Jurnal SPIRIT Vol. 12 No. 1 Mei 2020, hal 20-25 P- ISSN : 2085 – 3092
E- ISSN : 2721 – 057X

IMPLEMENTASI ENKRIPSI URL PADA WEBSITE MENGGUNAKAN METODE BASE64 DAN ROTATION13

Mochammad Firman Arif ; Muhammad Misdram
Program Studi Informatika, Universitas Merdeka Pasuruan,
mochammadfirmanarif@gmail.com

Abstract: *The development of technology in this era is getting faster this is unknown from the distribution of information which is also developing, the internet is one of the media of the dissemination of information that is very broad so fast. However, the services provided by each of these sites are one of several related issues: cross-site scripting, information leakage, authentication and authorization, Session management, SQL Injection, CSRF and others. Therefore based on this security issue and also some of the references above make researchers want to implement a security made with the introductory URL on the website using several encryption algorithms summarized in BASE64 and ROT13 as actions against attacks that attack the system.*

Keywords :*: URL, BASE64, ROT13, Website, Keamanan*

1. PENDAHULUAN

Perkembangan teknologi di era ini sangatlah cepat hal ini tidak luput dari pendistribusian informasi yang juga ikut berkembang, internet merupakan salah satu media dari penyebaran informasi yang sangat luas begitu cepat. Internet akhirnya menjadi candu dalam masyarakat, dengan berkembangnya internet segala bidang aktivitas sudah mulai menggunakan internet mulai dari komunikasi atau pencarian informasi.

Website merupakan bagian dari internet yang terdiri dari satu atau lebih halaman dimana terdapat sejumlah informasi, yang disediakan perorangan, lembaga, ataupun sebuah organisasi dengan tujuan tertentu yang dapat diakses semua orang atau pun hanya orang memiliki akses (terbatas).

Perkembangan *website* di Indonesia sekarang ini sangat pesat, hal ini terjadi karena semakin bertambahnya jumlah pengguna layanan internet dari tahun ke tahun. Beberapa *website* yang sering diakses oleh pengguna diantaranya search engine, *e-commerce*, social networking, forum, portal berita dan lain – lain. Akan tetapi dibalik kemudahan layanan yang disediakan oleh setiap *website* tersebut ternyata terdapat beberapa masalah pada celah keamanan diantaranya : *cross-site scripting*, *information leakage*, *authentication and authorization*, *Session management*, *SQL Injection*, CSRF dan lain–lain. Dengan memanfaatkan celah kemanan ini seseorang dapat melakukan *hacking* pada *website* tersebut. (Gultom & Harahap, 2015)

Dalam penilitian yang berjudul "Penerapan Kriptografi Base64 Untuk Keamanan URL (*Uniform Resource Locator*) *Website* Dari Serangan SQL Injection" pada penelitian ini membahas bagaimana cara menanggulangi serangan *SQL Injection* dengan mengenkripsi URL nya menggunakan metode kriptografi Base64, kemudian setelah diterapkan metode kriptografi BASE64 informasi *server* dan basis data bisa ditemukan oleh serangan *SQL Injection*. (Nugraha & Erwin, 2016)

Penelitian selanjutnya dengan judul "Implementasi *Aeschipper Class* Untuk Enkripsi URL di Sistem Informasi Akademik Fakultas Teknik Universitas Diponegoro" juga membahas tentang bagaimana cara menanggulangi kelemahan pada pengiriman data menggunakan metode *GET* pada SIA (Sistem Informasi Akademik) Fakultas Teknik Universitas Diponegoro, penerapan metode *Aeschipper Class* untuk mengenkrisi URL menghasilkan *chipertext* dan tidak menampilkan variabel yang sebenarnya. (Subari & Manan, 2014)

Pada dasarnya sistem yang benar-benar aman itu tidak ada, sebuah sistem selalu memiliki celah apakah itu sebuah celah yang besar atau celah yang kecil, setiap sistem pasti memiliki celah jadi tidak ada jenis apapun metode yang dapat membuat sebuah sistem benar-benar aman , bahkan setingkat sistem bank pun masih sering terdengar berita bahwa telah diretas, jika dianalogika kan bila sebuah

sistem itu adalah rumah maka metode untuk melindungi sistem tersebut adalah pintu, sebuah rumah yang bisa dimasuki pasti memiliki pintu, dan hanya pemilik rumah yang memiliki kunci dan tahu tepatnya dimana pintu tersebut berada sehingga hanya pemilik rumah yang dapat masuk kedalam rumah tersebut, kemudian seberapa aman pun rumah tersebut pasti memiliki celah untuk dimasuki pencuri, tergantung seberapa tinggi skill pencuri tersebut karena jika rumah tersebut bisa dimasuki pemilik rumah, pasti ada jalan lain agar orang lain juga bisa masuk, jika jalan tersebut tidak ada maka tinggal membuat sendiri jalan tersebut.

Oleh sebab itu berdasarkan permasalahan keamanan diatas dan juga beberapa referensi diatas membuat saya ingin menerapkan suatu pengamanan berlapis dengan mengenkripsi URL pada *website* menggunakan beberapa algoritma enkripsi yang dirangkap diantaranya BASE64 dan ROT13 sebagai tindakan pencegahan terhadap serangan-serangan yang menyerang sistem tersebut, memang sistem yang benar aman itu tidak ada tetapi dengan memberikan pengamanan berlapis dapat mencegah dan menghambat serangan-serangan tersebut.

2. TINJAUAN PUSTAKA

2.1 Penelitan Terkait

Penelitian terkait kedua ada pada Jurnal Algoritma dengan judul "Penerapan Kriptografi Base64 Untuk Keamanan URL (*Uniform Resource Locator*) *Website* Dari Serangan *SQL Injection*" yang diteliti oleh Aziz Pratama Nugraha dan Erwin Gunadhi dari Sekolah Tinggi Teknologi Garut pada tahun 2016 yang membahas tentang bagaimana enkripsi pada URL menggunakan metode BASE64 dapat mencegah dan mengantisipasi serangan *SQL Injection*, Berdasarkan pengujian yang telah dilakukan terhadap URL setelah diterapkan kriptografi BASE64 informasi *server* dan basis data tidak dapat ditemukan. **(Nugraha & Erwin, 2016)**

Penelitian terkait pertama ada pada Artikel Skripsi yang berjudul "Implementasi Algoritma ROT13 Dan ElGamal Untuk Enkripsi dan Dekripsi Pesan Rahasia" yang diteliti oleh M. Zainudin Zuhri dari Universitas Nusantara PGRI Kediri pada tahun 2018 yang membahas tentang bagaimana cara mengamankan data yang berupa teks dengan mengkombinasikan metode ROT13 dan ElGamal agar tidak bisa dibaca secara langsung oleh orang lain pada aplikasi berbasis android, pengujian dilakukan kepada 10 Mahasiswa UKM PSHT Universitas Nusantara PGRI Kediri. Hasil perhitungan angket dari 10 mahasiswa menyatakan bahwa 83,75% Sangat Layak. **(Zuhri, 2018)**

2.2 Landasan Teori

2.2.1 Website

Website adalah sebuah sistem dengan informasi yang disajikan dalam bentuk teks, gambar, suara dan lain-lain yang tersimpan dalam sebuah server *Website* Internet yang disajikan dalam bentuk *hypertext*. Informasi *Website* dalam bentuk teks umumnya ditulis dalam format HTML (*Hypertext Markup Language*).

2.2.2 URL

URL (Uniform Resource Locator) menunjukan alamat dari sebuah homepage atau menunjukan sumber daya Internet, yaitu alamat suatu dokumen atau program yang ingin ditampilkan atau digunakan. Bagian pertama URL menunjukan *protocol*, misalnya http:// atau https://. *Protocol* merupakan persetujuan bersama yang digunakan untuk melakukan komunikasi, dalam hal ini menggunakan *HTTP* (*Hypertext Transfer Protocol*). Bagian kedua dari URL menunjukan alamat server tempat disimpannya sumber daya tersebut, misalnya *www.microsoft.com* untuk *website Microsoft Corporation*. Selanjutnya untuk bagian ketiga dari URL adalah path file, merupakan bagian dari URL yang menunjukan lokasi dan nama dokumen atau program dalam server tersebut.

2.2.3 PHP

PHP adalah sebuah bahasa pemograman yangberjalan dalam sebuah *web-server* (*serverside*). PHP diciptakan oleh programmer unix dan Perl yang bernama Rasmus Lerdoft pada bulan Agustus September 1994. *Script* PHP adalah bahasa program yang berjalan pada sebuah *webserver*, atau sering disebut

serverside. Oleh karena itu, PHP dapat melakukan apa saja yang bisa dilakukan program CGI lain, yaitu mengolah data dengan tipe apapun, menciptakan halaman web yang dinamis, serta menerima dan menciptakan *cookies*, dan bahkan PHP bisa melakukan lebih dari itu.

2.2.4 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 kerahasiaan, keutuhan data dan otentikasi entitas.

2.2.5 Enkripsi

Enkripsi (*encryption*) adalah Proses yang dilakukan untuk mengamankan sebuah pesan (yang disebut *plaintext*) menjadi pesan yang tersembunyi (disebut *ciphertext*). Enkripsi digunakan untuk menyandikan data-data atau informasi sehingga tidak dapat dibaca oleh orang yang tidak berhak. Dengan enkripsi data anda disandikan (*encrypted*) dengan menggunakan sebuah kunci (*key*). Untuk membuka (*decrypt*) data tersebut digunakan juga sebuah kunci yang dapat sama dengan kunci untuk mengenkripsi (untuk kasus *private key cryptography*) atau dengan kunci yang berbeda (untuk kasus *public key cryptography*).

2.2.6 BASE4

Transformasi BASE64 merupakan salah satu algoritma untuk encoding dan decoding suatu data ke dalam format ASCII, yang didasarkan pada bilangan dasar 64 atau bisa dikatakan sebagai salah satu metoda yang digunakan untuk melakukan encoding (penyandian) terhadap data binary. Karakter yang dihasilkan pada transformasi BASE64 ini terdiri dari A..Z, a..z dan 0..9, serta ditambah simbol "+" dan "/" serta satu buah karakter sama dengan (=) di dua karakter terakhir yang dipakai untuk pengisian pad atau dengan kata lain penyesuaian dan menggenapkan data binary. Karakter simbol yang akan dihasilkan akan tergantung dari proses algoritma yang berjalan. Kriptografi transformasi BASE64 banyak digunakan di dunia Internet sebagai media data format untuk mengirimkan data, penggunaan tersebut dikarenakan hasil dari encode BASE64 berupa plaintext, maka data ini akan jauh lebih mudah dikirim, dibandingkan dengan format data yang berupa binary. Algoritma BASE64 menggunakan kode ASCII dan kode index BASE64 dalam melakukan proses enkripsi ataupun dekripsinya. Dalam melakukan enkripsi pada URL *website*, kode index BASE64 perlu dimodifikasi.

2.2.7 ROT13

Rotation 13 (ROT13) ROT13 (*Rotate 13*) adalah enkripsi substitution cipher yang umum digunakan di sistem operasi UNIX. Pada sistem enkripsi ROT13 sebuah huruf digantikan dengan huruf yang letaknya di atas 13 posisi darinya. (Frisai & Mesran, 2017)

Caesar Cipher ROT13 adalah fungsi yang menggunakan kode Kaisar dengan pergeseran k=13. ROT13 didesain untuk keamanan pada sistem operasi UNIX yang sering digunakan pada forum online, berfungsi untuk menyelubungi isi artikel sehingga hanya orang yang berhak yang dapat membacanya. Sistem enkripsi ROT13 kali ini dengan menggeser maju karakter sebanyak 13 kali, terhitung 1 adalah karakter didepannya, dan pergeseran karakter berdasarkan urutan karakter pada tabel ASCII. Sebagai dekripsinya, dengan menggeser mundur karakter sebanyak 13 kali. (Zuhri, 2018)

3. METODOLOGI PENELITIAN

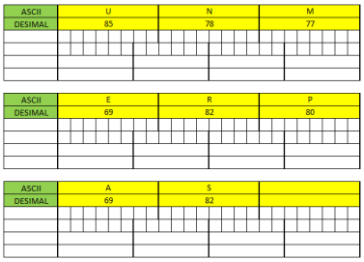
3.1 Analisa Metode

Plaintext pada awalnya akan di enkripsi menggunakan algoritma BASE64 terlebih dahulu ketika sudah didapatkan *chipertext* nya kemudian *chipertext* hasil enkripsi tersebut akan dianggap sebagai *plaintext* yang kemudian di enkripsi lagi menggunakan menggunakan algoritma ROT13. Berikut tahapan-tahapan dalam menyandikan sebuah *plaintext* menggunakan algoritma-algoritma tersebut :

P- ISSN : 2085 – 3092
E- ISSN : 2721 – 057X

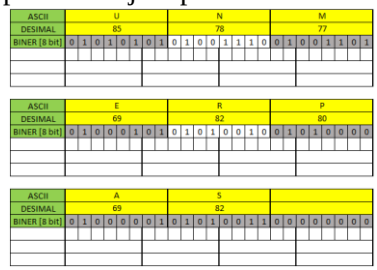
Plaintext =**UNMERPAS**
Tahapan Enkripsi :

- Ubah plaintext tersebut menjadi *binary*
  Binary =
  U=01010101
  N=01001110
  M=01001101
  E=01000101
  R=01010010
  P=01010000
  A=01000001
  S=01010011
- Kemudian hasil *binary* nya akan dipecah per 24 bit (per 3 huruf)



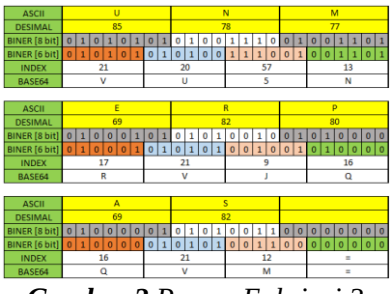
***Gambar 1** Proses Enkripsi 1*

- Setelah itu dari 24 bit biner tersbebut dipecah menjadi per 6 bit.



***Gambar 2** Proses Enkripsi 2*

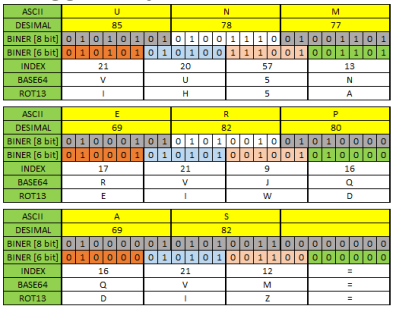
- Selanjutnya hitung bit biner tersebut untuk menentukan index dari BASE64.



***Gambar 3** Proses Enkripsi 3*

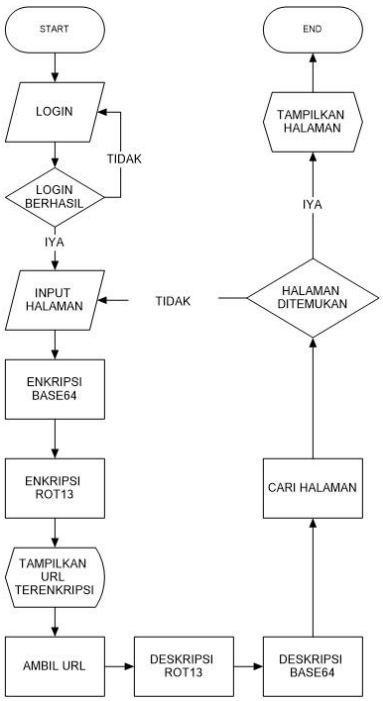
Jadi Hasil Enkripsi BASE64 dari **UNMERPAS** adalah **VU5NRVJQQVM=**

- Kemudian **VU5NRVJQQVM=** di Enkripsi Menggunakan ROT13 sehingga menjadi **IH5AEIWDDIZ=**



***Gambar 4** Proses Enkripsi 4*

3.2 Perancangan Flowchart



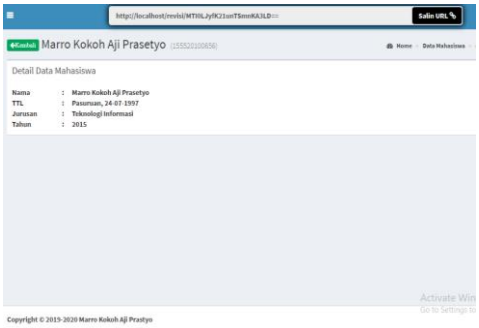
***Gambar 5** Flowchart Sistem*

4. HASIL DAN PEMBAHASAN

Setelah di enkripsi url jadi lebih sulit dibaca dan terkesan acak berikut adalah beberapa gambar hasil enkripsi :

a. <u>Halaman Detail Mahasiswa</u>

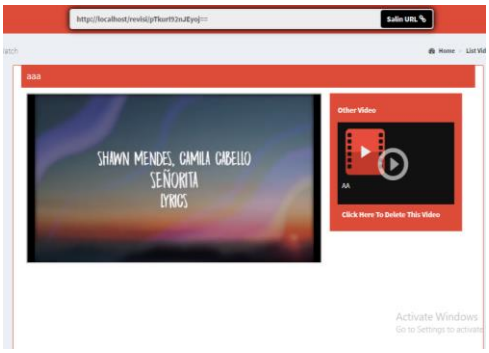
Halaman ini berisi informasi profile seorang mahasiswa dengan alamat URL yang sudah terenkrispisi.



Gambar 6 *Halaman Detail Mahasiswa*

b. Halaman Streaming Video

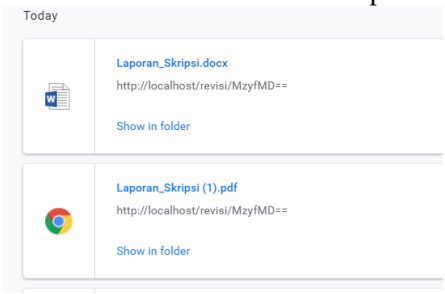
Halaman ini terdapat video yang bisa diputar langsung dengan alamat URL sudah Terenkripsi



Gambar 7 *Halaman Streaming Video*

c. URL Sumber Pada File Yang Terdownload

Alamat sumber *download* terenkripsi



Gambar 4.10 *Hasil Download*

5. KESIMPULAN

Dari hasil penelitian yang dilakukan peneliti dapat mengambil kesimpulan sebagai berikut:

1. Metode BASE64 dan ROT13 dapat dikombinasikan untuk mengenkripsi alamat URL pada sebuah *website*.
2. Dengan mengenkripsi sebuah URL sebuah *website*, *website* tersebut menjadi lebih aman dikarenakan celah pada URL telah ditutup menggunakan enkripsi BASE64 dan ROT13.

Berdasarkan hasil implementasi dari metode BASE64 dan ROT13 untuk mengenkripsi alamat URL pada *website* terdapat beberapa saran yang perlu diperhatikan dalam pengembangan penelitian ini diantara lain:

1. Menambahkan metode untuk mengenkripsi alamat URL tersebut agar bukan hanya celah tersebut sekedar tertutup tapi juga memiliki tingkat keamanan yang sangat tinggi.
2. Sistem ini dapat dikembangkan menjadi sebuah aplikasi *desktop browser* yang untuk *browsing* dengan alamat URL nya sudah terdaftar pada aplikasi tersebut , sehingga user hanya bisa memilih dari alamat yang sudah terdaftar mungkin aplikas tersebut akan cocok digunakan pada dunia pendidikan sehingga siswa lebih terfokus dan tidak membuka URL di luar list.

DAFTAR PUSTAKA

Azlin, & Musadat, F. (2018). APLIKASI KRIPTOGRAFI KEAMANAN DATA MENGGUNAKAN ALGORITMA BASE64. *Jurnal Informatika*.

Donny Seftyanto, M. T. (2012). PERAN ALGORITMA CAESAR CIPHER DALAM MEMBANGUN KARAKTER AKAN KESADARAN KEAMANAN INFORMASI. *Seminar Nasional Matematika dan Pendidikan Matematika FMIPA UNY*, (pp. 883-890). Yogyakarta.

Frisai, A. S., & Mesran. (2017). Implementasi algoritma rot13 dan algoritma caesar chiper dalam penyandian teks. *Pelita Informatika Budi Darma*, 38-41.

Gultom, L. M., & Harahap, M. (2015). Analisis Celah Keamanan Website Instansi. *Jurnal Teknovasi*, 1-7.

Hidayatullah, A., & Insanudin, E. (2016). PENGENALAN KRIPTOGRAFI DAN PEMAKAIANYA SEHARI-HARI. *Jurnal Pengenalan Kriptografi Dan Pemakaianya Sehari-Hari*.

Kodir, A. (2014). *Pengenalan Sistem Informasi edisi Revisi.* Yogyakarta: Andi Offset.

Kromodimoeljo, S. (2009). *Teori & Aplikasi Kriptografi.* SPK IT Consulting.

Mulyana, D. I. (2016). KAJIAN PENERAPAN ENCODE DATA DENGAN BASE64 PADA PEMROGRAMAN PHP. *Jurnal CKI On SPOT*, 47-52.

Nugraha, A. P., & Erwin, G. (2016). Penerapan Kriptografi Base64 Untuk Keamanan URL (Uniform Resource Locator) Website Dari Serangan SQL Injection. *Jurnal Algoritma Sekolah Tinggi Teknologi Garut, 13*, 491-498.

Primartha, R. (2011). Penerapan Enkripsi dan Dekripsi File Menggunakan Data Encryption Standard (DES). *Jurnal Sistem Informasi*, 371-387.

Raharjo, B. (1999). *Keamanan Informasi Berbasis Internet.* Bandung: PT Insan Komunikasi.

Solichin, A. (2005). *Pemrograman Web dengan PHP dan MySQL.* Jakarta: Universitas Budi Luhur.

Subari, A., & Manan, S. (2014). Implementasi Aeschipper Class Untuk Enkripsi URL di Sistem Informasi Akademik Fakultas Teknik Universitas Diponegoro. *Jurnal Sistem Komputer*.

Sumartono, I., Siahaan, A. P., & Arpan. (2016). Base64 Character Encoding and Decoding Modeling. *International Journal of Recent Trends in Engineering & Research (IJRTER)*, 63-68.

Zuhri, M. Z. (2018). IMPLEMENTASI ALGORITMA ROT13 DAN ELGAMAL UNTUK ENKRIPSI DAN DEKRIPSI PESAN RAHASIA. *Artikel Skripsi*, 1-10.