplikasi modifikasi metode *Nihilist Cipher* dengan pendekatan *Keystream Generator* yang diterapkan pada penyandian sistem *login* pada *interface* dibuat menjadi lebih menarik.
3. Diharapkan aplikasi modifikasi metode *Nihilist Cipher* dengan pendekatan *Keystream Generator* yang diterapkan pada penyandian sistem *login* dapat diterapkan berbasis *mobile*.

DAFTAR PUSTAKA

Inayah, dkk, 2012, ***Aplikasi Pemesanan Menu Makanan Di Rumah Makan Berbasis Web Service Menggunakan Mobile Android***, Jurnal Teknik Informatika, Universitas Bina Darma, Vol. 1, No. 1, Palembang.

Mukhlish, 2013, ***Modifikasi Nihilist Cipher***, Institut Teknologi Bandung, Jurnal Teknik Informatika, Vol. 1, No. 1, Bandung.

Nugraha, dkk, 2014, ***Aplikasi Pemesanan Makanan Berbasis Mobile Pada Rumah Makan Lek Nonong***, Universitas Diponegoro, Jurnal Teknologi Dan Sistem Komputer, Vol. 2, No. 2, Semarang.

Sitohang, dkk, 2013, ***Perangkat Aplikasi Keamanan Data Text Menggunakan Electronic Codebook Dengan Algoritma Des*****,** STMIK Budi Darma. Medan.

Sholeh, dkk, 2013, ***Mengamankan Skrip Pada Bahasa Pemrograman PHP Dengan Menggunakan Kriptografi Base64*****,** Sekolah Tinggi Teknologi Garut, Garut.

Urva dan Siregar, 2015, ***Pemodelan UML E-Marketing Minyak Goreng***, Universitas Sumatera Utara, Jurnal Informatika, Vol. 1, No. 1, Medan.

Warman dan Zahni, 2013, ***Rekayasa Web Untuk Pemesanan Handphone Berbasis Jquery Pada Permata Cell***, Institut Teknologi Padang, Jurnal Momentum, Vol. 15, No. 2, Padang.

Zulfauzi, 2015, ***Aplikasi Pengenalan Bidang Olahraga Berbasis Web Android***, Jurnal Teknologi Informasi, Vol. 7, No. 1.

Rifki Sadikin, 2013, **Kriptografi** Penerbit CV. Andi Offset Yogyakarta.

LAMPIRAN

LISTING PROGRAM

1. **Connect_db.php**

```
<?php
$link = mysql_connect('localhost', 'root', '') or die('Cannot connect to the DB');
mysql_select_db('login') or die('Cannot select the DB');
?>
```

2. **Index.php**

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>software company, free css template, website layout</title>
<meta name="keywords" content="software company, free css template, website layout, css, xhtml" />
<meta name="description" content="software company, free css template, website layout, xhtml css design" />
<link href="templatemo_style.css" rel="stylesheet" type="text/css" />
<script language="javascript" type="text/javascript">
function clearText(field)
{
   if (field.defaultValue == field.value) field.value = '';
   else if (field.value == '') field.value = field.defaultValue;
}
</script>
</head>
<body>
<center>
<div id="templatemo_container">
          <div id="templatemo_header_panel">
   <!--  Free CSS Template designed by TemplateMo.com  -->
          <div id="templatemo_site_title">
          <h1>Nihilist <span>Cipher</span></h1>
          <h2>Menggunakan Keystream Generator</h2>
       </div>
   </div> <!-- end of header panel -->
   <div id="templatemo_content_bottom" align=right>
<a href=login.php><button>Enkripsi</button></a>
<a href=log_in.php><button>Dekripsi</button></a>
<ahref=tes_login.php><button>Tes Login</button></a>             </div>
```

```
<br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><
br><br><br><br><br><br><br><br><br><br><br>
   <div id="templatemo_footer">
     Copyright © 2018 <a href="#"><strong><font
color=yellow>Universitas Potensi
Utama</font></strong></a>|<ahref="http://www.google.com" target="
_parent">Google</a><a title="free css templates"
href="http://www.gmail.com" target="_parent">Gmail</a>
   </div> <!-- end of footer -->
<!--  Free CSS Template designed by TemplateMo.com  -->
</div><!-- end of container -->
<div align=center>Aplikasi ini dapat mengamankan <font color=red>data
login</font> dengan kriptografi</div></body>
</html>
```

3. **Login.php**

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0
Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-
transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>software company, free css template, website layout</title>
<meta name="keywords" content="software company, free css template,
website layout, css, xhtml" />
<meta name="description" content="software company, free css template,
website layout, xhtml css design" />
<link href="templatemo_style.css" rel="stylesheet" type="text/css" />
<script language="javascript" type="text/javascript">
function clearText(field)
{
   if (field.defaultValue == field.value) field.value = '';
   else if (field.value == '') field.value = field.defaultValue;
}
</script>
</head>
<body>
<center>
<div id="templatemo_container">
        <div id="templatemo_header_panel">
   <!--  Free CSS Template designed by TemplateMo.com  -->
        <div id="templatemo_site_title">
        <h1>Nihilist <span>Cipher</span></h1>
        <h2>Menggunakan Keystream Generator</h2>
      </div>
   </div> <!-- end of header panel -->
```

```
   <div id="templatemo_content_bottom" align=right>
        <a href=login.php><button>Enkripsi</button></a>
<a href=log_in.php><button>Dekripsi</button></a>
<ahref=tes_login.php><button>Tes
Login</button></a>       &
nbsp;     </div>
<?php
echo"
<html>
<head>
<title>Nihilist Cipher</title>
</head>
<body>
<center>
        <form action=enkrip.php method=POST>
        <table>
                <tr>
                        <td      colspan=2      align=center><font      size=4
color=red>
<b>Penyandian Sistem Login</b></font></td>
                </tr>
                <tr>
                        <td colspan=2 align=center> </td>
                </tr>
                <tr>
                        <td>No.</td>
                        <td><input      type=text      name=no      size=31
value='$no'></td>
                </tr>
                <tr>
                        <td>Username</td>
                        <td><input type=text name=username size=31
value=$username></td>
                </tr>
                <tr>
                        <td>Password</td>
                        <td><input type=text name=password size=31
value='$password'></td>
                </tr>
                <tr>
                        <td>Key Nihilist</td>
                        <td><input      type=text      name=key      size=31
value='$key'></td>
                </tr>
                <tr>
```

```
                    <td colspan=2 align=right><input type=submit
name=enkrip value=enkrip></td>
                </tr>
                <tr>
                    <td colspan=2 align=center><input type=submit
name=simpan value=simpan><input type=submit name=cari
value=cari><input type=submit name=ubah value=ubah><input
type=submit name=hapus value=hapus><input type=submit name=kg
value='keystream generator'></td>
                </tr>
            </table>
</center>
</body>
</html>";
?>
<br><br><br><br><br><br><br><br><br><br><br><br><br><br><br>
   <div id="templatemo_footer">
      Copyright © 2018 <a href="#"><strong><font
color=yellow>Universitas Potensi Utama</font></strong></a> | <a
href="http://www.google.com" target="_parent">
Google</a><a title="free css templates" href="http://www.gmail.com"
target="
_parent">Gmail</a>
   </div> <!-- end of footer -->
<!--  Free CSS Template designed by TemplateMo.com  -->
</div><!-- end of container -->
<div align=center>Aplikasi ini dapat mengamankan <font color=red>data
login</font> dengan kriptografi</div></body>
</html>
```

4. Log_in.php

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0
Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-
transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>software company, free css template, website layout</title>
<meta name="keywords" content="software company, free css template,
website layout, css, xhtml" />
<meta name="description" content="software company, free css template,
website layout, xhtml css design" />
<link href="templatemo_style.css" rel="stylesheet" type="text/css" />
<script language="javascript" type="text/javascript">
function clearText(field)
{
```

```
   if (field.defaultValue == field.value) field.value = '';
   else if (field.value == '') field.value = field.defaultValue;
}
</script>
</head>
<body>
<center>
<div id="templatemo_container">
        <div id="templatemo_header_panel">
   <!--  Free CSS Template designed by TemplateMo.com  -->
        <div id="templatemo_site_title">
        <h1>Nihilist <span>Cipher</span></h1>
        <h2>Menggunakan Keystream Generator</h2>
      </div>
   </div> <!-- end of header panel -->
   <div id="templatemo_content_bottom" align=right>
        <a href=login.php><button>Enkripsi</button></a>
<a href=log_in.php><button>Dekripsi</button></a>
<a href=tes_login.php><button>Tes Login</button></a>
          
   </div>
<?php
echo"
<html>
<head>
<title>Nihilist Cipher</title>
</head>
<body>
<center>
        <form action=dekrip.php method=POST>
        <table>
                <tr>
                        <td colspan=2 align=center><font size=4
color=red>
<b>Penyandian Sistem Login</b></font></td>
                </tr>
                <tr>
                        <td colspan=2 align=center> </td>
                </tr>
                <tr>
                        <td>No.</td>
                        <td><input type=text name=no size=31
value='$no'></td>
                </tr>
                <tr>
                        <td>Username</td>
```

```
                        <td><input type=text name=username size=31
value='$username'></td>
                    </tr>
                    <tr>
                        <td>Password</td>
                        <td><input type=text name=password size=31
value='$password'></td>
                    </tr>
                    <tr>
                        <td>Key Nihilist</td>
                        <td><input type=text name=key size=31
value='$key'></td>
                    </tr>
                    <tr>
                        <td colspan=2 align=right><input type=submit
name=dekrip value=dekrip></td>
                    </tr>
                    <tr>
                        <td colspan=2 align=center><input type=submit
name=simpan value=simpan><input type=submit name=cari
value=cari><input type=submit name=ubah value=ubah><input
type=submit name=hapus value=hapus><input type=submit name=kg
value='keystream generator'></td>
                    </tr>
            </table>
</center>
</body>
</html>";
?>
<br><br><br><br><br><br><br><br><br><br><br><br><br><br><br>
   <div id="templatemo_footer">
      Copyright © 2018 <a href="#"><strong><font
color=yellow>Universitas Potensi Utama</font></strong></a> | <a
href="http://www.google.com" target="
_parent">Google</a><a title="free css templates"
href="http://www.gmail.com" target="_parent">Gmail</a>
   </div> <!-- end of footer -->
<!--  Free CSS Template designed by TemplateMo.com  -->
</div><!-- end of container -->
<div align=center>Aplikasi ini dapat mengamankan <font color=red>data
login</font> dengan kriptografi</div></body>
</html>
```

5. Enkrip.php

```
<?php
$no=$_POST['no'];
```

```
$username=$_POST['username'];
$password=$_POST['password'];
$enkrip=$_POST['enkrip'];
$dekrip=$_POST['dekrip'];
$simpan=$_POST['simpan'];
$cari=$_POST['cari'];
$ubah=$_POST['ubah'];
$hapus=$_POST['hapus'];
$keygen=$_POST['kg'];
$key=$_POST['key'];
$j=0;
function enkrip($skata, $skey)
{
for($i=0;$i<strlen($skata);$i++)
{
$nkata[$i]=ord($skata[$i]); //rubah ASCII ke desimal
$nkunci[$j]=ord($skey[$j]); //rubah ASCII ke desimal
                                if($nkata[$i]==65){
                    $nkata[$i]=11;
                }elseif($nkata[$i]==66){
                    $nkata[$i]=12;
                }elseif($nkata[$i]==67){
                    $nkata[$i]=13;
                }elseif($nkata[$i]==68){
                    $nkata[$i]=14;
                }elseif($nkata[$i]==69){
                    $nkata[$i]=15;
                }elseif($nkata[$i]==70){
                    $nkata[$i]=21;
                }elseif($nkata[$i]==71){
                    $nkata[$i]=22;
                }elseif($nkata[$i]==72){
                    $nkata[$i]=23;
                }elseif($nkata[$i]==73){
                    $nkata[$i]=24;
                }elseif($nkata[$i]==75){
                    $nkata[$i]=25;
                }elseif($nkata[$i]==76){
                    $nkata[$i]=31;
                }elseif($nkata[$i]==77){
                    $nkata[$i]=32;
                }elseif($nkata[$i]==78){
                    $nkata[$i]=33;
                }elseif($nkata[$i]==79){
                    $nkata[$i]=34;
                }elseif($nkata[$i]==80){
```

```
    $nkata[$i]=35;
}elseif($nkata[$i]==81){
    $nkata[$i]=41;
}elseif($nkata[$i]==82){
    $nkata[$i]=42;
}elseif($nkata[$i]==83){
    $nkata[$i]=43;
}elseif($nkata[$i]==84){
    $nkata[$i]=44;
}elseif($nkata[$i]==85){
    $nkata[$i]=45;
}elseif($nkata[$i]==86){
    $nkata[$i]=51;
}elseif($nkata[$i]==87){
    $nkata[$i]=52;
}elseif($nkata[$i]==88){
    $nkata[$i]=53;
}elseif($nkata[$i]==89){
    $nkata[$i]=54;
}

if($nkunci[$j]==65){
    $nkunci[$j]=11;
}elseif($nkunci[$j]==66){
    $nkunci[$j]=12;
}elseif($nkunci[$j]==67){
    $nkunci[$j]=13;
}elseif($nkunci[$j]==68){
    $nkunci[$j]=14;
}elseif($nkunci[$j]==69){
    $nkunci[$j]=15;
}elseif($nkunci[$j]==70){
    $nkunci[$j]=21;
}elseif($nkunci[$j]==71){
    $nkunci[$j]=22;
}elseif($nkunci[$j]==72){
    $nkunci[$j]=23;
}elseif($nkunci[$j]==73){
    $nkunci[$j]=24;
}elseif($nkunci[$j]==75){
    $nkunci[$j]=25;
}elseif($nkunci[$j]==76){
    $nkunci[$j]=31;
}elseif($nkunci[$j]==77){
    $nkunci[$j]=32;
}elseif($nkunci[$j]==78){
```

```
            $nkunci[$j]=33;
        }elseif($nkunci[$j]==79){
            $nkunci[$j]=34;
        }elseif($nkunci[$j]==80){
            $nkunci[$j]=35;
        }elseif($nkunci[$j]==81){
            $nkunci[$j]=41;
        }elseif($nkunci[$j]==82){
            $nkunci[$j]=42;
        }elseif($nkunci[$j]==83){
            $nkunci[$j]=43;
        }elseif($nkunci[$j]==84){
            $nkunci[$j]=44;
        }elseif($nkunci[$j]==85){
            $nkunci[$j]=45;
        }elseif($nkunci[$j]==86){
            $nkunci[$j]=51;
        }elseif($nkunci[$j]==87){
            $nkunci[$j]=52;
        }elseif($nkunci[$j]==88){
            $nkunci[$j]=53;
        }elseif($nkunci[$j]==89){
            $nkunci[$j]=54;
        }
//echo"$nkata[$i] + $nkunci[$j]<br>";
$b[$i]=$nkata[$i] + $nkunci[$j]; //proses enkripsi
$c[$i]=chr($b[$i]); //rubah desimal ke ASCII
$x="$x$c[$i]";

        if($j!=strlen($skey))
        {
                $j=$j+1;
        }
        else
        {
                $j=0;
        }
}
return $x;
}
if($enkrip==true)
{
        $username=enkrip($username,$key);
        $password=enkrip($password,$key);
include"login.php";
}
```

```
function dekrip($skata, $skey)
{
for($i=0;$i<strlen($skata);$i++)
{
$nkata[$i]=ord($skata[$i]); //rubah ASCII ke desimal
$nkunci[$j]=ord($skey[$j]); //rubah ASCII ke desimal
                                if($nkunci[$j]==65){
                $nkunci[$j]=11;
              }elseif($nkunci[$j]==66){
                $nkunci[$j]=12;
              }elseif($nkunci[$j]==67){
                $nkunci[$j]=13;
              }elseif($nkunci[$j]==68){
                $nkunci[$j]=14;
              }elseif($nkunci[$j]==69){
                $nkunci[$j]=15;
              }elseif($nkunci[$j]==70){
                $nkunci[$j]=21;
              }elseif($nkunci[$j]==71){
                $nkunci[$j]=22;
              }elseif($nkunci[$j]==72){
                $nkunci[$j]=23;
              }elseif($nkunci[$j]==73){
                $nkunci[$j]=24;
              }elseif($nkunci[$j]==75){
                $nkunci[$j]=25;
              }elseif($nkunci[$j]==76){
                $nkunci[$j]=31;
              }elseif($nkunci[$j]==77){
                $nkunci[$j]=32;
              }elseif($nkunci[$j]==78){
                $nkunci[$j]=33;
              }elseif($nkunci[$j]==79){
                $nkunci[$j]=34;
              }elseif($nkunci[$j]==80){
                $nkunci[$j]=35;
              }elseif($nkunci[$j]==81){
                $nkunci[$j]=41;
              }elseif($nkunci[$j]==82){
                $nkunci[$j]=42;
              }elseif($nkunci[$j]==83){
                $nkunci[$j]=43;
              }elseif($nkunci[$j]==84){
                $nkunci[$j]=44;
              }elseif($nkunci[$j]==85){
                $nkunci[$j]=45;
```

```
            }elseif($nkunci[$j]==86){
               $nkunci[$j]=51;
            }elseif($nkunci[$j]==87){
               $nkunci[$j]=52;
            }elseif($nkunci[$j]==88){
               $nkunci[$j]=53;
            }elseif($nkunci[$j]==89){
               $nkunci[$j]=54;
            }

//echo"$nkata[$i] + $nkunci[$j]<br>";
$b[$i]=$nkata[$i] - $nkunci[$j]; //proses enkripsi
                              if($b[$i]==11){
               $b[$i]=65;
            }elseif($b[$i]==12){
               $b[$i]=66;
            }elseif($b[$i]==13){
               $b[$i]=67;
            }elseif($b[$i]==14){
               $b[$i]=68;
            }elseif($b[$i]==15){
               $b[$i]=69;
            }elseif($b[$i]==21){
               $b[$i]=70;
            }elseif($b[$i]==22){
               $b[$i]=71;
            }elseif($b[$i]==23){
               $b[$i]=72;
            }elseif($b[$i]==24){
               $b[$i]=73;
            }elseif($b[$i]==25){
               $b[$i]=75;
            }elseif($b[$i]==31){
               $ba[$i]=76;
            }elseif($b[$i]==32){
               $b[$i]=77;
            }elseif($b[$i]==33){
               $b[$i]=78;
            }elseif($b[$i]==34){
               $b[$i]=79;
            }elseif($b[$i]==35){
               $b[$i]=80;
            }elseif($b[$i]==41){
               $b[$i]=81;
            }elseif($b[$i]==42){
               $b[$i]=82;
```

```
        }elseif($b[$i]==43){
           $b[$i]=83;
        }elseif($b[$i]==44){
           $b[$i]=84;
        }elseif($b[$i]==45){
           $b[$i]=85;
        }elseif($b[$i]==51){
           $b[$i]=86;
        }elseif($b[$i]==52){
           $b[$i]=87;
        }elseif($b[$i]==53){
           $b[$i]=88;
        }elseif($b[$i]==54){
           $b[$i]=89;
        }

$c[$i]=chr($b[$i]); //rubah desimal ke ASCII
$x="$x$c[$i]";

        if($j!=strlen($skey)-1)
        {
                $j=$j+1;
        }
        else
        {
                $j=0;
        }
}
return $x;
}

if($dekrip==true)
{
        $username=dekrip($_POST['username'],$_POST['key']);
        $password=dekrip($_POST['password'],$_POST['key']);
include"login.php";
}
include "connect_db.php";
if($simpan==true)
{
        $queryq = "insert into login(no,username,password)
values('".$no."','".$username."','".$password."')";
        $results = mysql_query($queryq, $link) or die('Error query:
'.$queryq);
        echo "<script language=\"Javascript\">\n";
        echo "window.alert('Data Telah Disimpan');";
```

```
        echo "</script>";
include"login.php";
}
if($cari==true)
{
        $queryy = mysql_query("select * from login where no
='$no'",$link);
        $jumlh=mysql_fetch_array($queryy);
        $no=$jumlh[0];
        $username=$jumlh[1];
        $password=$jumlh[2];
        echo "<script language=\"Javascript\">\n";
        echo "window.alert('Data Ditemukan');";
        echo "</script>";
include"login.php";
}
if($ubah==true)
{
        $query = "update login set username = '$username', password =
'$password' where no ='".$no."'";
        $result = mysql_query($query, $link) or die('Error query:
'.$query);
        echo "<script language=\"Javascript\">\n";
        echo "window.alert('Data Telah Diubah');";
        echo "</script>";
include"login.php";
}
if($hapus==true)
{
        $query = mysql_query("delete from login where no
='".$no."',$link);
        echo "<script language=\"Javascript\">\n";
        echo "window.alert('Data Telah Dihapus');";
        echo "</script>";
include"login.php";
}
if($keygen==true)
{
$no=$_POST['no'];
$username=$_POST['username'];
$password=$_POST['password'];
$key=$_POST['key'];
for($i=0;$i<strlen($key);$i++)
{
$nkata[$j]=ord($username[$j]);
$nkatas=chr($nkata[$j]);
```

```
$nka="$nka$nkatas";
        if($j!=strlen($username)-1)
        {
                $j=$j+1;
        }
        else
        {
                $j=0;
        }
}
$username=$nka;
$j=0;
for($i=0;$i<strlen($key);$i++)
{
$nkatap[$j]=ord($password[$j]);
$nkatasp=chr($nkatap[$j]);
$nkap="$nkap$nkatasp";
        if($j!=strlen($password)-1)
        {
                $j=$j+1;
        }
        else
        {
                $j=0;
        }
}
$password=$nkap;
include"login.php";
}
?>
```

6. **Dekrip.php**

```
<?php
$no=$_POST['no'];
$username=$_POST['username'];
$password=$_POST['password'];
$dekrip=$_POST['dekrip'];
$simpan=$_POST['simpan'];
$cari=$_POST['cari'];
$ubah=$_POST['ubah'];
$hapus=$_POST['hapus'];
$keygen=$_POST['kg'];
$key=$_POST['key'];
$j=0;
function dekrip($skata, $skey)
```

```
{
for($i=0;$i<strlen($skata);$i++)
{
$nkata[$i]=ord($skata[$i]); //rubah ASCII ke desimal
$nkunci[$j]=ord($skey[$j]); //rubah ASCII ke desimal
                        if($nkunci[$j]==65){
            $nkunci[$j]=11;
          }elseif($nkunci[$j]==66){
            $nkunci[$j]=12;
          }elseif($nkunci[$j]==67){
            $nkunci[$j]=13;
          }elseif($nkunci[$j]==68){
            $nkunci[$j]=14;
          }elseif($nkunci[$j]==69){
            $nkunci[$j]=15;
          }elseif($nkunci[$j]==70){
            $nkunci[$j]=21;
          }elseif($nkunci[$j]==71){
            $nkunci[$j]=22;
          }elseif($nkunci[$j]==72){
            $nkunci[$j]=23;
          }elseif($nkunci[$j]==73){
            $nkunci[$j]=24;
          }elseif($nkunci[$j]==75){
            $nkunci[$j]=25;
          }elseif($nkunci[$j]==76){
            $nkunci[$j]=31;
          }elseif($nkunci[$j]==77){
            $nkunci[$j]=32;
          }elseif($nkunci[$j]==78){
            $nkunci[$j]=33;
          }elseif($nkunci[$j]==79){
            $nkunci[$j]=34;
          }elseif($nkunci[$j]==80){
            $nkunci[$j]=35;
          }elseif($nkunci[$j]==81){
            $nkunci[$j]=41;
          }elseif($nkunci[$j]==82){
            $nkunci[$j]=42;
          }elseif($nkunci[$j]==83){
            $nkunci[$j]=43;
          }elseif($nkunci[$j]==84){
            $nkunci[$j]=44;
          }elseif($nkunci[$j]==85){
            $nkunci[$j]=45;
          }elseif($nkunci[$j]==86){
```

```
            $nkunci[$j]=51;
        }elseif($nkunci[$j]==87){
            $nkunci[$j]=52;
        }elseif($nkunci[$j]==88){
            $nkunci[$j]=53;
        }elseif($nkunci[$j]==89){
            $nkunci[$j]=54;
        }
$b[$i]=$nkata[$i] - $nkunci[$j]; //proses enkripsi
        if($b[$i]==11){
            $b[$i]=65;
        }elseif($b[$i]==12){
            $b[$i]=66;
        }elseif($b[$i]==13){
            $b[$i]=67;
        }elseif($b[$i]==14){
            $b[$i]=68;
        }elseif($b[$i]==15){
            $b[$i]=69;
        }elseif($b[$i]==21){
            $b[$i]=70;
        }elseif($b[$i]==22){
            $b[$i]=71;
        }elseif($b[$i]==23){
            $b[$i]=72;
        }elseif($b[$i]==24){
            $b[$i]=73;
        }elseif($b[$i]==25){
            $b[$i]=75;
        }elseif($b[$i]==31){
            $b[$i]=76;
        }elseif($b[$i]==32){
            $b[$i]=77;
        }elseif($b[$i]==33){
            $b[$i]=78;
        }elseif($b[$i]==34){
            $b[$i]=79;
        }elseif($b[$i]==35){
            $b[$i]=80;
        }elseif($b[$i]==41){
            $b[$i]=81;
        }elseif($b[$i]==42){
            $b[$i]=82;
        }elseif($b[$i]==43){
            $b[$i]=83;
        }elseif($b[$i]==44){
```

```
            $b[$i]=84;
        }elseif($b[$i]==45){
            $b[$i]=85;
        }elseif($b[$i]==51){
            $b[$i]=86;
        }elseif($b[$i]==52){
            $b[$i]=87;
        }elseif($b[$i]==53){
            $b[$i]=88;
        }elseif($b[$i]==54){
            $b[$i]=89;
        }
$c[$i]=chr($b[$i]); //rubah desimal ke ASCII
if($nkata[$i]>=92)
{
}
else
{
$x="$x$c[$i]";
//echo"$nkata[$i] - $nkunci[$j]<br>";
        if($j!=strlen($skey)-1)
        {
                $j=$j+1;
        }
        else
        {
                $j=0;
        }
}
}
return $x;
}
if($dekrip==true)
{
        $username=dekrip($_POST['username'],$_POST['key']);
        $password=dekrip($_POST['password'],$_POST['key']);
include"log_in.php";
}
include "connect_db.php";
if($simpan==true)
{
        $queryq = "insert into login(no,username,password)
values('".$no."','".$username."','".$password."')";
        $results = mysql_query($queryq, $link) or die('Error query:
'.$queryq);
        echo "<script language=\"Javascript\">\n";
```

```
        echo "window.alert('Data Telah Disimpan');";
        echo "</script>";
include"log_in.php";
}
if($cari==true)
{
        $queryy = mysql_query("select * from login where no
='$no'",$link);
        $jumlh=mysql_fetch_array($queryy);
        $no=$jumlh[0];
        $username=$jumlh[1];
        $password=$jumlh[2];
        echo "<script language=\"Javascript\">\n";
        echo "window.alert('Data Ditemukan');";
        echo "</script>";
include"log_in.php";
}
if($ubah==true)
{
        $query = "update login set username = '$username', password =
'$password' where no ='".$no."'";
        $result = mysql_query($query, $link) or die('Error query:
'.$query);
        echo "<script language=\"Javascript\">\n";
        echo "window.alert('Data Telah Diubah');";
        echo "</script>";
include"log_in.php";
}
if($hapus==true)
{
        $query = mysql_query("delete from login where no
='".$no."',$link);
        echo "<script language=\"Javascript\">\n";
        echo "window.alert('Data Telah Dihapus');";
        echo "</script>";
include"log_in.php";
}
if($keygen==true)
{
$no=$_POST['no'];
$username=$_POST['username'];
$password=$_POST['password'];
$key=$_POST['key'];
for($i=0;$i<strlen($key);$i++)
{
$nkata[$j]=ord($username[$j]);
```

```
$nkatas=chr($nkata[$j]);
$nka="$nka$nkatas";
        if($j!=strlen($username)-1)
        {
                $j=$j+1;
        }
        else
        {
                $j=0;
        }
}
$username=$nka;
$j=0;
for($i=0;$i<strlen($key);$i++)
{
$nkatap[$j]=ord($password[$j]);
$nkatasp=chr($nkatap[$j]);
$nkap="$nkap$nkatasp";
        if($j!=strlen($password)-1)
        {
                $j=$j+1;
        }
        else
        {
                $j=0;
        }}
$password=$nkap;
include"log_in.php";
}
?>
```

7. **Tes_Login.php**

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>software company, free css template, website layout</title>
<meta name="keywords" content="software company, free css template, website layout, css, xhtml" />
<meta name="description" content="software company, free css template, website layout, xhtml css design" />
<link href="templatemo_style.css" rel="stylesheet" type="text/css" />
<script language="javascript" type="text/javascript">
function clearText(field)
```

```
{
   if (field.defaultValue == field.value) field.value = '';
   else if (field.value == '') field.value = field.defaultValue;
}
</script>
</head>
<body>
<center>
<div id="templatemo_container">
          <div id="templatemo_header_panel">
   <!--  Free CSS Template designed by TemplateMo.com  -->
          <div id="templatemo_site_title">
          <h1>Nihilist <span>Cipher</span></h1>
          <h2>Menggunakan Keystream Generator</h2>
       </div>
   </div> <!-- end of header panel -->
   <div id="templatemo_content_bottom" align=right>
<a href=login.php><button>Enkripsi</button></a>
<a href=log_in.php><button>Dekripsi</button></a>
<a href=tes_login.php><button>Tes Login
</button></a>        
     </div>
<?php
echo"
<html>
<head>
<title>Metode Nihilist Cipher</title>
</head>
<body>
<center><br>
<form action=proses.php method=POST>
<table border=1>
<tr>
          <td colspan=2 align=center><font color=yellow size=4>Silahkan
Login
          </font></td>
</tr>
<tr>
          <td><font color=red>Username</font></td>
          <td><input type=text name=username value='$username'></td>
</tr>
<tr>
          <td><font color=red>Password</font></td>
          <td><input type=text name=password value='$password'></td>
</tr>
<tr>
```

```
        <td><font color=red>Kunci Nihlist</font></td>
        <td><input type=text name=key value='$key'></td>
</tr>
<tr>
        <td colspan=2 align=right><input type=submit name=submit1
value='Keystream
Generator'>        &nb
sp;    <input type=submit name=submit0
value='Log In'></td>
</tr>
</table>
</form>
</center>
</body>
</html>";
?>
<br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><
br><br>
   <div id="templatemo_footer">
      Copyright © 2018 <a href="#"><strong><font
color=yellow>Universitas Potensi
Utama</font></strong></a>|<ahref="http://www.google.com"
target="_parent">Google</a><a title="free css templates"
href="http://www.gmail.com" target="_parent">Gmail</a>
   </div> <!-- end of footer -->
<!--  Free CSS Template designed by TemplateMo.com  -->
</div><!-- end of container -->
<div align=center>Aplikasi ini dapat mengamankan <font color=red>data
login</font> dengan kriptografi</div></body>
</html>
```

8. Proses.php

```
<?php
$nama=$_POST['username'];
$sandi=$_POST['password'];
$key=$_POST['key'];
$login=$_POST['submit0'];
$keygen=$_POST['submit1'];
include "connect_db.php";
$query = mysql_query("select * from login",$link);
$jmlh=mysql_fetch_array($query);
$j=0;
function enkrip($skata, $skey)
{
for($i=0;$i<strlen($skata);$i++)
{
```

```
$nkata[$i]=ord($skata[$i]); //rubah ASCII ke desimal
$nkunci[$j]=ord($skey[$j]); //rubah ASCII ke desimal
        if($nkata[$i]==65){
           $nkata[$i]=11;
        }elseif($nkata[$i]==66){
           $nkata[$i]=12;
        }elseif($nkata[$i]==67){
           $nkata[$i]=13;
        }elseif($nkata[$i]==68){
           $nkata[$i]=14;
        }elseif($nkata[$i]==69){
           $nkata[$i]=15;
        }elseif($nkata[$i]==70){
           $nkata[$i]=21;
        }elseif($nkata[$i]==71){
           $nkata[$i]=22;
        }elseif($nkata[$i]==72){
           $nkata[$i]=23;
        }elseif($nkata[$i]==73){
           $nkata[$i]=24;
        }elseif($nkata[$i]==75){
           $nkata[$i]=25;
        }elseif($nkata[$i]==76){
           $nkata[$i]=31;
        }elseif($nkata[$i]==77){
           $nkata[$i]=32;
        }elseif($nkata[$i]==78){
           $nkata[$i]=33;
        }elseif($nkata[$i]==79){
           $nkata[$i]=34;
        }elseif($nkata[$i]==80){
           $nkata[$i]=35;
        }elseif($nkata[$i]==81){
           $nkata[$i]=41;
        }elseif($nkata[$i]==82){
           $nkata[$i]=42;
        }elseif($nkata[$i]==83){
           $nkata[$i]=43;
        }elseif($nkata[$i]==84){
           $nkata[$i]=44;
        }elseif($nkata[$i]==85){
           $nkata[$i]=45;
        }elseif($nkata[$i]==86){
           $nkata[$i]=51;
        }elseif($nkata[$i]==87){
           $nkata[$i]=52;
```

```
}elseif($nkata[$i]==88){
   $nkata[$i]=53;
}elseif($nkata[$i]==89){
   $nkata[$i]=54;
}

if($nkunci[$j]==65){
   $nkunci[$j]=11;
}elseif($nkunci[$j]==66){
   $nkunci[$j]=12;
}elseif($nkunci[$j]==67){
   $nkunci[$j]=13;
}elseif($nkunci[$j]==68){
   $nkunci[$j]=14;
}elseif($nkunci[$j]==69){
   $nkunci[$j]=15;
}elseif($nkunci[$j]==70){
   $nkunci[$j]=21;
}elseif($nkunci[$j]==71){
   $nkunci[$j]=22;
}elseif($nkunci[$j]==72){
   $nkunci[$j]=23;
}elseif($nkunci[$j]==73){
   $nkunci[$j]=24;
}elseif($nkunci[$j]==75){
   $nkunci[$j]=25;
}elseif($nkunci[$j]==76){
   $nkunci[$j]=31;
}elseif($nkunci[$j]==77){
   $nkunci[$j]=32;
}elseif($nkunci[$j]==78){
   $nkunci[$j]=33;
}elseif($nkunci[$j]==79){
   $nkunci[$j]=34;
}elseif($nkunci[$j]==80){
   $nkunci[$j]=35;
}elseif($nkunci[$j]==81){
   $nkunci[$j]=41;
}elseif($nkunci[$j]==82){
   $nkunci[$j]=42;
}elseif($nkunci[$j]==83){
   $nkunci[$j]=43;
}elseif($nkunci[$j]==84){
   $nkunci[$j]=44;
}elseif($nkunci[$j]==85){
   $nkunci[$j]=45;
```

```
        }elseif($nkunci[$j]==86){
           $nkunci[$j]=51;
        }elseif($nkunci[$j]==87){
           $nkunci[$j]=52;
        }elseif($nkunci[$j]==88){
           $nkunci[$j]=53;
        }elseif($nkunci[$j]==89){
           $nkunci[$j]=54;
        }
//echo"$nkata[$i] + $nkunci[$j]<br>";
$b[$i]=$nkata[$i] + $nkunci[$j]; //proses enkripsi
$c[$i]=chr($b[$i]); //rubah desimal ke ASCII
$x="$x$c[$i]";
        if($j!=strlen($skey)-1)
        {
                $j=$j+1;
        }
        else
        {
                $j=0;
        }
}
return $x;
}

if($login==true)
{
$nama=enkrip($_POST['username'],$_POST['key']);
$sandi=enkrip($_POST['password'],$_POST['key']);
include "connect_db.php";
$querys = mysql_query("select * from login",$link);
while($jmlh=mysql_fetch_array($querys))
{
if(($nama==$jmlh[1])&&($sandi==$jmlh[2]))
{
        echo "<script language=\"Javascript\">\n
        window.alert('Login Berhasil');
        </script>";
        $key="";
        include"tes_login.php";
        exit(0);
}
}
        echo "<script language=\"Javascript\">\n
        window.alert('Login Gagal');
        </script>";
```

```
		$key="";
		include"tes_login.php";
		exit(0);
}

if($keygen==true)
{
$username=$_POST['username'];
$password=$_POST['password'];
$key=$_POST['key'];
for($i=0;$i<strlen($key);$i++)
{
$nkata[$j]=ord($username[$j]);
$nkatas=chr($nkata[$j]);
$nka="$nka$nkatas";
		if($j!=strlen($username)-1)
		{
			$j=$j+1;
		}
		else
		{
			$j=0;
		}
}
$username=$nka;

$j=0;
for($i=0;$i<strlen($key);$i++)
{
$nkatap[$j]=ord($password[$j]);
$nkatasp=chr($nkatap[$j]);
$nkap="$nkap$nkatasp";
		if($j!=strlen($password)-1)
		{
			$j=$j+1;
		}
		else
		{
			$j=0;
		}
}
$password=$nkap;

include"tes_login.php";
}
?>
```

	DOKUMEN LEVEL FORM	NO. DOKUMEN F-FTIK-18-06
	JUDUL SURAT PENGAJUAN JUDUL SKRIPSI	Tanggal Terbit : 05 Desember 2016 Tanggal Efektif : 10 Desember 2016
	AREA PROGRAM STUDI	Halaman : 1 dari 1 NO.REVISI 02

Medan, 04 Januari 2018

Hal : Pengajuan Judul Skripsi
Lamp : -

Kepada Yth,
Ketua Program Studi Teknik Informatika
di
Medan

Dengan hormat,

Yang bertanda tangan dibawah ini :

NIM	: 1410000358
Nama	: Haris Munandar
Program Studi	: Teknik Informatika
Peminatan	: Keamanan Komputer

Mengajukan Judul Skripsi sebagai berikut :

1. Modifikasi Metode Nihilist Cipher Dengan Pendekatan Keystream Generator Yang Diterapkan Pada Penyandian Sistem Login
2. Penerapan Metode Nihilist Cipher Dengan Pendekatan Keystream Generator Pada Pesan Teks Yang Disisipkan Pada Gambar Menggunakan Metode LSB

Atas perhatiannya saya ucapkan terima kasih.

Pemohon

(Haris Munandar)
1410000358

~~Judul Skripsi yang~~ disetujui No.....1..... /tanggal : 4/1/2018
Nama Pembimbing : I. Budi Triandi, M.Kom
II. Yustrizal, M.Kom

Ketua Program Studi

(Budi Triandi, M.Kom)

Dibuat rangkap 4 :
1. Program Studi TIF
2. Mahasiswa
3. Pembimbing I
4. Pembimbing II

UNIVERSITAS POTENSI UTAMA

(FAKULTAS TEKNIK DAN ILMU KOMPUTER)

SK. Mendikbud No.: 424/E/O/2014

Kampus : Jl. [illegible] Tanjung Morawa
E-mail : info@[illegible]
Website : [illegible]

FORMULIR PENDAFTARAN JUDUL SKRIPSI

I. UMUM *(Diisi oleh mahasiswa)*

Nama Mahasiswa : Hana Ayunda

NIM : 1[illegible]

Program Studi : Teknik Informatika

Nama Dosen Wali : [illegible]

II. PERSYARATAN PENGAMBILAN SKRIPSI : *(Diperiksa oleh Ka Prodi/Sek Prodi)*

1. Sudah Lulus Praktek Kerja Lapangan:
   ☑ Ya ☐ Tidak
2. Sudah Menjalani Kuliah Minimum 137 SKS dari Total 146 SKS untuk Kurikulum 2008
   ☑ Ya ☐ Tidak
3. Mengambil Kredit Mata Kuliah Skripsi:
   ☑ Ya ☐ Tidak
4. Sudah Membuat Proposal Judul Skripsi:
   ☑ Ya ☐ Tidak

(Ketentuan: Persyaratan harus dipenuhi)

Tgl 04/01/2018

III. DATA SKRIPSI :

1. Judul : *(Diisi oleh mahasiswa)*

   Mendeteksi Wajah Manusia Cepat Dengan Pendekatan Segmentasi Berwarna Yang Diterapkan Pada Pengenalan Sistem Login

   (Diisi oleh Bagian Program Studi)

2. Pembimbing I : [illegible]
3. Pembimbing II : [illegible]

Medan, 4-1-2018

Mengetahui / Kepala Prodi TIF

(Budi Prasetiyo, S.Kom)

Pembimbing I

([illegible])

Pembimbing II

([illegible])

Diterima oleh BAAK Tanggal 4-1-2018

([illegible])

	DOKUMEN LEVEL FORM	NO. DOKUMEN F-FTIK-18-07
	JUDUL SURAT PERNYATAAN KESEDIAAN PEMBIMBING SKRIPSI	Tanggal Terbit : 05 Desember 2016 Tanggal Efektif : 10 Desember 2016
	AREA PROGRAM STUDI	Halaman : 1 dari 1 NO.REVISI 02

Saya yang bertanda tangan dibawah ini

Nama	: Budi Triandi, M.kom
Pangkat/ Golongan	: III-C
Jabatan	: Ka- Prodi
Alamat	: Jl.KL.Yos Sudarso km 15,5 Medan Labuhan

Dengan ini menyatakan kesediaan saya untuk memberikan bimbingan skripsi atas nama mahasiswa berikut:

Nama	: Haris Munandar
NIM	: 1410000358
Program Studi	: Teknik Informatika
Jenjang Pendidikan	: Strata -1

Demikian surat pernyataan diperbuat dengan sebenarnya untuk dapat digunakan seperlunya

Medan, 31 Maret 2018

(Budi Triandi, M.kom)

	DOKUMEN LEVEL FORM	NO. DOKUMEN F-FTIK-18-07
	JUDUL SURAT PERNYATAAN KESEDIAAN PEMBIMBING SKRIPSI	Tanggal Terbit :05 Desember 2016 Tanggal Efektif :10 Desember 2016
	AREA PROGRAM STUDI	Halaman : 1 dari 1 NO.REVISI 02

Saya yang bertanda tangan dibawah ini

Nama	: Yusfrizal, M.kom
Pangkat/ Golongan	: III/B
Jabatan	: Asisten Ahli
Alamat	: Jl.Al-Huda Dusun IV Gang Kerabat No.73 Klumpang Kampung

Dengan ini menyatakan kesedian saya untuk memberikan bimbingan skripsi atas nama mahasiswa berikut:

Nama	: Haris Munandar
NIM	: 1410000358
Program Studi	: Teknik Informatika
Jenjang Pendidikan	: Strata -1

Demikian surat pernyataan diperbuat dengan sebenarnya untuk dapat digunakan seperlunya

Medan, 31 Maret 2018

(Yusfrizal, M.kom)

UNIVERSITAS POTENSI UTAMA

(FAKULTAS TEKNIK DAN ILMU KOMPUTER)

SK. Mendiknas R.I. No.: 183/D/O/2003

Kampus : J. K.L. Yos Sudarso Ahlo No. 3-5 Telp (061) [illegible] Fax (061) [illegible] (Depan Kodim Medan)

Website : [illegible]

Email : [illegible]

FORMULIR PENDAFTARAN SEMINAR HASIL SKRIPSI

I. UMUM *(Diisi oleh mahasiswa)*

Nama Mahasiswa : Heri Purnadi

NIM : 44[illegible]398

Program Studi : ☐ Teknik Industri (S1)

☑ Teknik Informatika (S1)

☐ Sistem Informasi (S1)

II. PERSYARATAN SEMINAR HASIL SKRIPSI *(Diperiksa oleh Pembimbing)*

1. Sudah Melaksanakan Bimbingan dan Menyerahkan Laporan Skripsi (Rangkap 4):
   Pembimbing I : ☑ Ya ☐ Tidak
   Pembimbing II : ☑ Ya ☐ Tidak
2. Sudah Melakukan Test Keberhasilan Program atau Alat Interface Sebagai Bahan Hasil Penelitian Skripsi
   Pembimbing I : ☑ Ya ☐ Tidak
   Pembimbing II : ☑ Ya ☐ Tidak

(Ketentuan: Persyaratan harus dipenuhi)

III. DATA SKRIPSI *(Diisi oleh mahasiswa)*

1. Judul :
   Mengukur Metode Naïve Bayes Dengan Perbedaan Kecocokan Berdasar Yang Ditampilkan Pada Penyimpanan Citra Ikan
2. Pembimbing I : Budi Tarigan, M.Kom
3. Pembimbing II : Yuhefizar, M.Kom

Medan, ...

Mengetahui Ketua Prodi TIF

(Budi Hartadi, M.Kom)

Pembimbing I

(Budi Tarigan, M.Kom)

Pembimbing II

(Yuhefizar, M.Kom)

Diterima oleh Bagian BAAK Tanggal 03-02-2014

(SITI)

UNIVERSITAS POTENSI UTAMA

(FAKULTAS TEKNIK DAN ILMU KOMPUTER)

SK. Mendiknas R.I. No.: 103/D/O/2003

Jl. K.L. Yos Sudarso KM 6,5 No. 3A Tanjung Mulia (061-6640525 Fax.106) (6626837) Tanjung Mulia-Medan

Website : http://www.potensiutama.ac.id

Email : info@potensiutama.ac.id

BERITA ACARA SEMINAR SKRIPSI

Pada hari ini Kamis tanggal 05 bulan April tahun 2018 telah dilaksanakan seminar Skripsi kepada :

I. Data Mahasiswa

NIM	: 14.0308358
Nama	: Haris Munandar
Tempat/Tgl. Lahir	: Medan, 18 Januari 1996
Program Studi	: Teknik Informatika
Judul Skripsi	: Modifikasi Metode Nihilist Cipher Dengan Pendekatan Keystream Generator Yang Diterapkan Pada Pengamanan Sistem Login

II. Tim Pembimbing

Pembimbing I

NIDN : 0.1902[illegible]0

Nama : Budi Trisndi, M.Kom

Jabatan Akademik : Lektor

No	Pembahasan BAB Skripsi	Keterangan
1		Pembahasan Ulang mengenai UML Dan R'
2		
3		
4		
5		
6		

Saran : .....

Demikian Berita Acara Seminar Skripsi ini dipergunakan sebagaimana mestinya.

Medan, 05 April 2018

Tim Pembimbing

Pembimbing I

(Budi Trisndi, M.Kom)

Diketahui/Disetujui

(Saidi Fitriansyah, M.Kom)

UNIVERSITAS POTENSI UTAMA

(FAKULTAS TEKNIK DAN ILMU KOMPUTER)

SK. Mendiknas R.I. No.: 103/D/O/2002

Kampus : J. K.L. Yos Sudarso KM 6,5 No. 3-A Telp. 061-6613525 Fax (061-6613810 Tanjung Mulia-Medan

Website : [illegible]

E-mail : [illegible]

BERITA ACARA SEMINAR SKRIPSI

Pada hari ini Kamis tanggal 05 bulan April tahun 2018 telah dilaksanakan seminar Skripsi kepada :

III. Data Mahasiswa

NIM	:	1412000358
Nama	:	Haris Munandar
Tempat/Tgl. Lahir	:	Medan, 18 Januari 1996
Program Studi	:	Teknik Informatika
Judul Skripsi	:	Modifikasi Metode Kriptografi Cipher Dengan Pendekatan Keystream Generator Yang Diterapkan Pada Penyandian Sistem Login

IV. Team Pembimbing

Pembimbing II		
NIDN	:	0109078005
Nama	:	Yusfriadi, M.Kom
Jabatan Akademik	:	Asisten Ahli

No	Pembahasan BAB Skripsi	Keterangan
1	BAB I	Perbaiki Identifikasi Masalah & Batasan Penelitian
2	BAB II	Perbaiki Kerangka
3	BAB III	Use case perbaiki .
4		
5		
6		

Saran : .....

.....

Demikian Berita Acara Seminar Skripsi ini dibuat dengan sebenarnya untuk dipergunakan seperlunya.

Medan, 05 April 2018

Team Pembimbing

Pembimbing II :

(Yusfriadi, M.Kom)

Diketahui/Disetujui Oleh :

Ketua Program Studi

(Ruth Ema Manalu, M. Kom)

	DOKUMEN LEVEL FORM	NO. DOKUMEN F-FTIK-18-07
	JUDUL SURAT PERNYATAAN KESEDIAAN PEMBIMBING SKRIPSI	Tanggal Terbit : 05 Desember 2016 Tanggal Efektif : 10 Desember 2016
	AREA PROGRAM STUDI	Halaman : 1 dari 1 NO.REVISI 02

Saya yang bertanda tangan dibawah ini

Nama	: Budi Triandi, M.kom
Pangkat/ Golongan	: III-C
Jabatan	: Ka- Prodi
Alamat	: Jl.KL.Yos Sudarso km 15,5 Medan Labuhan

Dengan ini menyatakan kesedian saya untuk memberikan bimbingan skripsi atas nama mahasiswa berikut:

Nama	: Haris Munandar
NIM	: 1410000358
Program Studi	: Teknik Informatika
Jenjang Pendidikan	: Strata -1

Demikian surat pernyataan diperbuat dengan sebenarnya untuk dapat digunakan seperlunya

Medan, 31 Maret 2018

(Budi Triandi, M.kom)

UNIVERSITAS POTENSI UTAMA

(FAKULTAS TEKNIK DAN ILMU KOMPUTER)

SK. Mendiknas R.I. No.: 103/D/O/2003

Kampus : Jl. K.L. Yos Sudarso KM 6,5 No. 3-A Telp. (061) 6615683 Fax (061) 6616819 Tanjung Mulia-Medan

Website : http://www.potensiutama.ac.id

E-mail : admin@potensiutama.ac.id

BERITA ACARA SEMINAR SKRIPSI

Pada hari ini Kamis tanggal 05 bulan April tahun 2018 telah dilaksanakan seminar Skripsi kepada :

III. Data Mahasiswa

NIM	:	14.0403053
Nama	:	Hans Munandar
Tempat/Tgl. Lahir	:	Medan, 18 Januari 1996
Program Studi	:	Teknik Informatika
Judul Skripsi	:	Modifikasi Metode Nihilist Cipher Dengan Pendekatan Keystream Generator Yang Diterapkan Pada Penyandian Sistem Log

IV. Team Pembanding

Pembanding II

NIDN	:	0127098403
Nama	:	Hardianto, M.Kom
Jabatan Akademik	:	Asisten Ahli

No	Pembahasan BAB Skripsi	Keterangan
	BAB 1	- Perjelaskan identifikasi masalah
2		- Perjelas Use Case
3		
4		
5		
6		

Saran : .....

.....

Demikian Berita Acara Seminar Skripsi ini diperbuat dengan sebenarnya untuk dipergunakan seperlunya.

Medan, 05 April 2018

Team Pembanding

Pembanding II

(Hardianto, M.Kom)

Ketua Program Studi

(Rahmat Widia Sembiring, S.Kom, M.I.T)

	DOKUMEN LEVEL FORM	NO. DOKUMEN F-FTIK-20-08
	JUDUL DAFTAR HADIR MAHASISWA PESERTA SEMINAR HASIL SKRIPSI	Tanggal Terbit : 05 Desember 2016 Tanggal Efektif : 10 Desember 2016
	AREA PROGRAM STUDI	Halaman : 1 dari 1 NO.REVISI 02

PROGRAM STUDI : TEKNIK INFORMATIKA

JAM	NAMA DOSEN	TANDA TANGAN				NAMA MAHASISWA	TANDA TANGAN
		Pembimbing I	Pembimbing II	Pembanding I	Pembanding II		
09.00 s/d 10.00	Budi Tritoni, M.Kom					Haris Munandar	
09.00 s/d 10.00	Yusfrizal, M.Kom						
09.00 s/d 10.00	Iwan Fitrianto Rahmad, M.Kom						
09.00 s/d 10.00	Hardianto, M.Kom						

Ketua Program Studi Teknik Informatika

( )

UNIVERSITAS POTENSI UTAMA

(FAKULTAS TEKNIK DAN ILMU KOMPUTER)

SK. Mendiknas No. : 424/D/O/2014

Kampus : Jl. T.M. Yus Sukma No. 3 A-B Tp. 082366395 - Medan Marelan

E-mail : info@dosen.potensiutama.ac.id

Website : http://www.potensiutama.ac.id

FORMULIR PENDAFTARAN UJIAN SIDANG SKRIPSI II

I. UMUM *(Diisi oleh mahasiswa)*

Nama Mahasiswa : Hari Mirandi

NIM : 1802010355

Program Studi : ☐ Teknik Industri (S.1)

☒ Teknik Informatika (S.1)

☐ Sistem Informasi (S.1)

II. PERSYARATAN UJIAN SIDANG SKRIPSI *(Diperiksa oleh Pembanding)*

1. Sudah Melaksanakan Seminar Hasil Skripsi :
   Pembimbing I : ☒ Ya ☐ Tidak
   Pembimbing II : ☒ Ya ☐ Tidak
2. Sudah Melaksanakan Bimbingan dan Menyiapkan Laporan Skripsi (Rangkap 5) :
   Pembimbing I : ☒ Ya ☐ Tidak
   Pembimbing II : ☒ Ya ☐ Tidak
3. Sudah Ditanda Tangannya Lembar Persetujuan Sidang Skripsi Oleh Pembimbing Sesuai dengan Format yang Diberikan :
   Pembimbing I : ☒ Ya ☐ Tidak
   Pembimbing II : ☒ Ya ☐ Tidak

(Keterangan: Persyaratan harus dipenuhi)

III. DATA SKRIPSI: *(Diisi oleh mahasiswa)*

1. Judul :
   Menerapkan Metode Naïve Bayes Dengan Pendekatan Kriteria Pemerata Yang Tepat Dalam Pada Pengambilan Ujian Ujian
2. Pembimbing I : Hadi Tirandi, M.Kom
3. Pembimbing II : Yuhefizar, M.Kom
4. Pembanding I : Widi Sinaga, Rahmad, M.Kom
5. Pembanding II : Hartarto, M.Kom

Medan, ...

Mengetahui Ketua Prodi	Pembimbing I	Pembimbing II
(Hadi Tirandi, M.Kom)	(Hadi Tirandi, M.Kom)	(Yuhefizar, M.Kom)

Diterima oleh Bagian BAAK Tanggal : 1 September 2020

( )