Jurnal Sarjana Teknik Informatika
Volume 2 Nomor 1, Februari 2014
e-ISSN: 2338-5197

PENGEMBANGAN MODUL ENKRIPSI DAN DEKRIPSI PADA PHP DENGAN MODIFIKASI METODE KRIPTOGRAFI VIGENERE CIPHER DAN CIPHER BLOCK CHAINING (Studi Kasus pada geekybyte.com)

[1]Prade Septo Nugroho, [2]Eko Aribowo (0006027001)

[1,2] Program Studi Teknik Informatika
Universitas Ahmad Dahlan
Prof. Dr. Soepomo, S.H., Janturan, Umbulharjo, Yogyakarta 55164
[2]Email: ekoab@tif.uad.ac.id

ABSTRAK

Penggunaan fungsi hash pada pengamanan data atau informasi pada sebuah web site sudah tidak aman lagi, karena memiliki kelemahan berupa collision. Pengamanan yang dilakukan tidak tergantung pada kerahasiaan metode atau algortima yang digunakan, tetapi pada kreativitas memodifikasi dan mengimplementasikan algoritma atau metode yang digunakan. Berdasarkan keadaan di atas modifikasi dan implementasi algoritma kriptografi Vigenere Cipher dan Cipher Block Chaining pada pengamanan data sebuah web site sangat dibutuhkan agar data atau informasi tidak disalahgunakan.

Subjek pada penelitian ini adalah pengembangan algoritma kriptografi melalui metode modifikasi dan implementasi vigenere cipher dan cipher block chaining. Langkah penelitian yang dilakukan adalah dengan melakukan study literatur, analisa metode vigenere cipher dan cipher block chaining, merancang modifikasi vigenere cipher dan cipher block chaining untuk proses enkripsi dan dekripsi, melakukan percobaan dan implementasi pada sebuah web site dengan bahasa perograman PHP.

Dari penelitian ini akan dihasilkan "Pengembangan Modul Enkripsi Dan Dekripsi Pada PHP Dengan Modifikasi Metode Kriptografi Vigenere Cipher Dan Cipher Block Chaining (Studi kasus pada geekybyte.com)". Informasi yang dihasilkan yaitu hasil enkripsi data dari web yang tidak bisa dibaca oleh orang lain.

Kata kunci : Keamanan, Kriptografi, Vigenere Cipher, Cipher Block Chaining, Modifikasi

1. PENDAHULUAN

 e-ISSN: 2338-5197

Hasil survey yang dilakukan oleh High Technology Crime Investigation Associations (HTCIA) dari 445 responden, sekitar 14% membutuhkan peningkatan keamanan pada data, yaitu peningkatan privacy dan policy yang lebih baik dan 56,4 % membutuhkan pelatihan dan pengetahuan tentang pengamanan data pada komputer atau jaringan.[9] Hal ini menunjukan keamanan komputer sangat dibutuhkan untuk mencegah timbulnya lebih banyak kerugian. Tujuan utama keamanan komputer yaitu menjaga kerahasiaan data (confidentiality), menjaga agar data tetap utuh (integrity), dan menyediakan data ketika diperlukan (availability).[15]

Pengamanan data masih bersifat standar dengan menggunakan fungsi hash, yaitu Message Digest atau Secure Hash Algorithm. Fungsi hash mengubah string input menjadi string output dengan panjang tertentu yang disebut nilai hash. MD5 merupakan fungsi hash yang sangat populer. Orang menganggap MD5 sebagai algoritma enkripsi. MD5 digunakan dalam kriptografi, namun sebenarnya MD bukan algoritma enkripsi. Enkripsi yaitu mengubah plaintext menjadi ciphertext yang ukurannya berbanding lurus dengan ukuran file aslinya.[16] Semakin panjang plaintext maka hasil enkripsinya juga semakin panjang. Hasil enkripsi bisa dikembalikan ke plaintext semula dengan proses dekripsi. Jadi enkripsi adalah fungsi dua arah dan reversible.

Berbeda dengan enkripsi, fungsi hash tidak butuh kunci dan sifatnya hanya satu arah, yaitu dari teks masukan menjadi nilai hash yang panjangnya selalu sama. Setelah menjadi nilai hash, tidak ada fungsi yang bisa mengembalikan nilai hash itu menjadi teks semula. Fungsi hash mempunyai kelemahan utama yang disebut dengan collision. Demonstrasi yang dilakukan Selinger pada fungsi hash yaitu MD5 membuktikan adanya collision pada fungsi hash tersebut. Pengujian tersebut dilakukan pada sistem operasi Windows version dan Linux version (i386).[13] Algoritma MD5 dianggap sudah tidak aman lagi oleh para pengembang software, hal ini terjadi setelah kebocoran lebih dari 6,46 juta hash password pada situs LinkedIn. [17] Keamanan penggunaan MD5 dalam pengamanan data juga sudah tidak aman lagi. Selain adanya collision fungsi hash pada MD5, beredar tabel-tabel heksadesimal untuk membalikkan kode dan dekriptor dari MD5.[2]

Penggunaan kriptografi klasik tanpa adanya modifikasi algoritma dalam menangani adanya collision masih belum efisien. Modifikasi kriptografi dalam pengamanan data masih jarang dilakukan karena kurangnya pengetahun dari pengguna web site untuk mengamankan data. Pengamanan data yang masih standar dan tidak adanya pengetahuan untuk memodifikasi metode yang digunakan untuk mengamankan data akan membuat data mudah untuk dilihat, diambil, dan diakses oleh pihak yang tidak berhak.

Salah satu algoritma klasik yang populer dan tidak begitu rentan dengan metode pemecahan sandi atau analisis frekuensi adalah vigenere cipher.[6] Vigenere cipher memiliki cara kerja yang sederhana, tetapi sulit untuk dipecahkan karena menggunakan metode polialfabetik. Kemajuan teknologi membuat algoritma klasik tidak aman lagi untuk digunakan sebagai algrotima enkripsi. Penggunaan algoritma modern dipadukan dengan algoritma modern akana meningkatkan keamanan data. Cipher Block Chaining (CBC) merupakan salah satu kriptografi yang memecah plainteks menjadi blok-blok kemudian dienkripsi dengan kunci yang tetap. Hasil enkripsi dari block akan digunakan

untuk melakukan enkripsi plainteks berikutnya. Kelemahan metode ini yaitu hanya menggunakan satu kunci dalam melakukan enkripsi.

2. KAJIAN PUSTAKA

Pada penelitian yang dilakukan mengacu pada penelitian yang dilakukan oleh Muhammad Iqbal Faruqi yang berjudul *"Modifikasi Vigenere Cipher dengan Kunci Bergeser*".[6] Pada penelitian tersebut dijelaskan tentang kelemahan vigenere cipher yang bisa dipecahkan dengan metode kasiski. Pada penelitian yang dilakukan oleh Fatardhi Rizky Andhika dengan judul "*Modifikasi Vigenere Cipher dengan Menggunakan Caesar Cipher dan Enkripsi Berlanjut untuk Pembentukan Key-nya*".[1] Penelitian tersebut membahas tentang keamanan *vigenere cipher* modifikasi menjadi lebih sulit untuk dipecahkan oleh kriptanalis dari pada *vigenere cipher* biasa. Selain itu juga, tingkat keamanan vigenere cipher modifikasi menjadi meningkat apabila menggunakan kunci yang panjang. Pergeseran kunci pada algoritma klasik dapat diterapkan pada algoritma modern yaitu dengan *Cipher Block Chaining* (CBC) dengan merubah plainteks menjadi ASCII kemudian menggeser setiap bit kunci.

2.1. Dasar Kriptografi

Kriptografi (*cryptography*) merupakan ilmu dan seni penyimpanan pesan, data, atau informasi secara aman. Kriptografi (*cryptography*) berasal dari bahasa Yunani yaitu dari kata *Crypto* (tersembunyi) dan *Graphia* (tulisan). *Cryptanalysis* adalah aksi untuk memecahkan mekanisme kriptografi dengan cara mendapatkan plaintext atau kunci dari ciphertext. [4]

2.2. Kriptografi Simetris dan Asimetris

Kriptografi simetri disebut juga sebagai kriptografi konvensional adalah algoritma kriptografi yang menggunakan kunci enkripsi yang sama dengan kunci dekripsinya. Kriptografi simetri sering disebut sebagai algoritma kunci rahasia, algortima kunci. Kelebihan kriptografi simetri dari kriptografi asimetri adalah lebih cepat.[14]

2.3. Fungsi Hash

Fungsi hash adalah fungsi yang mengambil dan menghitung beberapa input string atau pesan kemudian mengeluarkan output dengan panjangan string n atau panjang yang sudah ditentukan. [4] Fungsi hash tidak seperti algoritma kriptografi lainnya, fungsi hash tidak memiliki kunci. Fungsi hash pada kriptografi yaitu SHA-1 (*Secure Hash Algorithm*) dan MD5 (*Message Digest*).

2.4. Vigenere Cipher

Vigenere cipher merupakan jenis cipher abjad majemuk yang paling sederhana. *Vigenere cipher* menerapkan metode substitusi poli alfabetik dan termasuk ke dalam kategori kunci simetris dimana kunci yang digunakan untuk proses enkripsi adalah sama

dengan kunci yang digunakan untuk proses dekripsi.Tujuan utama dari *Vigenere cipher* ini adalah menyembunyikan keterhubungan antara plainteks dan cipherteks dengan menggunakan kata kunci sebagai penentu pergeseran karakternya.[1]

2.5. Cipher Block Chaining

Ada dua ide utama di balik *Cipher Blok Chaining* modus (CBC). Pertama, enkripsi semua blok adalah "dirantai bersama-sama". Kedua, enkripsi secara acak dengan menggunakan inisialisasi vektor.[11] Mode ini menerapkan umpan-balik (*feedback*) pada sebuah blok, dalam hal ini hasil enkripsi blok sebelumnya diumpanbalikan ke dalam enkripsi blok yang *current*. Blok plainteks yang current di-XOR-kan terlebih dahulu dengan blok cipherteks hasil enkripsi sebelumnya, selanjutnya hasil peng-XOR-an masuk ke dalam fungsi enkripsi. Pada mode CBC, setiap blok cipherteks tidak hanya tergantung pada blok plainteks tetapi juga pada seluruh blok plainteks sebelumnya.[10]

3. METODE PENELITIAN

Subjek penelitian yang akan dibahas dalam tugas akhir ini adalah "Pengembangan Modul Enkripsi Dan Dekripsi Pada Php Dengan Modifikasi Metode Kriptografi Vigenere Cipher Dan Cipher Block Chaining (Studi Kasus pada geekybyte.com)". Sistem ini diharapkan dapat meningkatkan keaman data yang disimpan pada sebuah web site yaitu berupa ekripsi data penting. Adapun metode pengumpulan data yang dilakukan dalam penulisan tugas akhir ini adalah observasi, wawancara, dan studi pustaka. Proses yang dilakukan dalam tahap perancangan sistem yaitu merancang proses dan merancang algoritma.

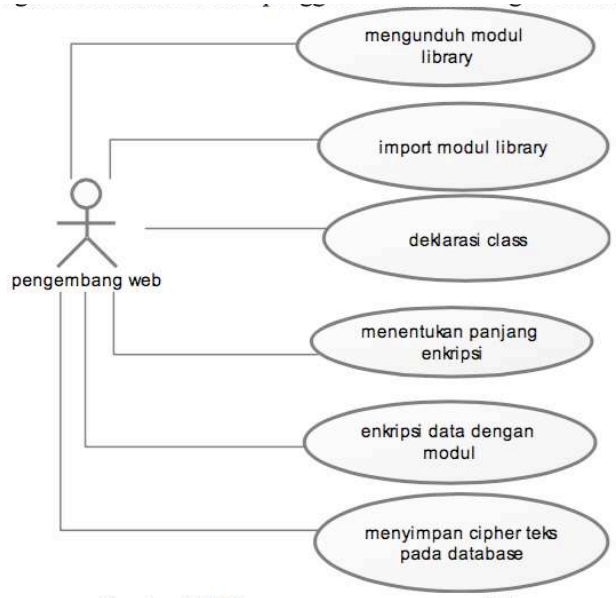
Implementasi yang dilakukan yaitu bagaimana menggunakan modul pada sistem. Mulai dari *import* sampai proses enkripsi dan dekripsi, serta pemasangan modul untuk bisa digunakan dalam enkripsi data pasa database. Sistem ini diimplementasikan dengan bahasa pemrograman PHP berbasis *Object Oriented Programming* (OOP). Paket server yang digunakan yaitu XAMPP didalamnya terdapat Apache, PHP, dan MySQL. *Object Oriented Programming* (OOP) digunakan untuk mempermudah implementasi algoritma kriptografi agar dapat digunakan oleh web developer dalam bentuk library sendiri.

Pengujian ini dilakukan dengan dua metode, yaitu *black box test* dan *black box test*. *Black box test* dilakukan pada perancangan algoritma yang telah dimodifikasi. *White box test* dilakukan dengan mengamati keluaran dari berbagai masukan.

4. Hasil dan Pembahasan

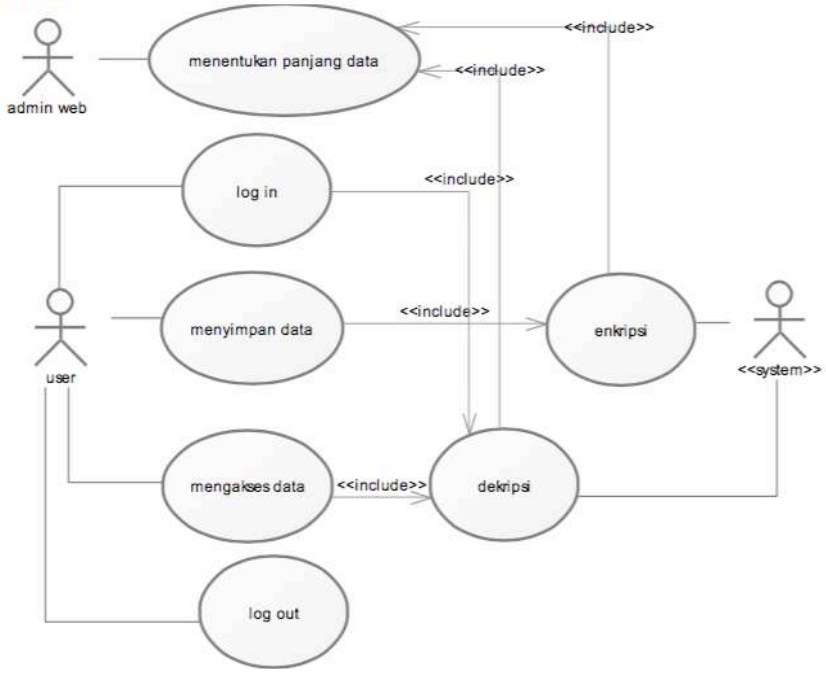
Penelitian ini dapat dihasilkan sebuah modul *cryptography* untuk mengamankan data pada sebuah web sites dengan memodifikasi metode *vigenere cipher* dan *cipher block chaining*. Modul yang dihasilkan dalam OOP sehingga bisa digunakan pada aplikasi yang berbasis PHP baik *structural* atau *object oriented*, panjang dari hasil enkripsi, serta melakukan enkripsi password dan data lain dengan menggunakan fungsi sederhana. *Use case* penggunaan modul sebagai berikut:

 e-ISSN: 2338-5197



Gambar 20. Use case penggunaan modul

Pada use case di atas pengembang web terlebih dahulu mengunduh modul library yang akan digunakan pada situs web yang telah disediakan. Setelah modul berhasil diunduh pengembang web selanjutnya mengimport library pada sistem yang akan digunakan. Deklarasi terhadap class dilakukan untuk menentukan panjang hasil enkripsi dan melakukan enkripsi. Setelah data dienkripsi maka data akan disimpan pada database.



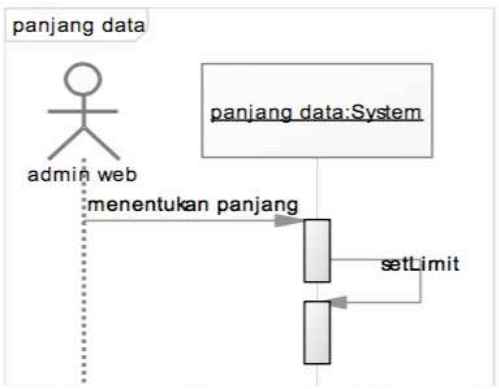
Gambar 21. Use Case enkripsi dan dekripsi

Pada use case di atas, admin web menentukan panjang data yang akan digunakan dalam sebuah web. Setelah panjang data ditentukan maka system dapat melakukan proses

 e-ISSN: 2338-5197

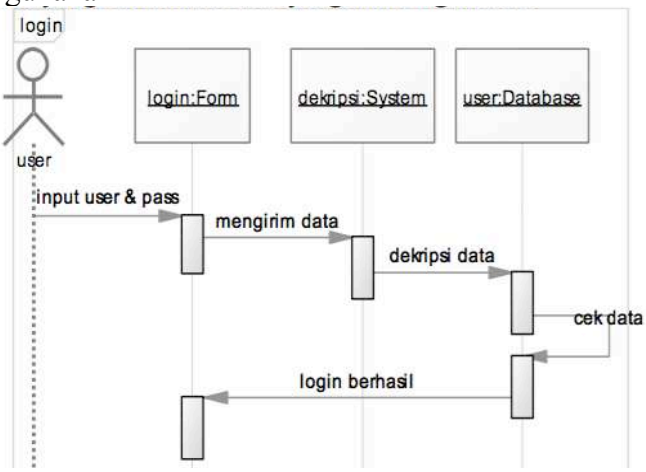
enkripsi dan dekripsi. Ketika user login maka akan dilakukan dekripsi terhadap username dan password yang dimasukkan oleh user.

Saat user menyimpan data maka data akan dienkripsi oleh system berdasarkan panjang data yang telah ditentukan oleh admin web, kemudian data akan disimpan oleh system. Saat user mengakses data, data akan didekripsi sebelum bisa dibaca oleh user. Hal tersebut untuk menghindari pengaksesan oleh pihak yang tidak berhak untuk mengakses data.



Gambar 30. Sequence diagram menentukan panjang data

Admin web menentukan panjang data yang akan digunakan sebagai default dalam enkripsi data pada system. Panjang data akan digunakan dalam setiap proses enkripsi dan dekripsi dari algoritma kriptografi yang telah dimodifikasi. Setelah panjang data ditentukan maka system akan melakukan setLimit yang digunakan sebagai default enkripsi dan dekripsi data. Jika panjang data yang ditentukan kurang dari panjang data default, maka panjang data yang digunakan yaitu panjang data default. Akan tetapi, jika panjang data melebihi default panjang data sistem, maka panjang data yang ditentukan user yang akan digunakan

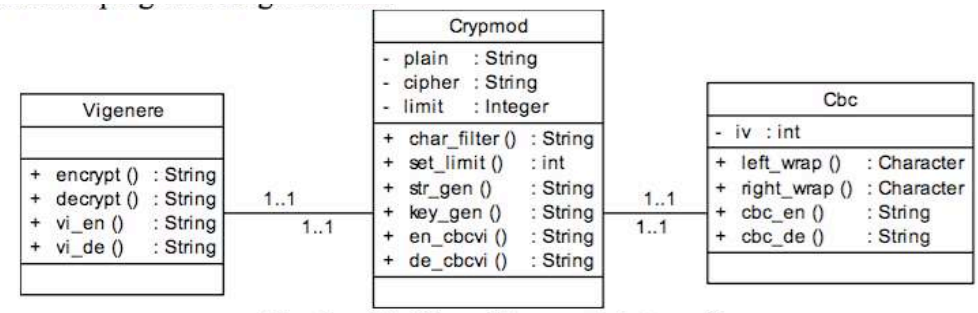


Gambar 31. Sequence diagram login

User memasukkan username dan password pada form login yang tersedia. Data kemudian dikirim untuk dienkripsi oleh system. Data yang sudah dienkripsi akan dicek pada database. Jika data sesuai maka login berhasil dilakukan oleh user.

Class diagram dari perancangan sistem yang akan digunakan untuk penerapan modifikasi kriptografi sebagai berikut:

 e-ISSN: 2338-5197



Gambar 34. Class diagram kriptografi

Pada class vigenere terdapat fungsi encrypt() yang berisi algoritma dari vigenere cipher yang digunakan untuk melakukan enkripsi plain teks menjadi cipher teks. Fungsi decrypt() berisi algoritma vigenere cipher untuk melakukan dekripsi cipher teks. Fungsi encrypt() dan decrypt() hanya melakukan proses enkripsi dan dekripsi terhadap satu karakter dengan satu kunci. Fungsi vi_en() dan vi_de() digunakan untuk melakukan enkripsi dan dekripsi terhadap seluruh string yang dimasukkan. Seluruh fungsi pada class Vigenere bersifat public agar dapat diakses oleh class lain.

Class Cbc terdapat atribut iv yang bersifat private. Atribut iv digunakan sebagai inisial vector yang akan digunakan untuk melakukan enkripsi chaining pada plain teks awal. Fungsi cbc_en() digunakan untuk melakukan enkripsi string dengan metode cipher block chaining, sedangkan cbc_de() merupakan fungsi untuk melakukan dekripsi cipher teks. Pada class Cbc plain teks dirubah menjadi biner kemudian dilakukan proses XOR pada masing-masing proses enkripsi dan dekripsi. Fungsi left_wrap() digunakan untuk menggeser bit satu langkah ke kiri. Sedangkan fungsi right_wrap() digunakan untuk menggeser bit satu langkah ke kanan.

Fungsi-fungsi pada class Cbc bersifat public agar dapat diakses oleh class lain. Class Crypmod merupakan class hasil modifikasi antara class Vigenere dan class Cbc. Pada class Crypmod terdapat atribut plain, cipher, dan limit. Seluruh atribut bersifat private karena hanya diakses oleh class Crypmod sendiri. Atribut plain merupakan atribut yang digunakan untuk menampung hasil dari proses dekripsi yaitu plain teks. Atribut cipher merupakan atribut yang akan digunakan untuk menampung hasil dari proses enkripsi yaitu cipher teks. Limit merupakan atribut untuk menampung panjang data yang akan digunakan untuk melakukan generate panjang.

Fungsi-fungsi yang terdapat pada class Cbc yaitu char_filter(), set_limit(), str_gen(), key_gen(), en_cbcvi(), dan de_cbcvi(). FUngsi char_filter() digunakan untuk menyaring karakter yang dimasukkan oleh admin web atau user. Fungsi ini memperbolehkan karakter dengan kode ASCII dengan nilai desimal antara 48 sampai dengan 122. Fungsi set_limit() digunakan untuk mengatur panjang cipher teks yang akan digunakan dari hasil proses enkripsi. Fungsi str_gen() digunakan untuk mengatur panjang plain teks agar sesuai dengan panjang batas yang telah ditentukan berdasarkan fungsi setLimit. Fungsi key_gen() digunakan untuk mengatur kata kunci agar sesuai dengan panjang yang telah ditentukan pada fungsi set_limit().

Fungsi en_cbcvi() digunakan untuk melakukan enkripsi dengan metode vigenere chipher, kemudian hasil enkripsi berupa cipher teks akan dienkripsi lagi dengan proses cipher block chaining. Proses dekripsi dilakukan dengan menggunakan fungsi

de_cbcvi(), cipher teks didekripsi dengan metode vigenere cipher kemudian hasil plain teks akan didekripsikan lagi dengan metode cipher block chaining.

Implementasi penggunaan modul enkripsi pada sistem sebagai berikut:

1. Import terlebih dahulu file library modifikasi kriptografi (Crypmod.php, Vigenere.php, dan Cbc.php) yang telah didownload pada web geekybyte.com.
2. Deklarasikan class Crypmod yang akan digunakan dan tentukan panjang hasil enkripsi yang kita inginkan.
3. Misalnya kita akan menggunakan username sebagai plain teks dan password sebagai kata kunci dan fungsi en_cbcvi() sebagai metode enkripsi.
4. Menyimpan data hasil enkripsi (cipher teks) ke dalam data base.

Implementasi penggunaan modul dekripsi pada sistem sebagai berikut:

1. Import terlebih dahulu file library modifikasi kriptografi (Crypmod.php, Vigenere.php, dan Cbc.php) yang telah didownload pada web geekybyte.com.
2. Deklarasikan class Crypmod yang akan digunakan dan sesuaikan dengan panjang yang kita gunakan untuk melakukan enkripsi.
3. Enkripsi data yang telah diinput untuk dicocokan dengan database.
4. Ambil data password yang tersimpan pada database dan simpan pada sebuah variabel.
5. Dekripsi data yang telah diambil dari database.
6. Kemudian lakukan proses login dengan mencocokan plainteks.

5. SIMPULAN

Berdasarkan hasil penelitian dan pembahasan, maka dapat disimpulkan hal sebagai berikut:

1. Dari penelitian dihasilkan modul enkripsi dan dekripsi pada PHP dengan modifikasi metode kriptografi Vigenere Cipher dan Cipher Block Chaining (CBC).
2. Modul mampu melakukan generate panjang terhadap hasil enkripsi atau cipher teks berdasarkan panjang yang telah ditentukan.
3. Modul melakukan enkripsi terhadap karakter ASCII dengan kode desimal 48 – 122.
4. Modul dapat digunakan pada PHP dengan metode structural atau Object Oriented Programming (OOP).

DAFTAR PUSTAKA

[1] Andhika, Fatardhi Rizky. 2011. *Modifikasi Vigenere Cipher dengan Menggunakan Caesar Cipher dan Enkripsi Berlanjut untuk Pembentukan Key-nya*. Bandung. Institut Teknologi Bandung.

[2] Anggoro, Akhmad Ratriono, dkk. *Kriptografi Message Digest sebagai Salah Satu Enkripsi Modern*. Bandung: Institut Teknologi Bandung.

[3] Booch, Grady, dkk. 2005. *The Unified Modeling Language User Guide Second Edition*. Amerika Serikat: Addison Wesley Professional.

[4] Delfs, Hans, and Helmut Knebl. 2007. *Introduction to Cryptography: Principles and Applications*. Verlag Berlin Heidelberg: Springer.

[5] Denis, Tom St. and Simon Johnson. 2007. *Cryptography for Developers*. Canada: O'Reilly Media. Inc.

 e-ISSN: 2338-5197

[6] Faruqi, Muhammad Iqbal. 2010. *Modifikasi Vigenere Cipher dengan Kunci Bergeser*. Bandung: Institut Teknologi Bandung.

[7] Fowler, Martin dan Kendall Scott. 1999. *ML Distilled Second Edition A Brief Guide to the Standard Object Modeling Language*. Amerika Serikat: Addison Wesley Professional.

[8] Kurniawan, Yusuf. 2004. *Kriptografi: Keamanan Internet dan Jaringan Telekomunikasi.* Bandung: Informatika.

[9] Monkhouse, H. Duncan. 2011. *2011 Repost on Cyber Crime Investigation*. HTCIA.Inc.

[10] Munir, Rinaldi. 2006. *Kriptografi*. Bandung: Informatika.

[11] Paar, Christof. and Jan Pelzl. 2010. *Understanding Criptography*. Jerman: Springer.

[12] Powers, David. 2010. *PHP Solutions Dynamic Web Design Made Easy*. Amerika Setikat: An Apress Company.

[13] Selinger, Peter. 2006. *MD5 Collision Demo*. Diakses dari http://www.mathstat.dal.ca/~selinger/md5collision/ pada tanggal 26 Desember 2012.

[14] Sianturi, Vera Magdalena. 2008. *Studi dan Implementasi Data Dengan Tanda Tangan Digital*. Medan: Universitas Sumatra Utara.

[15] Simarmata, Janner. 2006. *Pengenalan Teknologi dan Informasi*. Yogyakarta: Andi. Wicaksono, Rizki. 2009. *MD5 Itu Berbahaya, Titik!*. Diakses dari http://www.ilmuhacking.com/cryptography/md5-itu-berbahaya/ pada tanggal 13 April 2012.

[16] Whittaker, Zack. 2012. *MD5 password scrambler 'no longer safe'*. Diakses dari http://www.zdnet.com/blog/security/md5-password-scrambler-no-longer-safe/12317 pada tanggal 26 Desember 2012.

[17] ---. 2012. *Stream Cipher*. Diakses dari http://en.wikipedia.org/wiki/Stream_cipher pada tanggal 10 April 2012.

[18] ---. 2012. *Block Cipher*. Diakses dari http://en.wikipedia.org/wiki/Block_cipher pada tanggal 10 April 2012.