ARTIKEL

JUST ME (JM) APLIKASI KEAMANAN *WINDOWS* DENGAN MEMANFAATKAN METODE STEGANOGRAFI DAN KRIPTOGRAFI KLASIK *CAESAR CIPHER*

Oleh:

JAMAL ABDUL NASIR

13.1.03.02.0358

Dibimbing oleh :

1. **Intan Nur Farida, M.Kom.**
2. **Fajar Rohman Hariri, M.Kom.**

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS TEKNIK

UNIVERSITAS NUSANTARA PGRI KEDIRI

2017

Skripsi Oleh :

JAMAL ABDUL NASIR
NPM : 13.1.03.02.0358

Judul :

JUST ME* (JM) APLIKASI KEAMANAN *WINDOWS* DENGAN MEMANFAATKAN METODE STEGANOGRAFI DAN KRIPTOGRAFI KLASIK *CAESAR CIPHER

Telah Disetujui untuk Diajukan Kepada
Panitia Ujian/Sidang Skripsi
Program Studi Teknik Informatika Fakultas Teknik
Universitas Nusantara PGRI Kediri

Tanggal : 14 JUNI 2017

Pembimbing I	Pembimbing II
Intan Nur Farida, M.Kom.	Fajar Rohman Hariri, M.Kom.
NIDN. 0704108701	NIDN. 0715058902

ii

Skripsi Oleh :

JAMAL ABDUL NASIR
NPM : 13.1.03.02.0358

Judul :

JUST ME* (JM) APLIKASI KEAMANAN *WINDOWS* DENGAN MEMANFAATKAN METODE STEGANOGRAFI DAN KRIPTOGRAFI KLASIK *CAESAR CIPHER

Telah dipertahankan di depan Panitia Ujian/Sidang Skripsi
Program Studi Teknik Informatika Fakultas Teknik
Universitas Nusantara PGRI Kediri
Pada tanggal : 3 Agustus 2017

Dan Dinyatakan telah Memenuhi Persyaratan

Panitia Penguji :

1. Ketua : Intan Nur Farida, M.Kom.
2. Penguji I : Ahmad Bagus Setiawan, S.T., M.M., M.Kom.
3. Penguji II : Fajar Rohman Hariri, M.Kom.

Mengetahui,
Dekan Fakultas Teknik

Dr. Suryo Widodo, M.Pd.
NIP.19640202 199103 1 002

iii

Artikel Skripsi
Universitas Nusantara PGRI Kediri

SURAT PERNYATAAN

ARTIKEL SKRIPSI TAHUN 2017

Yang bertanda tangan di bawah ini:

Nama Lengkap	: Jamal Abdul Nasir
NPM	: 13.1.03.02.0358
Telepun/HP	: 085755531502
Alamat Surel (Email)	: deviljm_26@yahoo.com
Judul Artikel	: *Just Me* (JM) Aplikasi Keamanan *Windows* dengan Memanfaatkan Metode Steganografi dan Kriptografi Klasik *Caesar Cipher*
Fakultas - Program Studi	: Teknik - Teknik Informatika
Nama Perguruan Tinggi	: Universitas Nusantara PGRI Kediri
Alamat Perguruan Tinggi	: Jalan K.H. Ahmad Dahlan 76, Mojoroto, Kota Kediri

Dengan ini menyatakan bahwa :

a. artikel yang saya tulis merupakan karya saya pribadi (bersama tim penulis) dan bebas plagiarisme;

b. artikel telah diteliti dan disetujui untuk diterbitkan oleh Dosen Pembimbing I dan II.

Demikian surat pernyataan ini saya buat dengan sesungguhnya. Apabila di kemudian hari ditemukan ketidaksesuaian data dengan pernyataan ini dan atau ada tuntutan dari pihak lain, saya bersedia bertanggungjawab dan diproses sesuai dengan ketentuan yang berlaku.

Mengetahui		Kediri, 8 Agustus 2017
Pembimbing I	Pembimbing II	Penulis,
Intan Nur Farida, M.Kom NIDN. 0704108701	Fajar rohman Hariri, M.Kom NIDN. 0715058902	Jamal Abdul Nasir NPM. 13.1.03.02.0358

JUST ME (JM) APLIKASI KEAMANAN *WINDOWS* DENGAN MEMANFAATKAN METODE STEGANOGRAFI DAN KRIPTOGRAFI KLASIK *CAESAR CIPHER*

JAMAL ABDUL NASIR
13.1.03.02.0358
TEKNIK - TEKNIK INFORMATIKA
deviljm_26@yahoo.com
Intan Nur Farida, M.Kom. dan Fajar Rohman Hariri, M.Kom.

UNIVERSITAS NUSANTARA PGRI KEDIRI

ABSTRAK

Penelitian ini dilatar belakangi dari pengamatan dan pengalaman peneliti selama masa perkuliahan ataupun dari lingkungan sekitar, bahwa keamanan terhadap sistem komputer dan data sering kali terabaikan. Sehingga komputer rentan terhadap pengubahan konfigurasi sistem operasi, pencurian data, modifikasi data, dan pengaksesan data pribadi dari pihak yang tidak berwenang. Permasalahan penelitian ini adalah (1) Bagaimana membangun aplikasi untuk mempermudah pengguna dalam mengamankan sistem operasi dan data. (2) Bagaimana cara mengamankan data dengan mengenkripsi nama ataupun ekstensi file menggunakan metode Kriptografi Klasik *Caesar Cipher*. Penelitian ini menggunakan metode Steganografi yang berfungsi untuk mengamankan data berupa *folder*, menggunakan metode Kriptografi Klasik *Caesar Cipher* untuk mengamankan data dengan cara mengenkripsi *file* ataupun ekstensi *file* sehingga data tidak mudah dibaca, serta memanfaatkan fungsi dari sistem operasi *Windows* untuk membantu mengamankan sistem operasi dan data. Berdasarkan hasil dari penelitian, dengan memanfaatkan beberapa fungsi sistem operasi *Windows* yang dapat digunakan untuk mengamankan sistem operasi dan data, konfigurasinya dapat dilakukan dengan mudah melalui *Just Me*. Pengamanan data menggunakan metode Steganografi berfungsi untuk mengubah fungsi dan icon *folder* menjadi suatu fungsi *Windows* sehingga data pada *folder* tidak dapat dilihat, dicari, ataupun disalin. Pengamanan data dengan cara mengenkripsi nama atau ekstensi *file* dengan metode Kriptografi Klasik *Caesar Cipher* membuat *file* tidak terbaca atau sulit dikenali oleh program ataupun penglihatan manusia, sehingga data menjadi aman karena sulit untuk diakses dan dicari.

Kata Kunci : *Just Me*, Steganografi, *Caesar Cipher*, Keamanan *Windows*.

I. Latar Belakang

Keamanan sistem operasi dan data merupakan suatu hal yang penting, namun kebanyakan orang yang awam dalam komputer kurang memperhatikan hal tersebut dikarenakan keterbatasan pengetahuan ataupun hal lainnya yang menyebabkan pengabaian terhadap keamanan sistem operasi dan data. Kita tidak pernah tahu apa yang akan dilakukan pada komputer atau laptop kita jika digunakan orang lain, seperti halnya mengakses

program yang dapat mengubah konfigurasi sistem ataupun program yang berbahaya seperti virus, mengakses folder-folder atau *local disk drive* pribadi maupun data-data penting yang bersifat pribadi. Tindakan tersebut dapat menyebabkan terjadinya pencurian data, kerusakan data, kerusakan sitem operasi, pengubahan konfigurasi sistem, pengoperasian aplikasi yang seharusnya tidak dibolehkan untuk umum, dan sebagainya.

Sebenarnya di dalam sistem operasi *windows* sendiri sudah terdapat beberapa fitur yang berfungsi untuk keamanan komputer, namun untuk mengakses dan menggunakan fitur tersebut harus mempelajari sistem operasi *windows*, dan pengetahuan tentang pengoperasian *command prompt*, *registry editor*, dan *group policy editor*, tetapi untuk mengakses dan memanfaatkan fitur-fitur tersebut sedikit sulit dan jarang sekali orang awam yang memanfaatkannya karena program tersebut memiliki *interface* yang cukup rumit.

Dalam era teknologi seperti sekarang ini banyak kejahatan yang memanfaatkan teknologi yang bertujuan untuk mencari keuntungan dengan cara tertentu seperti mencuri, memanipulasi, dan bahkan mengenkripsi data menggunakan *ransomware* dan memberikan suatu ancaman kepada pemilik data tersebut untuk memberikan tebusan apabila ingin data tersebut dikembalikan.

Dengan permasalahan tersebut maka diperlukan suatu aplikasi untuk mempermudah pengguna dalam mengamankan sistem operasi dan data pada komputer dengan memanfaatkan steganografi, kriptografi klasik, dan sistem operasi *windows* itu sendiri. Aplikasi ini dapat digunakan pada komputer yang menggunakan sistem operasi *windows* untuk mempermudah konfigurasi keamanan sistem operasi maupun mengamankan data-data yang bersifat pribadi. Dengan demikian pengguna tidak perlu kesuliatan dalam mengamankan data secara manual seperti memanipulasi kode *registry* pada sistem operasi *windows* yang dapat menyebabkan kerusakan pada sistem operasi jika tidak dilakukan secara tepat.

Berdasarkan uraian diatas dapat disimpulkan bahwa keamanan terhadap sistem operasi dan data itu

sangatlah diperlukan, sehingga peneliti tertarik untuk membangun "**Aplikasi Keamanan *Windows* Dengan Memanfaatkan Metode Steganografi dan Kriptografi Klasik *Caesar Cipher***" untuk mempermudah pengamanan sistem operasi dan data pada komputer.

II. Metode

1. Konfigurasi Registry *Windows*

Menurut Simpony (2015) pengertian *Registry* sebagai berikut :

> *Registry Editor* pada sistem operasi *Windows* merupakan pusat dari segala konfigurasi sistem operasi baik itu perangkat lunak maupun perangkat keras. Pengubahan pengaturan di *registry* bisa mengakibatkan sistem tidak berjalan sebagaimana mestinya.

Menurut Fatkhiyah (2012) isi dari *registry* adalah :

> Isi dari *registry* secara umum terdiri dari dua unsur, yaitu *Hive* dan *Value Entry*. *Hive* merupakan sarang atau cabang utama dari *registry* yang berfungsi menangani kasus-kasus tertentu. Umumnya dalam *registry* terdapat 5 macam *Hive*, yaitu :
> 1) HKEY_CLASSES_ROOT, Merupakan *Subkey* dari HKEY_LOCAL_MACHINE\Software. Biasa digunakan untuk mengatur file asosiasi ketika membuka suatu file melalui *Windows Explorer*.
> 2) HKEY_CURRENT_USER, yang akan digunakan untuk menyimpan informasi konfigurasi dari *user* yang sedang aktif saat ini, dan merupakan *subkey* dari HKEY_USERS. Pada *key* ini dapat dilakukan pengaturan yang diantaranya adalah pengaturan seputar *Folder*, *Control Panel*, *Windows Explorer*, dan tampilan layar yang digunakan oleh *user* tersebut.
> 3) HKEY_LOCAL_MACHINE, berisi informasi seputar *hardware*, *software*, dan lain sebagainya yang terpasang dan berhubungan dengan *Windows*. *Key* ini berlaku untuk semua aplikasi *user*.
> 4) HKEY_USERS, merupakan induk dari HKEY_CURRENT_USER. Fungsinya adalah menyimpan informasi semua *user* yang ada di komputer tersebut.
> 5) HKEY_CURRENT_CONFIG, memuat informasi seputar *profile hardware* yang digunakan pada suatu komputer.

Konfigurasi *registry windows* digunakan untuk mengaktifkan ataupun menonaktifkan beberapa fungsi *windows* yang dapat digunakan untuk mengamankan sistem operasi *windows*, berikut ini merupakan sebagian contoh dari konfigurasi *registry* secara manual dengan merubah konfigurasi *Windows* melalui registry :

1) *Disable - Enable Command Prompt* (CMD.exe)

HKEY_CURRENT_USER\SOFTWARE\Policies\Microsoft\Windows\System\
Name : DisableCMD
Type : REG_DWORD
Value : 0 (Enable), 1 (Disable), 2 (Disable, Allow Batch Files)

2) *Disable - Enable Registry Editor* (RegEdit.exe)
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\
Name : DisableRegistryTools
Type : REG_DWORD
Value : 0 (Enable), 1 (Disable), 2 (Disable, Allow Runnning Silently)

2. Konfigurasi *Hosts File*

Dalam fungsinya *hosts file* dapat diguanakan untuk memetakan nama *host* atau *domain* kedalam alamat IP, untuk *mengkonfigurasi hosts file* maka diperlukan akses administrator untuk dapat menambahkan *list* nama *host* atau *domain* kedalam *hosts file*, untuk mengakses *hosts file* berikut ini merupakan lokasi *hosts file* dari sistem operasi *Windows*.

Untuk memetakan host/domain kedalam IP *address* dengan format :

IP [spasi] Nama *Host/Domain*

Berikut contoh memetakan alamat *host/domain* dengan IP *localhost* :

127.0.0.1 www.google.com
127.0.0.1 google.com
127.0.0.1 facebook.com

Dari contoh konfigurasi diatas akan menyebabkan *host/domain* tersebut akan mengarah ke *localhost* komputer apabila diakses menggunakan browser sehingga *hosts/domain* tidak bisa diakses, proses ini dapat digunakan sebagai pengamanan terhadap akses alamat suatu sistus yang terdapat mengandung konten yang kurang baik bagi pengguna.

3. Steganografi Folder

Menurut Ibrahim (2008) pengertian steganografi adalah :

> Kata steganografi (*steganography*) berasal dari bahasa Yunani *steganos*, yang artinya 'tersembunyi/terselubung', dan *graphein*, 'menulis' sehingga kurang lebih artinya "menulis (tulisan) terselubung". Teknik ini meliputi banyak sekali metoda komunikasi untuk menyembunyikan pesan rahasia. Metode ini termasuk tinta yang tidak tampak, *microdots*, pengaturan kata, tanda tangan digital, jalur tersembunyi dan komunikasi spektrum lebar.

Implementasi metode steganografi pada folder ini akan membuat *icon* dan fungsi folder akan berubah menjadi suatu fungsi

windows yang telah terdaftarkan di dalam *registry*, untuk mengubah folder menjadi fungsi *windows* yang lain yaitu dengan cara :

1) *Rename* FolderPath Menjadi FolderPath + ekstensi CLSIDKey
2) Merubah Atribut folder menjadi *SystemFile*
3) Aktifkan Konfigurasi *Hide System File*

Untuk menemukan nomer register suatu fungsi *windows* seperti *recycle bin, windows security, my computer, user folder,* dan *public folder* dapat dilakukan dengan cara mencarinya melalui *registry editor (regedit.exe).*

```
procedure TForm1.ProteksiFolder(Sender:
TObject);
var
folderpath, new_foldername:string;
const
K_publicfolder='.{4336a54d-038b-4685-ab02-
99bb52d3fb8b}';
begin
  folderpath:='E:\Testing';
  new_foldername:=folderpath+K_publicfolder;
     if RenameFile(folderpath, new_foldername)
then
      begin
        SetFileAttributes(pchar(new_foldername),
faSysFile);
        ShowMessage('Folder Berhasil di Proteksi');
      end
      else
        ShowMessage('Folder Gagal di Proteksi');
end;
```

Prosedur tersebut merupakan prosedur untuk memproteksi folder dengan alamat E:\Testing dengan menambahkan ekstensi dari variabel K_publicfolder ke folder tersebut menjadi

Folder awal :

E:\Testing

Folder terproteksi menjadi :

E:\Testing.{4336a54d-038b-4685-ab02-99bb52d3fb8b}

Maka folder tersebut akan berubah *icon* dan fungsinya menjadi *Public Folder* sehingga apabila folder tersebut dieksekusi atau di buka akan mengarahkan ke *Public Folder* dan pengguna lain tidak bisa membuka isi dari folder tersebut.

4. Kriptografi

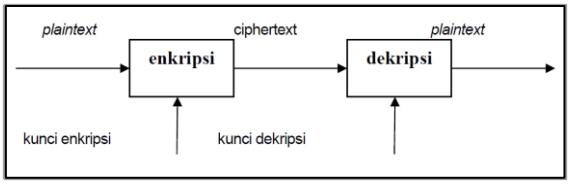
Menurut Fairuzabadi (2010) pengertian kriptografi adalah :

> Kriptografi adalah suatu ilmu yang mempelajari bagaimana cara menjaga agar data atau pesan tetap aman saat dikirimkan, dari pengirim ke penerima tanpa mengalami gangguan dari pihak ketiga. Konsep kriptografi sendiri telah lama digunakan oleh manusia misalnya pada peradaban Mesir dan Romawi walau masih sangat sederhana.

Menurut Kurniawan (2004) pengertian kriptografi adalah :

> Penyandian merupakan salah satu alternatif atau cara untuk mengamankan atau menjaga suatu

kerahasiaan data atau gambar. Seni dan ilmu untuk menyandikan atau menjaga keamanan atau serta kerahasian pesan disebut kriptografi.



Gambar 1. Diagram proses enkripsi dan dekripsi (Fairuzabadi, 2010).

5. ***Caesar Cipher***

Menurut Husein (2014) pengertian *Caesar Cipher* sebgai berikut :

> *Caesar Cipher* atau sering disebut juga subtitusi *cipher* merupakan penggantian setiap karakter dari *plaintext* dengan karakter lainnya. Pada zaman Romawi kuno dikisahkan tentang Julius Caesar yang ingin mengirimkan satu pesan rahasia kepada seorang jenderal di medan perang. Pesan tersebut harus dikirimkan melalui seorang kurir, tetapi karena pesan tersebut mengandung rahasia, Julius Caesar tidak ingin pesan tersebut terbuka di tengah jalan. Julius caesar kemudian memikirkan cara mengatasinya, yaitu dengan mengacak pesan tersebut menjadi suatu pesan yang tidak dapat dipahami oleh siapapun kecuali hanya dapat dipahami oleh jenderal saja. Tentu sang jenderal telah diberitahu sebelumnya bagaimana cara membaca pesan yang teracak tersebut karena telah mengetahui kuncinya.

Menurut Husein (2014) algoritma *Caesar Cipher* sebagai berikut :

> Algoritma dari *Caesar Cipher* adalah jika (a=1, b=2, dan seterusnya). *Plaintext* diberi simbol "P" dan *Ciphertext* adalah "C", dan kunci adalah "K" :

C = E(P) = (P + K) mod (26)

Dari contoh di atas, enkripsi dapat dilakukan dengan rumus :
C = E(P) = (P + K) mod (26)

Rumus untuk melakukan dekripsi dari *ciphertext* :
P = D(C) = (C - K) mod (26)

III. HASIL DAN KESIMPULAN

1. Hasil

a. Tampilan Menu *System Editor*

Halaman System Editor merupakan menu digunakan untuk enable/disable sistem editor.

Gambar 2. Tampilan *System Editor*

b. Tampilan Menu *Control Panel*

Halaman *Control Panel* menu yang berfungsi untuk *show/hide control panel items* tampilan menu.

Gambar 3. Tampilan *Control Panel*

c. Tampilan Menu *Desktop Explorer*

Menu *desktop explorer* menu yang diakses dari menu *system* yang berfungsi untuk *disable/enable* menu-menu *desktop* & *windows explorer*.

Gambar 4. Tampilan *Desktop Explorer*

d. Tampilan Menu *Disk Drives*

Menu *Disk Drives* berfungsi untuk *show/hide atau allow/block local disk drives*.

Gambar 5. Tampilan *Disk Drives*

e. Tampilan Menu Folder Protector

Menu *folder protector* merupakan menu steganografi yang digunakan untuk memproteksi *folder* dengan menggunakan metode steganografi.

Gambar 6. Tampilan *Folder Protector*

f. Tampilan *File Encryptor*

Menu *File Encryptor* merupakan menu kriptografi klasik *caesar cipher* berfungsi untuk enkripsi/dekripsi ekstensi atau nama *file*.

Gambar 7. Tampilan *File Encryptor*

g. Tampilan *Drive Freezer*

Menu *Drive Freezer* berfungsi untuk membatasi hak akses terhadap penggunaan *removable disk drives*.

Gambar 8. Tampilan *Drive Freeze*

h. Tampilan *App Blocker*

Pada halaman ini berfungsi untuk membatasi hak akses terhadap penggunaan aplikasi.

Gambar 9. Tampilan *App Blocker*

i. Tampilan *Web Blocker*

Pada halaman ini berfungsi untuk membatasi hak akses terhadap suatu domain/*website*.

Gambar 10. Tampilan Menu *Web Blocker*

j. Tampilan Menu *Options*

Menu *Options* merupakan menu yang berfungsi untuk menambahkan *password* dan untuk menginstal *Just Me*.

Gambar 11. Tampilan Menu *Options*

2. Kesimpulan

Setelah menyelesaikan perancangan dan pembuatan *Just Me (JM)* Aplikasi Keamanan *Windows* dengan Memanfaatkan Metode Steganografi dan Kriptografi Klasik *Caesar Cipher* serta melakukan uji coba dan evaluasi, maka dapat ditarik kesimpulan sebagai berikut :

1. Aplikasi berfungsi untuk melakukan konfigurasi pada sistem operasi *Windows* yang dapat digunakan untuk mengamankan sistem operasi dan data dengan mudah. Pengamanan data menggunakan metode Steganografi berfungsi untuk mengubah fungsi dan icon *folder* menjadi suatu fungsi *Windows* sehingga data pada *folder* tidak dapat dilihat, dicari, ataupun disalin.

2. Pengamanan data dengan cara mengenkripsi nama atau ekstensi *file* dengan metode Kriptografi Klasik *Caesar Cipher* membuat *file* tidak terbaca atau sulit dikenali oleh program ataupun penglihatan manusia, sehingga data menjadi aman karena sulit untuk diakses dan dicari.

IV. DAFTAR PUSTAKA

Fairuzabadi, M. 2010. Implementasi Kriptografi Klasik Menggunakan Borland Delphi, (Online), 4 (2): 65-78, tersedia : http://upy.ac.id/dinamika-informatika/wp-content/uploads/2013/01/Fairuz-Jurnal-Implemntasi-Kriptografi-Klasik-Menggunakan-Borland-Delphi.pdf, diunduh 05 Nopember 2016.

Fatkhiyah, E., & Doddy, M.I. 2012. Sistem Virus Batch Sederhana. Jurnal Teknologi TECHNOSCIENTIA 4 (2): 161-168.

Husein, M. 2014. Implementasi Caesar Cipher Untuk Penyembunyian Pesan Teks Rahasia Pada Citra dengan Menggunakan Metode Least Significant Bit. Jurnal Pelita Informatika Budi Darma, 7 (2): 116-122.

Ibrahim, R.N. 2008. Proteksi File dan Folder Menggunakan Metode Steganografi. Jurnal Computech & Bisnis. 2 (2): 69-107.

Kurniawan, Y., 2004, *Kriptografi Keamanan Internet dan Jaringan*, Informatika, Bandung.

Simpony, B.K. 2015. Remote Registry Editor. Jurnal Informatika. 2 (1): 173-180.