Building Informatics, Technology and Science (BITS), Vol 1, No 1, Juni 2019
ISSN 2684-8910 (media cetak)
Hal 1-6

Implementasi Algoritma Route Cipher Dalam Pengamanan File Pdf

Meylisa Siska Bangun

Program Studi Teknik Informatika, STMIK Budi Darma, Medan, Indonesia
Email: meylisasiska@gmail.com *)

Abstrak

Keamanan data merupakan suatu cara yang dilakukan untuk menjaga kerahasiaan informasi agar tidak dicuri atau dimanipulasi oleh pihak yang tidak bertanggungjawab. Aspek-aspek keamanan data meliputi authentication, integrity, nonrepudation, authority, confidentiality, privacy, availability dan acces control. Salah satu masalah kemanan data yang sering terjadi adalah pengambilan data rahasia yang dimiliki suatu perusahaan ataupun perorangan yang sangat merugikan apabila disalahgunakan oleh pihak yang tidak bertanggungjawab. Banyaknya aplikasi-aplikasi yang dapat membantu dalam memecahkan kode keamanan yang ada sekarang ini, sehingga diperlukan suatu sistem keamanan yang berfungsi untuk melindungi informasi dari berbaai ancaman. File Portable Document Format (PDF) merupakan format berkas yang banyak digunakan di dalam pertukaran informasi, oleh karena itu setiap dokumen yang memilki format tersebut harus diamankan terlebih dahulu agar tidak dimanipulasi dan dimanfaatkan oleh pihak-pihak yang tidak berhak.

Kata Kunci: Algoritma, Route, Cipher, Pengamanan, File

Abstract

Data security is a way that is done to maintain the confidentiality of information so that it is not stolen or manipulated by irresponsible parties. Data security aspects include authentication, integrity, nonrepudiation, authority, confidentiality, privacy, availability and access control. One of the data security problems that often occurs is confidential data retrieval owned by a company or individual which is very detrimental if misused by irresponsible parties. The number of applications that can help in solving security codes that exist today, so we need a security system that serves to protect information from various threats. Portable Document Format (PDF) is a file format that is widely used in information exchange, therefore every document that has this format must be secured in advance so that it is not manipulated and utilized by unauthorized parties.

Keywords: Algorithm, Route, Cipher, Security, File

1. PENDAHULUAN

Banyaknya aplikasi-aplikasi yang dapat membantu dalam memecahkan kode keamanan yang ada sekarang ini, sehingga diperlukan suatu sistem keamanan yang berfungsi untuk melindungi informasi dari berbaai ancaman. *File Portable Document Format* (*PDF*) merupakan format berkas yang banyak digunakan di dalam pertukaran informasi, oleh karena itu setiap dokumen yang memilki format tersebut harus diamankan terlebih dahulu agar tidak dimanipulasi dan dimanfaatkan oleh pihak-pihak yang tidak berhak.

Salah satu cara yang dapat digunakan adalah dengan teknik kriptografi, Kriptografi merupakan ilmu sekaligus seni untuk menjaga keamanan informasi. Secara umum ada 2 jenis kriptografi yaitu kriptografi klasik dan kriptografi modern. Algoritma yang dapat digunakan untuk mengamankan suatu data adalah algoritma *Route cipher* yaitu sebuah kriptografi klasik yang menggunakan *transposisi* dalam melakukan enkripsi. Plainteks pertama kali ditulis dalam *grid* dimensi yang diberikan kemudian membacakan pola yang diberikan dalam kunci. Untuk pesan yang panjang jumlah kemungkinan kunci berpotensi terlalu besar untuk dihitung. Namun tidak semua kunci sama-sama baik. Jalur buruk yang dipilih akan meninggalkan potongan plainteks yang berlebih atau teks hanya terbalik dan ini akan memberikan kriptanalis petunjuk mengenai rute yang digunakan.

Proses yang akan dilakukan di dalam penelitian ini adalah menganalisa proses enkripsi dan dekripsi menggunakan algoritma *route cipher* kemudian merancang aplikasi keamanan *file PDF* menggunakan alat bantu perancangan seperti *Unified Modelling Language* dan dengan *tools Microsoft Visual Studio .Net 2008* , sehingga menghasilkan aplikasi yang dapat mengamankan *file PDF* dengan cara menyandikan *file* tersebut menggunakan algoritma *route cipher*. Setelah selesai perancangan, kemudian *file* PDF akan dienkripsi dan didekripsi menggunakan aplikasi keamanan tersebut. Hasil dari proses enkripsi dan dekripsi berupa karakter yang sulit dimengerti oleh orang yang tidak memiliki izin untuk melihat *file* tersebut.

2. METODE PENELITIAN

2.1 Kriptografi

Kriptografi berasal dari bahasa Yunani, yaitu dari kata *crypto* dan *graphia* yang berarti pesan rahasia, Kriptografi adalah ilmu ataupun seni yang mempelajari bagaimana membuat suatu pesan yang dikirim oleh pengirim dapat disampaikan kepada penerima dengan aman. Kriptografi merupakan bagian dari cabang ilmu Matematika yang disebut kriptologi. Kriptografi bertujuan menjaga kerahasiaan informasi yang terkandung dalam data sehingga informasi tersebut tidak dapat diketahui oleh pihak yang tidak sah. Perancang algoritma kriptografi disebut kriptografer.

2.2 Route Cipher

Building Informatics, Technology and Science (BITS), Vol 1, No 1, Juni 2019
ISSN 2684-8910 (media cetak)
Hal 1-6

Pada algoritma *route cipher*, *plaintext* ditulis ke dalam sebuah *array* atau beberapa kata yang tersusun, kemudian dibaca sebagai perintah yang menentukan sebuah rute yang melalui *array*. Contohnya dapat dilihat pada gambar dibawah ini dimana *plaintext* ditulis ke dalam sebuah *array* kemudian *ciphertext* dibaca dalam beberapa perintah.

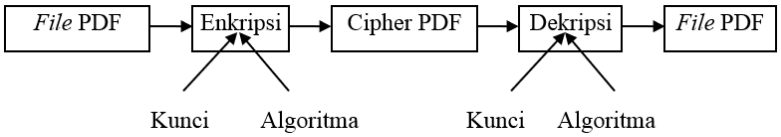
Langkah-langkah algoritma *route cipher* adalah sebagai berikut:

1. Buat matriks dengan jumlah baris yang akan diisi *plaintext* dengan membagi jumlah *plaintext* dengan kunci.
2. Melakukan penentuan arah transposisi *plaintext*, contohnya jika arah yang ditentukan adalah spiral, maka *ciphertext* dihasilkan dengan membaca *plaintext* dalam matriks dengan arah spiral.
3. Untuk proses dekripsinya, algoritma *route cipher* hanya membaca posisi berdasarkan urutan kata yang disusun dalam matriks berdasarkan susunan dari arah yang digunakan untuk membentuk *ciphertext*.

3. ANALISA DAN PEMBAHASAN

Proses pegamanan *file Portable Document Format* (PDF) dengan teknik kriptografi adalah melakukan penyandian terhadap *file* PDF tersebut sehingga informasi yang ada di dalam *file* tersebut tidak sama lagi dengan aslinya dan menjadi informasi yang tidak dapat dimengerti. Proses penyandian *file* PDF dengan teknik kriptografi membutuhkan sebuah kunci yang akan digunakan untuk proses enkripsi, yaitu proses penyandian *file* PDF menjadi kode-kode yang tidak dimengerti yang disebut *ciphertext* dan proses dekripsi, yaitu proses pengembalian *ciphertext* ke bentuk awalnya yang disebut *plaintext*.

Prosedur pengamanan *file* PDF secara umum dapat dilihat pada gambar berikut yang merupakan mekanisme kerja teknik kriptografi dalam mengamankan *file*.

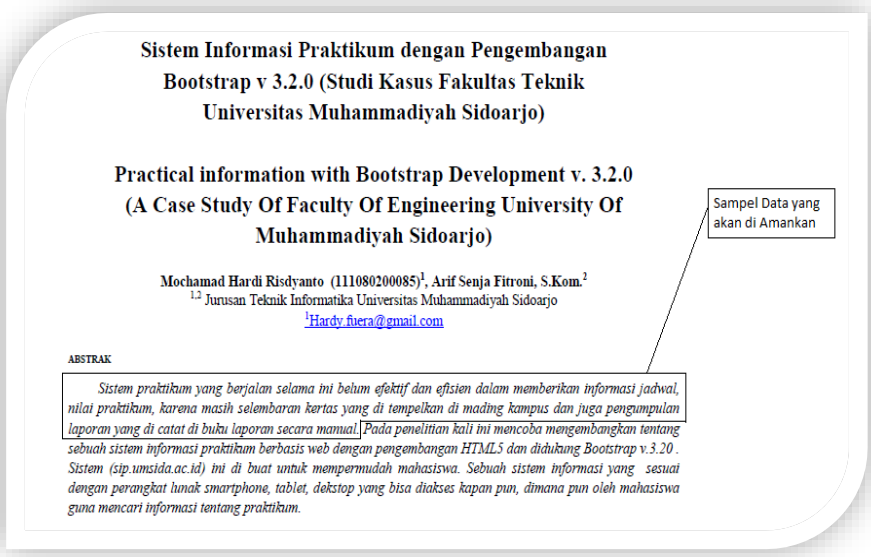


Gambar 1. Prosedur Pengamanan *File* PDF dengan Teknik Kriptografi

Algoritma *route cipher* merupakan salah satu teknik kriptografi yang termasuk di dalam teknik kriptografi klasik yang menggunakan transposisi dalam melakukan penyandian terhadap *plaintext*. *Route cipher* melakukan transposisi dengan cara menuliskan teks asli secara kolom dari atas ke bawah dalam sebuah kisi-kisi imajiner dengan ukuran yang telah disepakati. Teks sandinya dibaca dengan arah (*route*) sesuai perjanjian, misalnya dibaca secara spiral dengan arah
jarum jam, mulai dari kiri atas atau secara ular tangga, mulai dari kanan bawah dan lain-lain cara pembacaannya.

3.1 Proses Enkripsi

Berikut ini sampel data yang akan dienkripsi menggunakan algoritma transposisi *route cipher*:



Gambar 2. Teks Yang Akan Diamankan

Berdasarkan gambar 2 *plaintext* yang akan digunakan adalah teks yang terdapat didalam garis kotak. Adapun langkah-langkah dari algoritma *route cipher* adalah sebagai berikut:

Building Informatics, Technology and Science (BITS), Vol 1, No 1, Juni 2019
ISSN 2684-8910 (media cetak)
Hal 1-6

a. Membaca *plaintext* yang akan dienkripsi.
Plaintext : Sistem praktikum yang berjalan selama ini belum efektif dan efisien dalam memberikan informasi jadwal, nilai praktikum, karena masih selembaran kertas yang di tempel kan di madding kampus dan juga pengumpulan laporan yang di catat di buku laporan secara manual.

b. Konversi teks ke bilangan desimal dan *input*-kan kunci untuk membentuk larik (*array*) yang berdasarkan kunci, di dalam contoh ini kunci yang digunakan adalah 7, jika kata yang di karakter melebihi dari 7x7 *array* yang terbentuk akan dilakukan enkripsi kembali, maka nilai desimal dari *plaintext* akan terbentuk seperti berikut:

Tabel 1. Konversi *Array* I

83	105	115	116	101	109	32
112	114	97	107	116	105	107
117	109	32	121	97	110	103
32	98	101	114	106	97	108
97	110	32	115	101	108	97
109	97	32	105	110	105	32
98	101	108	117	109	32	101

Kemudian *ciphertext* didapatkan dengan menyusun *teks* sesuai dengan arah yang sudah ditentukan dan mendapatkan hasil sebagai berikut:
Ciphertext array I = 83 112 117 32 97 109 98 101 108 117 109 32 101 32 97 108 103 107 32 109 101 116 115 105 114 109 98 110 97 32 105 110 105 108 97 110 105 116 107 97 32 101 32 115 101 106 97 121 114

Jika dikonversi ke karakter menjadi:
Ciphertext = Spu ambelum e algkmetsirmbna inilanitka e sejayr

Tabel 2. Konversi *Array* II

102	104	107	116	105	102	32
100	97	110	32	101	102	105
115	105	101	110	32	100	97
108	97	109	32	109	101	109
98	101	114	105	107	97	110
32	105	110	102	111	114	109
97	115	105	32	106	97	100

Kemudian *ciphertext* didapatkan dengan menyusun *teks* sesuai dengan arah yang sudah ditentukan dan mendapatkan hasil sebagai berikut:
Ciphertext array II = 102 100 115 108 98 32 97 115 105 32 106 97 100 109 110 109 97 105 32 102 105 116 107 101 97 105 97 101 105 110 102
111 114 97 101 100 102 101 32 110 101 109 114 105 107 109 32 110 32.

Jika dikonversi ke karakter menjadi:
Ciphertext = Fdslb a si jadmnmaife naiaerikm n

Tabel 3. Konversi *Array* III

119	97	108	44	32	110	105
108	97	105	32	112	114	97
107	116	105	107	117	109	44
32	107	97	114	101	110	97
32	109	97	115	105	104	32
115	101	108	101	109	98	97
114	97	110	32	107	101	114

Building Informatics, Technology and Science (BITS), Vol 1, No 1, Juni 2019
ISSN 2684-8910 (media cetak)
Hal 1-6

Kemudian *ciphertext* didapatkan dengan menyusun *teks* sesuai dengan arah yang sudah ditentukan dan mendapatkan hasil sebagai berikut:
Ciphertext array III = 119 108 107 32 32 115 114 97 110 32 107 101 114 97 32 97 97 105 110 32 44 108 97 97 116 107 109 101 108 101 109 98 104 110 109 114 112 32 105 105 97 97 115 105 101 117 107 114

Jika dikonversi ke karakter menjadi:
Ciphertext = wlk sran kera a,arp iatkmasihnmrp iiaasieukr

Tabel 4. Konversi *Array* IV

116	97	115	32	121	97	110
103	32	100	105	32	116	101
109	112	101	108	107	97	110
32	100	105	32	109	97	100
105	110	103	32	107	97	109
112	117	115	32	100	97	110
32	106	117	103	97	32	112

Kemudian *ciphertext* didapatkan dengan menyusun *teks* sesuai dengan arah yang sudah ditentukan dan mendapatkan hasil sebagai berikut:
Ciphertext array IV= 116 103 109 32 105 112 32 106 117 103 97 32 112 110 109 100 110 101 110 97 121 32 115 97 32 112 100 110 117 115 32 100 97 97 97 116 32 105 100 101 105 103 32 107 109 107 108 32

Jika dikonversi ke karakter menjadi:
Ciphertext = tgm ip juga pnmdnenay sa pdnus daaaat ideig kmkl

Tabel 5. Konversi *Array* V

101	110	103	117	109	112	117
108	97	110	32	108	97	112
111	114	97	110	32	121	97
110	103	32	100	105	99	97
116	97	116	32	100	105	32
98	117	107	117	32	108	97
112	111	114	97	110	32	115

Kemudian *ciphertext* didapatkan dengan menyusun *teks* sesuai dengan arah yang sudah ditentukan dan mendapatkan hasil sebagai berikut:
Ciphertext array V= 101 108 111 110 116 98 112 111 114 97 110 32 115 97 32 97 97 112 117 112 109 117 103 110 97 114 103 97 117 107 117 32 108 105 99 121 97 108 32 110 97 32 116 32 100 105 32 110 100

Jika dikonversi ke karakter menjadi:
Ciphertext = elontbporan sa aapupmugnargauku licyal na t di lnd
Jadi, setelah dienkripsi seluruhnya, maka *ciphertext* yang didapat adalah:

Ciphertext = Spu ambelum e algkmetsirmbna inilanitka e sejayr Fdslb a si jadmnmaife naiaerikm n wlk sran kera a,arp iatkmasihnmrp iiaasieukr tgm ip juga pnmdnenay sa pdnus daaaat ideig kmkl elontbporan sa aapupmugnargauku licyal na t di lnd

3.2 Proses Dekripsi

Proses dekripsi merupakan proses mengembalikan pesan menjadi seperti awal kembali. Langkah-langkah proses dekripsi adalah dengan mengkonversi *ciphertext* terlebih dahulu, kemudian melakukan pembentukan *array* berdasarkan kunci yang digunakan dan *cipherteks* dibaca dan disusun berdasarkan arah yang digunakan pada saat proses enkripsi sehingga dapat mengembalikan *plaintext*.

Ciphertext = Spu ambelum e algkmetsirmbna inilanitka e sejayr Fdslb a si jadmnmaife naiaerikm n wlk sran kera a,arp iatkmasihnmrp iiaasieukr tgm ip juga pnmdnenay sa pdnus daaaat ideig kmkl elontbporan saaapupmu gnargau
ku licyal na t di lnd.

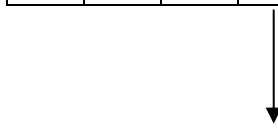
Langkah-langkah proses dekripsi adalah sebagai berikut:

a. Lakukan pembacaan *array* dan mengkonversi ke nilai desimal.
Ciphertext I : Spu ambelum e algkmetsirmbna inilanitka e sejayr
Desimal : 83 112 117 32 97 109 98 101 108 117 109 32 101 32 97 108 103 107 32 109 101 116 115 105 114 109 98 110 97 32 105 110 105 108 97 110 105 109 116 107 97 32 101 32 115 101 106 97 121 114

Membentuk *array* sesuai dengan arah dari proses enkripsi. Kunci yang digunakan 7 sehingga pembentukan *array* enkripsi juga 7x7 sebagai berikut:

Tabel 6. Pembentukan *Array* Dekripsi I

83	112	117	32	97	109	98
101	108	117	109	32	101	32
97	108	103	107	32	109	101
116	115	105	114	109	98	110
97	32	105	110	105	108	97
110	105	116	107	97	32	101
32	115	101	106	97	121	114



83	115	116	101	109	32	107
112	105	97	107	116	105	103
117	114	32	121	97	110	108
32	109	101	114	106	97	97
97	98	32	115	101	108	32
109	110	32	105	110	105	101
98	101	108	103	107	109	32

Kemudian didapatkan *plaintext* sebagai berikut:
83 115 116 101 109 32 107 112 105 97 107 116 105 103 117 114 32 121 97 110 108 32 109 101 114 106 97 97 97 98 32 115 101 108 32 109 110 32 105 110 105 101 98 101 108 103 107 109 32.
Jika dikonversi ke dalam karakter menjadi:
Sistem praktikum yang berjalan selama ini belum e
Ciphertext II : Fdslb a si jadmnmaife naiaerikm n
Desimal : 102 100 115 108 98 32 97 115 105 32 106 97 100 109 110 109 97 105 32 102 105 116 107 101 97 105 97 101 105 110 102 111 114 97 101 100 102 101 32 110 101 109 114 105 107 109 32 110 32.

Membentuk *array* sesuai dengan arah dari proses enkripsi. Kunci yang digunakan 7 sehingga pembentukan *array* enkripsi juga 7x7 sebagai berikut:

Tabel 7. Pembentukan *Array* Dekripsi II

102	100	115	108	98	32	97
115	105	32	106	97	100	109
110	109	97	105	32	102	105
116	107	101	97	105	97	101
105	110	102	111	114	97	101
100	102	101	32	110	101	109
114	105	107	109	32	110	32

102	101	107	116	105	102	32
100	97	110	32	101	102	105
115	105	101	110	32	100	97
108	97	109	32	109	101	109
98	101	114	105	107	97	110
32	105	110	102	111	114	109
97	115	105	32	106	97	100

Kemudian didapatkan *plaintext* sebagai berikut:
83 115 116 101 109 32 107 112 105 97 107 116 105 103 117 114 32 121 97 110 108 32 109 101 114 106 97 97 97 98 32 115 101 108 32 109 110 32 105 110 105 101 98 101 108 103 107 109 32.

Jika dikonversi ke dalam karakter menjadi:
fektif dan efisien dalam memberikan informasi jad.
Proses tersebut dilakukan terhadap seluruh *ciphertext* sehingga didapatkan *plaintext* sebagai berikut:

Plaintext = Sistem praktikum yang berjalan selama ini belum efektif dan efisien dalam memberikan informasi jadwal, nilai praktikum, karena masih selembaran kertas yang di tempelkan di madding kampus dan juga pengumpulan laporan yang di catat di buku laporan secara manual.

4. KESIMPULAN

Berikut merupakan kesimpulan dari penelitian yang penulis lakukan.

1. Prosedur pengamanan *file Portabel Document Format* adalah dengan menghitung nilai-nilai dari karakter isi *file* dengan menggunakan kunci yang menghasilkan *cipherteks* yang didapat berdasarkan algoritma yang digunakan.
2. Algoritma *route cipher* melakukan enkripsi terhadap *file* dengan menggunakan kunci yang dapat membentuk matriks, kemudian menentukan arah enkripsi berdasarkan persetujuan antara penerima dan pengirim. Apabila arah yang ditentukan adalah *spiral*, maka *ciphertext* yang didapatkan adalah karakter yang sudah ditransposisi dengan arah *spiral*.
3. Perancangan aplikasi pengamanan *file* PDF dapat dilakukan dengan alat bantu perancangan *Unified Modelling Language* dan *tools* pemrograman *Visual Studio* 2008.

REFERENCES

[1] E. Setyaningsih, Kriptografi & Implementasinya Menggunakan Matlab, Yogyakarta: Penerbit Andi. 2015
[2] L.Sitorus, Algoritma dan Pemrograman, Yogyakarta: Penerbit Andi. 2015
[3] R.Stephens, Essential Algorithms A Practical Approach to Computer Algoritms, Canada: John Wiley & Sons.Inc. 2013
[4] A.Aneta, "Implementasi Kebijakan Program Penanggulangan Kemiskinan Perkotaan (P2KP) di Kota Gorontalo", Jurnal Administrasi Publik, vol.I, pp. 54-65. 2010
[5] H.Christian, "Studi tentang Pelaksanaan Rencana Kerja Pembangunan Desa Tahun 2013 di Desa Loa Janan Ulu Kecamatan Loa Janan Kabupaten Kutai Kartanegara", eJournal Pemerintahan Integratif, vol.III, pp. 190-210. 2015
[6] Z.Amin, "Desain dan Implementasi Tunneling IPSEC Berbasis UNIX dengan [1] [1] [2]ESP (Encapsulating Security Payload)", STMIK PalComTech, vol.II, pp109-119. 2012.