

# IMPLEMENTASI KRIPTOGRAFI PADA WEB SERVICE DENGAN METODE CAESAR CIPHER BERBASIS JAVA DI PT. INTEGRASI MEDIA KREASI

**Bima Galih Ritwiyani<sup>1)</sup>, Rizky Pradana<sup>2)</sup>**

Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur  
Jl. Raya Ciledug, Petukangan Utara, Kebayoran Lama, Jakarta Selatan 12260  
E-mail : bimagalihritwiyani@gmail.com, rizky.pradana@budiluhur.ac.id

## Abstrak

*PT. Integrasi Media Kreasi saat ini mempunyai web service di aplikasi asset management, dimana aplikasi tersebut terdistribusi secara umum tanpa ada pengamanan khusus yang dapat mengakibatkan kebocoran data atau manipulasi data oleh orang yang tidak bertanggung jawab. Sehingga perlu dibuat suatu keamanan dengan menggunakan teknik kriptografi salah satunya adalah algoritme Caesar Cipher. Algoritme ini sebagai pergeseran cipher yang merupakan salah satu teknik enkripsi yang paling sederhana dan dasar yang mempunyai kemampuan menggantikan angka di mana setiap huruf dalam plaintext diganti dengan huruf dengan posisi tetap dipisahkan oleh nilai numerik yang digunakan sebagai "kunci". Aplikasi dibangun menggunakan bahasa pemrograman Java. Dengan menambahkan algoritme Caesar Cipher pada web service maka mampu meningkatkan keamanan data terdistribusi pada PT. Integrasi Media Kreasi.*

**Kata kunci:** Kriptografi, Algoritme, Enkripsi, Dekripsi, Web Service

## 1. PENDAHULUAN

Pemanfaatan teknologi saat ini, memberikan pengaruh besar baik dalam lingkup individu maupun organisasi. Teknologi selalu dikembangkan dengan tujuan untuk memenuhi setiap kebutuhan bagi para penggunanya. Dalam lingkungan bisnis, proses bisnis saat ini lebih cenderung bersifat dinamis, didistribusikan dan kolaboratif, sehingga perlu untuk beradaptasi dengan proses bisnis yang lain dengan lebih sering, dan integrasi proses melalui batas organisasi. Pada proses integrasi, dibutuhkan adanya *web service* untuk saling komunikasi antar platform lain dengan mempublikasikan secara umum data informasi pada sistem data terdistribusi.

Pada sebuah data informasi yang di distribusi harus dapat dijaga kerahasiaan data untuk mengurangi resiko tingkat kecurangan. Secara khusus, pada PT. Integrasi Media Kreasi kecurangan tersebut dapat dilakukan oleh internal karyawan salah satu tujuannya untuk mengambil data dan membuat manipulasi tampilan data lalu menjebak korban untuk login, bertujuan untuk mengambil data informasi kredensial seperti email dan password selanjutnya login dan mengubah data yang ada.

Dari segi tinjauan masalah secara umum, kecurangan dapat terjadi bertujuan untuk mengintegrasikan atau mengkolaborasi sebuah data pada aplikasi yang sudah mereka miliki, hal ini dapat menimbulkan masalah legalitas data perusahaan karena mereka belum memiliki izin untuk berkolaborasi oleh platform atau aplikasi mereka.

Solusi dari masalah-masalah yang akan muncul dapat dicegah dengan dibutuhkannya suatu metode yang dapat menjaga kerahasiaan data terdistribusi untuk meminimalisir tingkat kecurangan oleh pihak-pihak yang tidak bertanggung jawab dan juga oleh pihak internal dari perusahaan.

Pada pembuatan metode ini, untuk memecahkan masalah ini tertarik untuk membangun sebuah sistem keamanan algoritme kriptografi Caesar Cipher untuk keamanan pada sistem data terdistribusi yang di implementasikan pada aplikasi *asset management* di PT. Integrasi Media Kreasi.

Secara garis besar ada dua jenis kriptografi, yaitu kriptografi klasik dan kriptografi modern. Kriptografi klasik adalah kriptografi yang berbasis karakter (enkripsi dan dekripsi dilakukan pada setiap karakter). Sedangkan kriptografi modern adalah kriptografi yang beroperasi dalam mode bit (dinyatakan dalam 0 dan 1). Pada penelitian ini akan dibangun sistem keamanan dengan menggunakan kriptografi klasik dengan algoritme Caesar Cipher yang diimplementasikan pada *web service*, dimana Caesar Cipher merupakan salah satu enkripsi paling sederhana dengan menggantikan angka di mana setiap huruf dalam plaintext diganti dengan huruf dengan posisi tetap dipisahkan oleh nilai numerik yang digunakan sebagai "kunci". (Khairani dan Wahyudi 2015).

Berdasarkan latar belakang yang telah disampaikan, rumusan masalah yang dihadapi dalam perancangan sistem yaitu:

- Bagaimana menemukan celah untuk manipulasi data pada aplikasi *asset management*?
- Bagaimana cara dekripsi data *asset management* yang sudah dilakukan enkripsi tanpa mengalami perubahan isi data sedikitpun?
- Bagaimana pengembang lain melakukan integrasi data terdistribusi tanpa izin terlebih dahulu kepada pemilik? Kecuali untuk abstrak, awal paragraf isi tulisan ditulis menjorok ke dalam (*first line indent*) sejauh 7,5 mm. Tata cara penulisan telah disusun pada tulisan ini.

Maksud penulisan untuk laporan tugas akhir ini adalah mengimplementasikan enkripsi pada *web service* dengan algoritme kriptografi Caesar Cipher, lalu data tersebut akan didekripsikan oleh client side dengan algoritme kriptografi Caesar Cipher

Tujuan laporan penelitian ini adalah untuk mengamankan data yang telah di distribusi oleh *web service* agar terhindar dari pengembangan ilegal yang memanfaatkan data dan mencuri data.

Dalam penelitian ini metode pengembangan yang digunakan adalah:

- Observasi**  
Melakukan kunjungan ke tempat riset dan melakukan wawancara langsung kepada Manajer IT, Ibu Tabita Dewi di PT. Integrasi Media Kreasi.
- Studi Literatur**  
Melalui studi laporan tugas akhir ini memperoleh informasi dengan mengumpulkan data, mempelajari dan membaca berbagai referensi baik itu dari buku-buku, jurnal, makalah, maupun internet dan berbagai sumber lainnya yang menunjang dalam penulisan ini.
- Analisis Data**  
Menganalisa algoritme kriptografi Caesar Cipher pada *web service* dengan enkripsi menggunakan Java dan dekripsi menggunakan Javascript.
- Perancangan Sistem**  
Merancang sistem program untuk mengimplementasikan algoritme Caesar Cipher pada *web service* dengan menggunakan bahasa pemrograman Java dan Javascript.
- Pengujian Sistem**  
Melakukan pengujian terhadap aplikasi *asset management* pada bagian *web service* yang telah dirancang serta menyimpulkan hasil dari pengujian.
- Penarikan Kesimpulan**  
Menyimpulkan hasil selama menjalani riset dan mengimplementasikan kriptografi pada *web service* di aplikasi *asset management* pada PT. Integrasi Media Kreasi.

## 2. ANALISA MASALAH

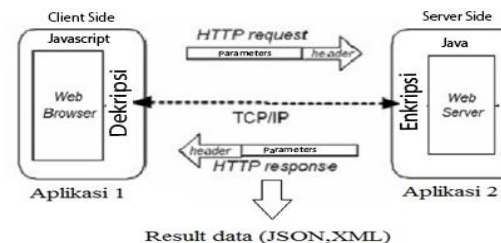
Perkembangan teknologi informasi yang semakin pesat, mempermudah siapapun untuk mengembangkan aplikasi dengan mudah dan cepat. Pengembangan suatu aplikasi dengan sistem data terdistribusi (*Web Service*) perlu diperhatikan karena kemudahannya untuk integrasi dengan platform lain, sehingga dapat menimbulkan ancaman oleh pihak-pihak yang memanfaatkan untuk berbuat kecurangan manipulasi data dan tidak bertanggung jawab. Oleh karena itu pengamanan data terdistribusi juga diperlukan untuk menjaga kerahasiaan suatu data dari tindakan kecurangan.

Dari analisis masalah, perlu adanya sebuah enkripsi pada *web service* untuk mengamankan data dengan sistem terdistribusi untuk menjaga

kerahasiaan sehingga dapat meminimalisir kecurangan dan manipulasi data.

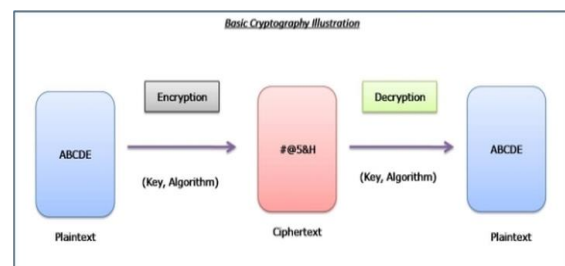
Untuk dapat memahami konsep aplikasi yang akan dibangun, dapat melihat gambar arsitektur sistem pada Gambar 1, dan Gambar 2. Pada gambar tersebut, menggambarkan secara garis besar proses dari keseluruhan sistem *web service* yang di enkripsi dan dekripsi.

### a. Web Service



Gambar 1. Arsitektur Web Service

### b. Enkripsi



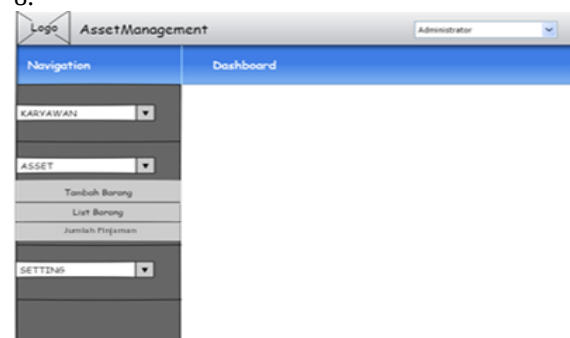
Gambar 2. Arsitektur Enkripsi

## 3. Rancangan Layar dan Peran User

Dalam membuat suatu sistem aplikasi, rancangan layar merupakan suatu hal yang sangat penting. Rancangan layar harus mudah dipahami, agar pengguna atau user yang belum tahu merasa nyaman dalam menggunakan aplikasi *asset management* ini.

### a. Rancangan Menu Asset

Berikut ini rancangan layar untuk menu Asset gambar 3, pada menu Asset ini terdapat form tambah Asset, form view Asset, form List Asset, dan form edit Asset. yang berfungsi untuk menambahkan input barang, melihat data barang yang dipinjamkan pada karyawan, untuk mengubah data barang, dan rancangan layar bisa dilihat pada gambar 4, 5, 6, 7 dan 8.



Gambar 3 Rancangan Layar Menu Asset

Gambar 4. Rancangan Layar Form Tambah Asset

Gambar 8. Rancangan Layar Form Edit Asset

Gambar 5. Rancangan Layar Form View Asset

Gambar 6. Rancangan Layar List Pinjam Barang

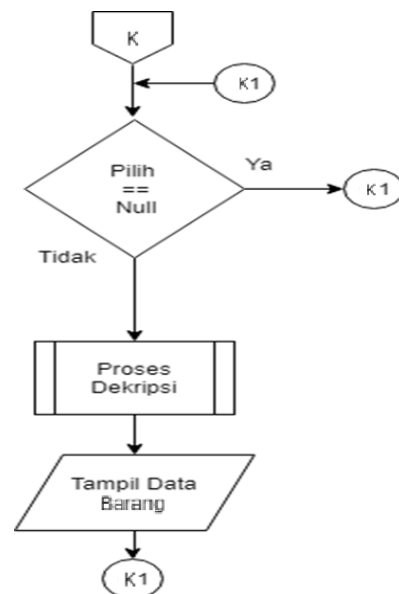
Gambar 7. Rancangan Layar Form List Asset

## b. Flowchart

Berikut ini adalah flowchart yang digunakan untuk menelusuri proses program pada aplikasi *asset management*.

### 1) Flowchart Form Detail Asset Barang

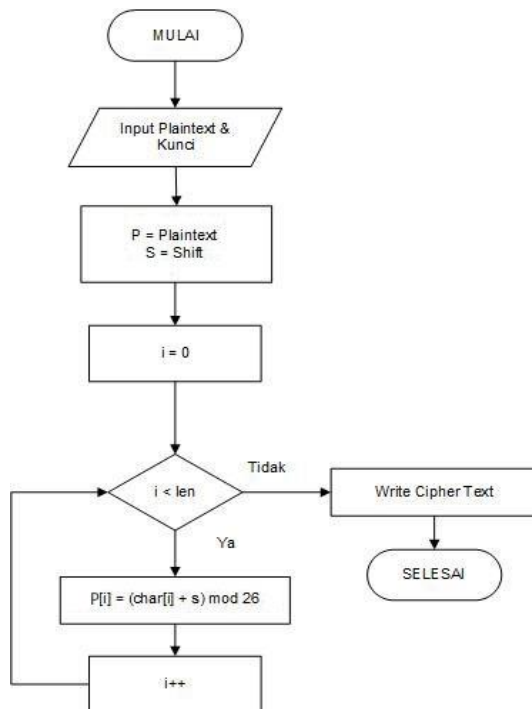
Flowchart tampil form *Detail Asset* barang seperti yang tertera pada Gambar 9 di bawah ini adalah alur atau jalannya proses untuk melihat barang yang dipakai oleh karyawan.



Gambar 9. Flowchart Form Detail Asset Barang

### 2) Flowchart Proses Enkripsi

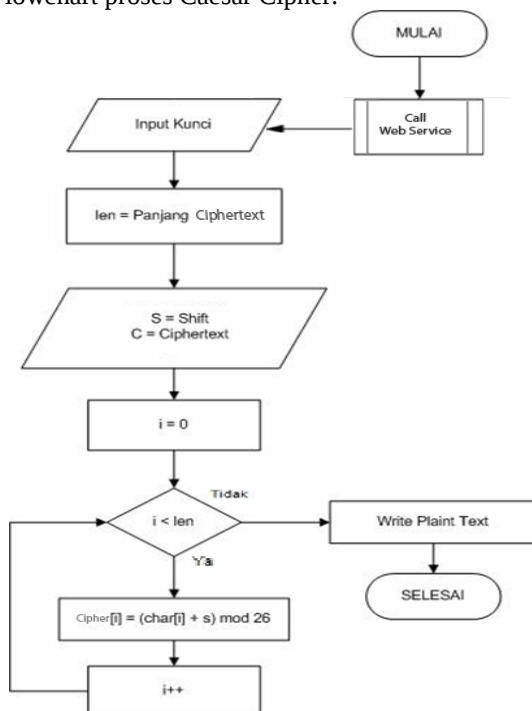
Pada Flowchart proses enkripsi Caesar Cipher ini, akan dijelaskan bagaimana proses perubahan plaintext ke ciphertext. Berikut gambar 10 adalah Flowchart proses Caesar Cipher



Gambar 10. Flowchart Menu Proses Enkripsi

### 3) Flowchart Proses Dekripsi

Pada Flowchart proses dekripsi Caesar Cipher ini, akan dijelaskan bagaimana proses perubahan chipertext ke plaintext. Berikut gambar 11 adalah Flowchart proses Caesar Cipher.



Gambar 11. Flowchart Menu Proses Dekripsi

### c. Desain Sistem

#### 1) Algoritme Alur Proses

Algoritme digunakan untuk mempermudah dalam pembuatan perancangan web service, enkripsi dan dekripsi. Algoritme yang telah dibuat adalah terjemahan dari flowchart, dimana algoritme ini akan

menjabarkan cara kerja web service, enkripsi dan dekripsi. Berikut ini akan dijelaskan algoritme proses, yang dikelompokkan dalam beberapa proses dan fungsi masing-masing.

#### Algoritme 1. Writer Hashmap Web Service

```

Masukan plaintext
H = Hashmap
P = Plaintext
G = Gson
Writer(G.json(H(P, P)))
  
```

### 2) Algoritme Proses Enkripsi

Algoritme proses enkripsi ini menjelaskan bagaimana proses algoritme Caesar Cipher melakukan proses enkripsi hingga berhasil mendapatkan data ciphertext. Pada proses ini akan menjelaskan plaintext menjadi chipertext yang nantinya akan diproses dengan algoritme Caesar Cipher.

#### Algoritme 2. Proses Enkripsi

```

Masukan plaintext
len = Panjang plaintext
P = Plaintext; CP = Ciphertext
© = 0; j = 0; c = char Plaintext to array; key = 10;
For (© < c.len; i++)
  For(j < CP.len; j++)
    If (j <= CP.len - key)
      If (c[i] == CP[j])
        c[i] = CP[j + key]
        Break;
      Else If (c[i] == CP[j])
        c[i] = CP[j - (CP.len - key + 1)]
    End If
  End For
End For
Write ©
  
```

### 3) Algoritme Proses Dekripsi

Algoritme proses dekripsi ini menjelaskan bagaimana proses dekripsi algoritme Caesar Cipher melakukan proses dekripsi hingga berhasil mendapatkan data yang asli atau plaintext.

#### Algoritme 3.3. Proses Dekripsi

```

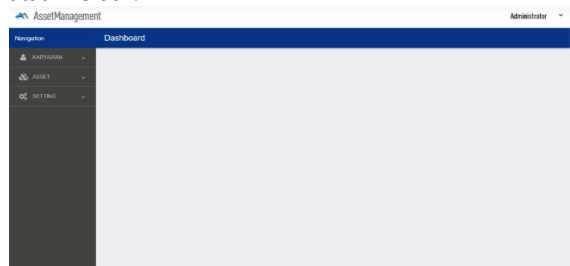
Masukan plaintext
len = Panjang plaintext
P = Plaintext; CP = Ciphertext
i = 0; j = 0; c = char Plaintext to array CP; key = 10;
For (i < c.len; i++)
  For(j < CP.len; j++)
    If (j >= key && c[i] == CP[j])
      c[i] = CP[j - key]
      Break;
    If (c[i] == CP[j] && j < key)
      c[i] = CP[(CP.len - key + 1) + j]
      Break
    End If
  End For
End For
Write (c)
  
```

### d. IMPLEMENTASI DAN ANALISIS HASIL UJI COBA PROGRAM

#### 1) Tampilan Layar Menu Dashboard Asset Management

Tampilan layar dari menu utama pada Gambar 12. muncul setelah melalui proses login dengan

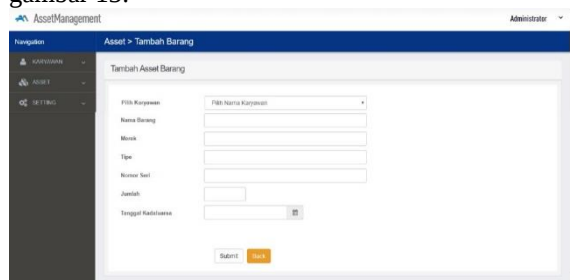
Administrator. Didalam menu utama terdapat menu-menu yang dapat dipilih oleh user. Diantaranya adalah Karyawan => Tambah Karyawan, Karyawan => List Karyawan, Asset => Tambah Barang, Asset => List Barang, Setting => User Login, dan LogOut atau Keluar.



Gambar 12. Tampilan Layar Menu Dashboard

#### 4) Tampilan Layar Tambah Barang

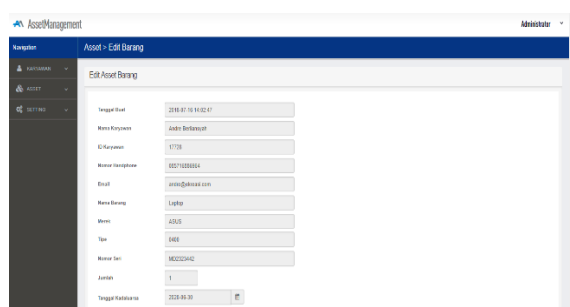
Form ini untuk menambahkan aset barang dengan cara klik menu Asset yang ada pada baris menu layar utama lalu pilih tambah barang lalu memilih daftar nama karyawan yang akan dipinjamkan barang oleh perusahaan dan mengisi data yang ada pada form tambah barang. Lihat gambar 13.



Gambar 13. Tampilan Tambah Barang

#### 5) Tampilan Layar View Barang

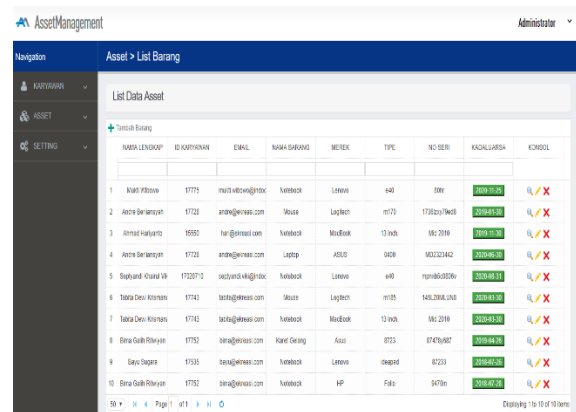
Form ini untuk menampilkan detail data lengkap barang pada bagian aset barang dimana user dapat melihat rincian aset barang yang dipinjamkan kepada karyawan. Lihat Gambar 14.



Gambar 14. Tampilan View Barang

#### 6) Tampilan Layar List Barang

Pada tampilan menu ini akan menampilkan data aset barang yang telah dipinjamkan kepada karyawan. Lihat gambar 15.



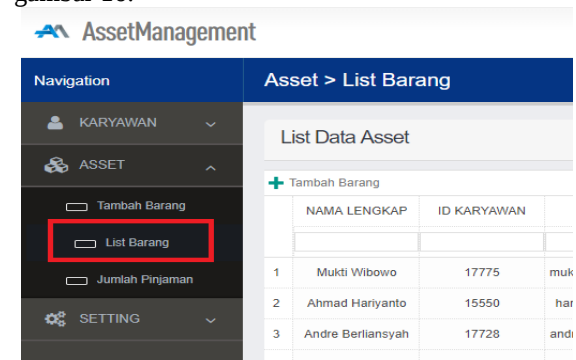
Gambar 15. Tampilan Layar List Barang

#### e. PROSES PENGUJIAN

Setelah semua kebutuhan terpenuhi baik software maupun hardware, maka tahapan selanjutnya adalah melakukan uji coba terhadap aplikasi. Pada tahap ini akan diuraikan mengenai pengujian enkripsi dan dekripsi pada web service.

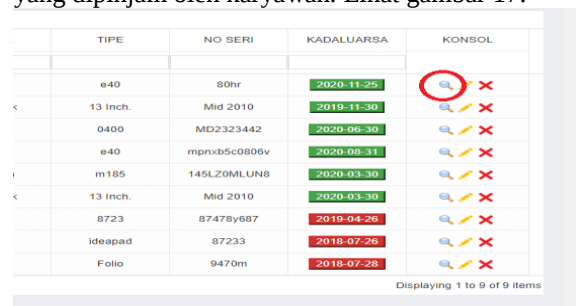
#### f. Proses Enkripsi

Untuk melakukan proses enkripsi dan dekripsi maka akan mencoba salah satu menampilkan data detail list barang yang dipinjam oleh karyawan. Pilih menu ASSET, selanjutnya pilih List Barang. Lihat gambar 16.



Gambar 16. Tampilan Menu List Barang

Jika sudah tampil list table barang, selanjutnya pilih icon kaca pembesar untuk melihat detail barang yang dipinjam oleh karyawan. Lihat gambar 17.



Gambar 17. Tampilan Icon Kaca Pembesar Pada List Table Barang

Gambar 18. Tampilan *Detail* Barang.

Pada gambar 18 tersebut kita bisa lihat bahwa form text yang di disabled tersebut menampilkan data dari server yang di distribusikan oleh web service yang sebenarnya masih berupa data hasil enkripsi, lalu diterima oleh *client side* (Browser) dan didekripsi oleh Javascript. Hasil dari dekripsi tersebut selanjutnya ditampilkan pada form input. Jika kita buka browser dan panggil url pada browser `http://localhost:8080/AssetManagement_API/WebService?doing=view-data-asset&id=19` maka hasil datanya masih ter-enkripsi. Lihat gambar 19.

Gambar 19. Data Enkripsi Pada *Web Service*

Untuk uji coba proses enkripsi itu sendiri maka kita akan mencoba tambah *user login* baru. Buka menu **SETTING** klik *User Login* dan pilih Tambah *User Login*. Lihat gambar 20.

Gambar 20. Tampilan Uji Coba Enkripsi di Form Penambahan *User Login*

## 7) Proses Dekripsi

Untuk melakukan uji coba proses dekripsi maka bisa langsung akses menu , **SETTING** lalu pilih *User Login* dan pilih salah satu icon kaca pembesar yang berada di *list* tabel. Lihat gambar 21.

Gambar 22 . Tampilan Salah Satu Informasi *User Login*

Bisa dilihat gambar 22 bahwa kita dapat mengetahui tulisan informasi yang ditampilkan, yang sebenarnya data tersebut telah di dekripsi oleh client browser. Proses dekripsi itu sendiri dilakukan oleh Bahasa pemrograman Javascript. Lihat gambar 23.

Gambar 23. Proses Dekripsi Pada Javascript

Dari hasil panggilan data dari *web service*, hasil response tulisan yang di berikan oleh web service masih berupa data enkripsi. Untuk proses dekripsi terletak pada nama *function decrypt*. Lihat gambar 24 untuk melihat detail dari isi *function decrypt*.

Gambar 25. Algoritme Dekripsi Caesar Cipher

Pada rumus algoritme gambar 25 memakai kriptografi Caesar Cipher. Data plain text yang berupa tulisan masih terenkripsi di proses dengan rumus yang sudah disediakan pada huru-huruf tertentu dan dimasukan ke array dengan nama variable *char*. Selanjutnya huruf yang masih terenkripsi dihitung jumlah array nya dan ditambahkan jumlah array dengan key offset. Lihat gambar 4.28, dan dicocokkan pada huruf-huruf yang ditentukan. Hasil dari proses pencocokan array dengan tulisan selanjutnya di keluarkan melalui variable *cipher* dengan join string kosong. Hasilnya tulisan yang ter enkripsi tadi akan bisa kita baca.

**8) Kelebihan Aplikasi**

- a. Hasil data yang didistribusi oleh web service akan lebih aman, karena data telah dienkripsi sehingga tidak dapat dibaca oleh pihak yang tidak bertanggung jawab.
- b. Tingkat keamanan data setelah di enkripsi dan di dekripsi tidak mengalami perubahan kata.
- c. Kinerja aplikasi tergolong cepat, karena data yang di enkripsi dan dekripsi hanya berupa string plain text.
- d. Pada saat proses pengembangan aplikasi di platform lain lebih singkat karena adanya sistem data terdistribusi (Web Service).

**9) Kekurangan Aplikasi**

- a. Proses enkripsi dan dekripsi berbeda bahasa pemrograman, sehingga pada saat koneksi antar client side dan server side terputus maka proses dekripsi atau enkripsi tidak akan berjalan.
- 2) Proses terdapat di client side browser dengan bahasa pemrograman Javascript sehingga jika didebug browser dan diteliti satu persatu akan terbaca algoritme dekripsi pada web service.
- 3) Aplikasi *asset management* hanya bisa berjalan pada server web Jboss 7.1.

**4. KESIMPULAN**

Kesimpulan yang didapat dari hasil analisa atas masalah dan pemecahannya adalah:

- a. Dengan adanya enkripsi, tampilan user interface aplikasi masih dapat dimanipulasi tetapi data terdistribusi tidak dapat terbaca, karena sudah ada nya enkripsi pada web service maka pencuri tidak dapat melihat isi data.
- b. Pada data web service terdapat data penting *asset* perusahaan, maka pencuri tidak dapat lagi melihat atau mencuri isi data tersebut untuk kepentingan pribadi, karena web service dengan data terdistribusi yang di enkripsi tidak dapat dibaca oleh pencuri.
- c. Dengan kriptografi Caesar Cipher, maka kunci yang dipakai satu arah (konvensional) lalu yang dienkripsi hanya plain text, hasilnya tidak ada perubahan data ukuran dan perubahan setelah di dekripsi.
- d. Pengembang lain bisa saja mengintegrasikan aplikasi mereka dengan web service *asset management* tanpa izin dari perusahaan PT. Integrasi Media Kreasi, akan tetapi data hasil dari web service tidak akan terbaca karena sudah terenkripsi.
- e. Web service pada aplikasi *asset management* telah berhasil 100% di enkripsi dan dekripsi dengan baik dan benar.

**5. DAFTAR PUSTAKA**

- [1] A. Rahmatulloh, H. Sulastri and R. Nugroho. (2016), "Keamanan RESTful Web Service Menggunakan JSON Web Token (JWT) HMAC SHA-512", *JNTETI*, vol 7, no. 2, 2018, pp.131-137.

- [2] A. Prapdipta, (2016). "Implementasi Metode Caesar Chip Alphabet Majemuk Dalam Kriptografi Untuk Pengamanan Informasi", *Indonesian Journal on Networking and Security*, vol 5, no. 3, pp. 16-19/
- [3] I., Gunawan, (2018), "Kombinasi Algoritma Caesar Cipher dan Algoritma RSA untuk Pengamanan File Dokumen dan Pesan Teks", *InfoTekJar(Jurnal Nasional Informatika dan Teknologi Jaringan)*, vol. 2, no. 2, pp. 124-129.
- [4] A., Rulloh, D., E., Mahmudah, and H., Kabetta, (2017), "Implementasi REST API Pada Aplikasi Panduan Kepaskibraan Berbasis Android", *Teknikom*, vol. 1, no. 2, pp. 85-89.
- [5] M., I., Perkasa and E., B., Setiawan, (2017), "Pembangunan Web Service Data Masyarakat Menggunakan REST API dengan Access Token", *ULTIMA Computing*, vol. x, no. 1, pp.19-26.
- [6] F. Winda Sari adm A. Triwinarko, (2015). "Pemanfaatan Kriptografi Pada RESTful Web Service", *Jurnal INTEGRASI*, vol. 7, no. 1, pp. 77-81.
- [7] P. F. Tanaem, D. Manongga, dan A. Iriani, (2016), "RESTful Web Service untuk Sistem Pencatatan Transaksi Studi Kasus PT. XYZ," *Jurnal Teknik Informatika dan Sistem Informasi*, vol. 2, pp. 1-10.
- [8] Siregar, I. M., & Purba, J., (2012), "Membongkar Teknologi Pemrograman Web Service", Yogyakarta: Gava Media.
- [9] Khairani and Wahyudi, (2015), "Analisis Kombinasi Metode Caesar Cipher, Vernam Cipher dan Hill Cipher Dalam Proses Kriptografi" *IEEE Electron Device Lett.*, vol. 30, pp. 1-15.
- [10] Priyono, (2016), "Penerapan Algoritma Caesar Cipher dan Algoritma Vigenere Cipher Dalam Pengamanan Pesan Teks", *Jurnal Riset Komputer (JURIKOM)*, vol. 3, no. 5, pp. 351-356.
- [11] I., Yatini B., and F., D., Astuti, (2015), "Analisis Performansi Kriptografi Menggunakan Algoritma Affine Cipher, Vigenere Cipher Base64", *Jurnal Teknik*, vol. 5, no. 1, pp. 64-70.
- [12] A.Menezes, P.Van Oorschot dan S.Vanstone. (1996), "Handbook of Applied Cryptography", NewYork: CRC Press, 1996.