ALGORITMA MD5 DAN RC5 UNTUK PENGAMANAN FILE PDF

Manuel Luis Belo [1], Derwin R. Sina [2], Yelly Y. Nabuasa [3].
[1,2,3] Program Studi Ilmu Komputer, Fakultas Sains Dan Teknik Universitas Nusa Cendana
Email : [1]nuelbelo7@gmail.com, [2]derwinsina@staf.undana.ac.id, [3]yelly.yosiana.n@gmail.com

ABSTRAK

Dokumen elektronik adalah jenis berkas digital yang digunakan untuk menyimpan data atau informasi penting seseorang atau suatu lembaga. Terdapat beberapa format file dokumen yang paling banyak digunakan yaitu .docx, .xlsx, .pptx, dan .pdf. Masalah yang muncul ketika suatu perusahaan, institusi atau organisasi yang mempunyai dokumen-dokumen rahasia dan data-data yang penting berupa file dokumen bisa diakses oleh orang atau pihak yang tidak memiliki wewenang. Solusi pengamanan dokumen dapat menggunakan konsep kriptografi. Jenis file dokumen yang dapat dienkripsi dibatasi pada file Portable Document Format (.pdf). Pada penelitian ini dilakukan pengamanan kunci inputan user menggunakan algoritma Message Digest 5 (MD5) dan pengacakan nilai binary pada file pdf menggunakan algoritma Rivest Code (RC5). Hasil pengujian menggunakan (i) kunci yang sama pada file pdf yang berbeda menunjukkan bahwa binary chiperfile yang dihasilkan berbeda dengan binary plainfile yang diambil.Hal ini diketahui dari tingkat kesamaan binary chiperfile dan binary plainfile yang kecil/rendah berdasar pada nilai kolerasi yang dihasilkan tiap pengujian adalah (i) 0,205795252, (ii) 0,24692765, (iii) 0,22421886.
Kata Kunci: Kriptografi, Message Digest 5, Rivest Code 5, PDF

ABSTRACT

Electronic documents are digital file types used to store the important data or information of a person or an institution. There are some of the most widely used document file formats that are. docx,. xlsx,. pptx, and. pdf. Issues that arise when a company, institution or organization that has confidential documents and important data in the form of document files can be accessed by persons or parties who have no authority. A document security solution can use cryptographic onsep. The document file types that can be encrypted are restricted to the Portable Document Format (. pdf) file. In this research is done lock security user input using the algorithm Message Digest 5 (MD5) and binary value multiplier in PDF files using Rivest Code algorithm (RC5). The test results using (i) the same key on a different PDF file indicate that the resulting binary chiperfile is different from the derived binary Plainfile, (ii) the key length of 1 to 8 characters on the same PDF file indicates that binary The chiperfile generated each key length differs from the binary plainfile taken, (iii) a change of 1 character at the beginning, in the middle, and at the end of the input key indicates that the method used is sensitive to the character changes on the key Input. It is known from the level of similarity of binary chiperfile and small/low binary plainfile based on the value of the collation generated per test is (i) 0.205795252, (ii) 0.24692765, (iii) 0.22421886.
Keyword: Cryptography, Message Digest 5, Rivest Code 5, PDF

I PENDAHULUAN

Kehidupan modern saat ini sangat membutuhkan sesuatu yang namanya informasi. Informasi yang banyak digunakan saat ini yaitu informasi digital. Informasi digital adalah jenis informasi yang menggunakan teknologi sebagai media-nya. Media yang banyak digunakan yaitu dokumen elektronik. Terdapat beberapa format file dokumen yang paling banyak digunakan yaitu .docx, .xlsx, .pptx, dan .pdf.

Masalah yang muncul ketika suatu perusahaan, institusi atau organisasi yang mempunyai dokumen-dokumen rahasia dan data-data yang penting berupa file dokumen bisa diakses oleh orang atau pihak yang tidak memiliki wewenang. Hal ini menyebabkan file yang awalnya bersifat rahasia menjadi tidak rahasia lagi. Oleh sebab itu, perlu menjaga keamanan dari dokumen-dokumen tersebut agar terhindar dari gangguan orang lain. Salah satu cara untuk mengamankan data file dokumen dari tindak kejahatan tersebut adalah menggunakan konsep kriptografi [3]. Sebelumnya, telah ada penelitian mengenai implementasi kriptografi enkripsi file dokumen yaitu hybrid cryptosystem untuk pengamanan e-dokumen menggunakan algoritma RC4, RSA dan MD5 [1].

Berdasar pada penelitian di atas, penulis ingin melakukan penelitian tentang mengamankan file pdf dengan mengacak 16 struktur binary file saja. Pengamanan akan dilakukan dengan mengacak 16 struktur binary dari file PDF. Pengamanan struktur file pdf yang akan diteliti menggunakan algoritma Message Digest 5 (MD5) dan Rivest Code 5 (RC5).

II MATERI DAN METODE

2.1 Dokumen

Dokumen merupakan salah satu hal yang sangat penting karena merupakan sumber informasi yang diperlukan oleh suatu instansi, organisasi, atau negara. Dokumen adalah surat penting atau berharga yang sifatnya tertulis atau tercetak yang berfungsi atau dapat dipakai sebagai bukti ataupun keterangan [1].

2.2 Kriptografi

Kriptografi merupakan ilmu yang mempelajari mengenai cara untuk menyandikan pesan yang berguna untuk membuat pesan, data maupun informasi tidak dapat dibaca atau dimengerti oleh orang lain, kecuali untuk penerima yang berhak mengetahui.

Dalam Kriptografi, Pesan atau informasi yang dapat dibaca disebut sebagai plaintext. Plaintext dinyatakan dengan M (message) atau P (plaintext). Pesan dapat berupa aliran bit, file teks, bitmap, aliran suara yang digitasi, Gambar video digital dan sebagainya.

2.3 *Messasge Digest* 5

Message Digest 5 (MD5) adalah salah satu dari serangkaian algoritma Message Digest yang didesain oleh Professor Ronald Rivest dari MIT. MD5 banyak digunakan pada bermacam-macam aplikasi termasuk SSL/TLS, IPSec dan protokol-protokol kriptografi lainnya. MD5 juga biasa digunakan pada implementasi Timestamping Mechanism, Commitment Schemes, dan aplikasi pengecekan integritas pada online software. MD5 tidak memiliki sistim pengamanan seperti persamaan matematika, namun untuk setiap fungsi hash h, domain D dan range R membutuhkan tiga hal.

1. Pre Image Resistance: jika diberi suatu nilai y ε R, maka kita tidak akan dapat mencari suatu nilai x ε D dimana h(x) = y.
2. Second Pre Image Resistance: jika diberi suatu nilai x ε D, maka kita tidak akan dapat mencari nilai x' ε D dimana h(x) = h(x').
3. Collision Resistance: kita tidak akan dapat mencari nilai x, x' ε D dimana h(x) = h(x').

2.4 *Rivest Code* 5

Algoritma enkripsi Rivest Code 5 (RC5) didesain oleh Profesor Ronald Rivest dan pertama kali dipublikasikan pada Desember 1994. Sejak publikasinya, RC5 telah menarik perhatian banyak peneliti dalambidang kriptografi dalam rangka menguji tingkat keamanan yang ditawarkan oleh algoritma RC5 (RSA Laboratory Technical Report TR-602).

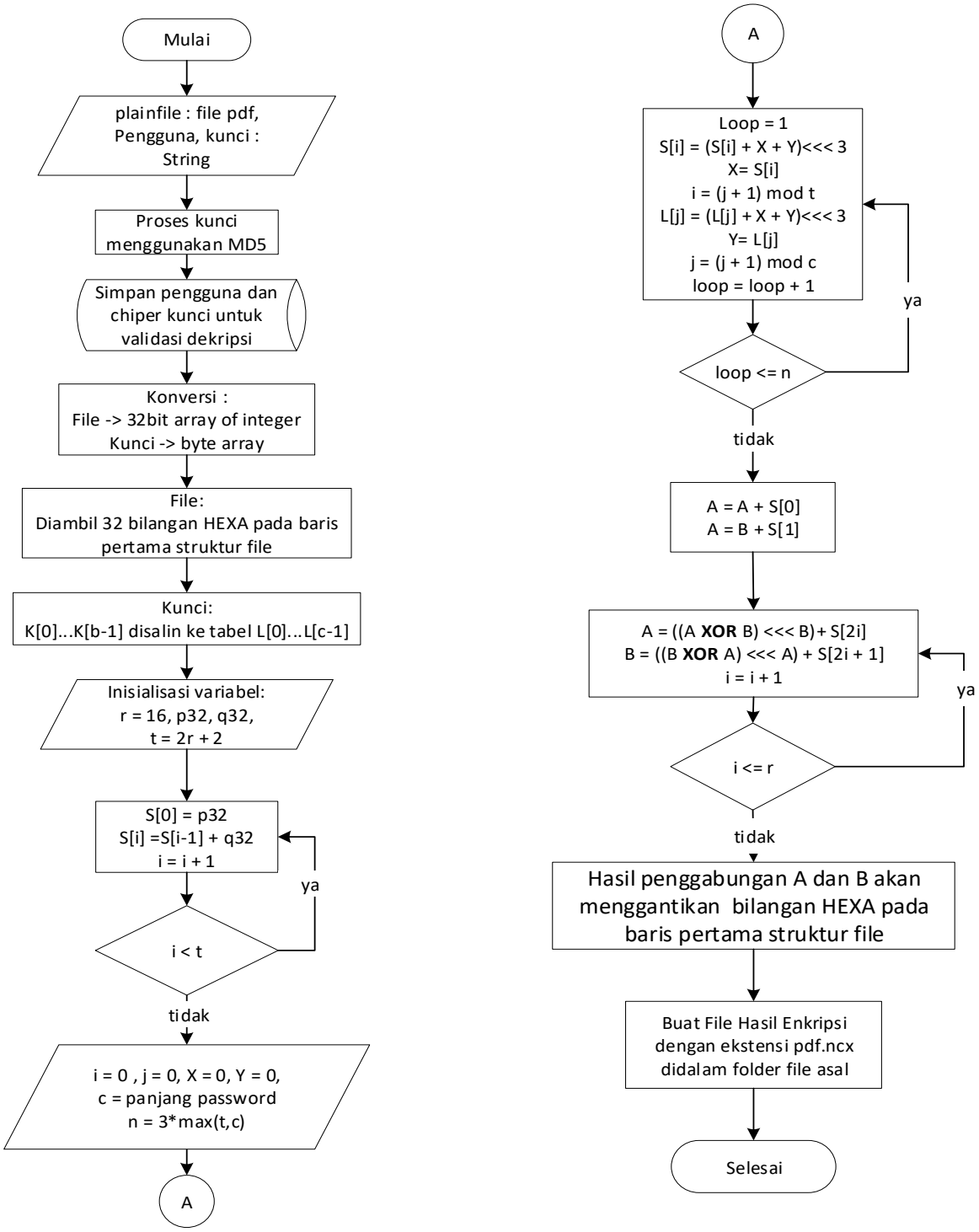
Algoritma RC5 merupakan metode enkripsi menggunakan metode simetrik dan pengolahan dalam bentuk blok chiper, jadi kata kunci yang sama digunakan untuk proses enkripsi dan dekripsi. Parameter-parameter yang digunakan dalam RC5 adalah sebagai berikut:

1. Round atau jumlah putaran disimbolkan dengan r yang memiki nilai antara 1, 2, 3, 4, ..., 225.
2. Jumlah word dalam bit disimbolkan dengan w. Jumlah yang disupport adalah 16 bit, 32 bit, dan 64 bit.
3. Kata kunci (key word) disimbolkan dengan b dengan range 1, 2, 3, 4, ..., 225. Ada 3 proses utama dalam RC5, yaitu perluasan kunci, enkripsi dan dekripsi. Perluasan kunci merupakan proses membangkitkan kunci internal dengan memanfaatkan komputasi rotasi left regular shift (<<<) dan right regular shift (>>>), dengan panjang kunci tergantung dari jumlah putaran. Kunci internal kemudian digunakan dalam proses enkripsi dan dekripsi.

2.5 Gambaran Umum

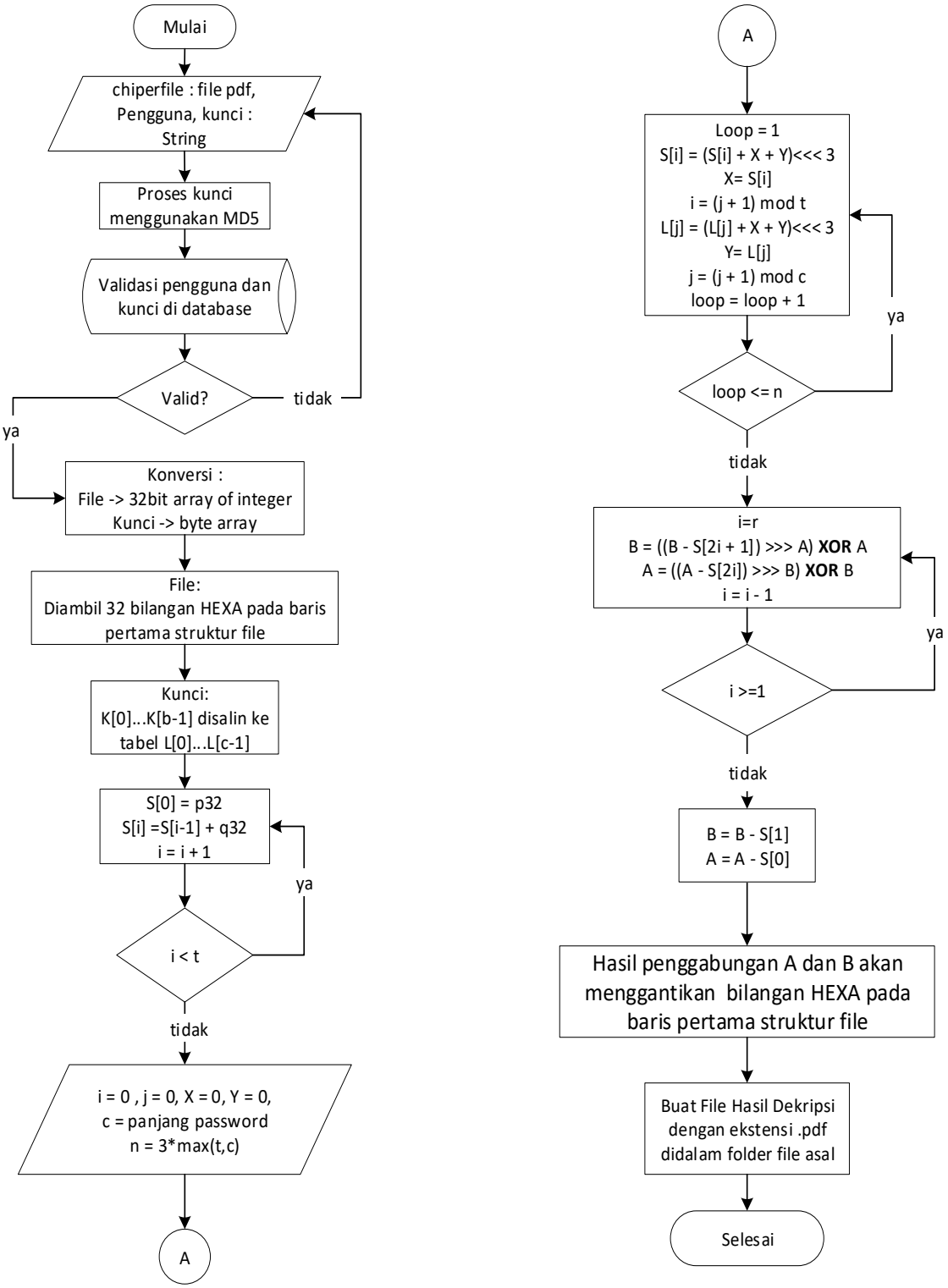
Gambaran umum alur sistem disajikan dalam bentuk flowchart ditunjukkan pada gambar 1 dan 2 dijelaskan mengenai perancangan dari sistem yang diusulkan yaitu pengamanan file pdf menggunakam algoritma MD5 dan RC5 dengan menggunakan *flowchart* urutan proses dalam sistem enkripsi dan dekripsi file pdf.

Flowchart urutan proses dalam sistem enkripsi *file* pdf dapat dilihat pada Gambar 1.



Gambar 1. *Flowchart* enkripsi *file* pdf

Flowchart urutan proses dalam sistem dekripsi *file* pdf dapat dilihat pada Gambar 2



Gambar 2. *Flowchart* dekripsi *file* pdf

III HASIL DAN PEMBAHASAN

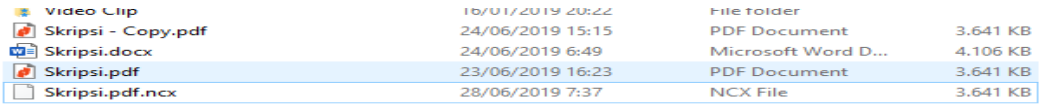
3.1 Hasil Pengujian

Pengujian sistem dilakukan untuk mengetahui performa dari sistem yang dibangun. Pengujian terdiri dari pengujian aplikasi dan perbandingan korelasi koefisien antara *plainfile* dan *cipherfile*.

a. Pengujian Aplikasi

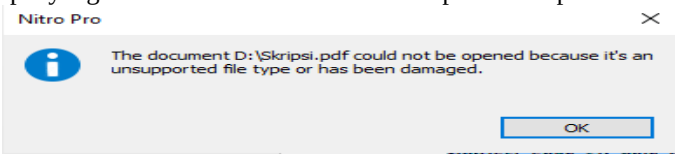
Pengujian pada aplikasi pengamanan data pada file pdf difokuskan pada kemampuan aplikasi dalam melakukan pengamanan data. Hal ini difokuskan pada file yang telah dienkripsi dibandingkan dengan file

asli dan kemampuan aplikasi dalam mengembalikan file yang telah dienkripsi ke bentuk semula. File pdf yang dienkripsikan akan mendapatkan ekstensi baru yaitu *.ncx. File terenkripsi akan disimpan pada lokasi yang sama dengan file asli dan dinamai dengan nama yang sama dengan file asli ditambah dengan ekstensi file asli. Semisal file asli adalah "D:\Skripsi.pdf" maka file terenkripsi akan disimpan sebagai "D:\Skripsi.pdf.ncx". Hal tersebut dapat ditunjukkan pada Gambar 3.



Gambar 3. Perbandingan antara file asli dan terenkripsi

Proses pengamanan file pdf tidak hanya mengubah ekstensi file sehingga file tidak dapat dibuka, namun aplikasi pengaman data melakukan enkripsi pada *binary* data pada file tersebut sehingga struktur dari file akan berubah dan tidak dapat dibuka meskipun dilakukan pengembalian ekstensi secara manual. Contoh hasil file terenkripsi yang dikembalikan secara manual dapat dilihat pada Gambar 4.



Gambar 4. *Error* saat buka file pdf yang dikembalikan secara manual

Untuk mengembalikan file pdf kedalam bentuk semula, diperlukan proses dekripsi yang merupakan kebalikan dari proses enkripsi, dimana proses tersebut akan mengembalikan nilai dan struktur *binary* data pada file pdf kedalam bentuk semula.

b. Perhitungan Korelasi Koefisien

Perhitungan korelasi koefisien merupakan sebuah perhitungan untuk mencari derajat korelasi di antara dua variabel. Jika nilai korelasi mendekati 0 maka *binary cipherfile* yang dihasilkan benar-benar teracak (sangat berbeda dengan *binary plainfile* yang diambil), namun jika mendekati 1 maka *binary cipherfile* yang dihasilkan tidak begitu teracak (masih memiliki hubungan linear dengan *binary plainfile* yang diambil).

Perhitungan korelasi koefisien yang dilakukan pertama adalah perbandingan nilai korelasi koefisien antara *binary plainfile* yang diambil dan *chiperfile* yang dihasilkan pada 5 file pdf berbeda menggunakan kunci yang sama dapat dilihat pada Tabel 1.

Tabel 1 Korelasi *binary* menggunakan kunci yang sama

No.	*Plainfile*	Kunci	*Binary Plainfile* Yang Diambil	*Binary Chiperfile* Yang Dihasilkan	Korelasi
1	FILE1.pdf	NUEL	%PDF-1-.5..%.....	.2)t../"…..5.( )	0,115488997
2	FILE2.pdf	NUEL	%PDF-1-.7..%.....	.2)t.r.O"…….	0,040318418
3	FILE3.pdf	NUEL	%PDF-1-.7…….	G..C…A….J…	0,023821865
4	FILE4.pdf	NUEL	%PDF-1.6.%.....1	…ky9..7.6)d-.M	0,46861155
5	FILE5.pdf	NUEL	%PDF-1.3.%.....	…OP,X.(….I..	0,380735428
TOTAL					1,028976258
RATA-RATA					**0,205795252**

Pada Tabel 1 menunjukkan bahwa nilai rata-rata korelasi antara *binary plainfile* yang diambil dan *binary cipherfile* yang dihasilkan termasuk kategori rendah yaitu 0,205795252. Hal ini menunjukkan bahwa *binary cipher* tersebut menghasilkan *binary cipherfile* yang acak.

Perhitungan korelasi koefisien yang dilakukan kedua adalah perbandingan kolerasi koefisien *binary plainfile* yang diambil dan *binary chiperfile* yang dihasilkan pada file pdf yang sama dengan variasi panjang kunci 1 sampai 8 karakter. Hasil perhitungan nilai korelasi antara *binary plainfile* yang diambil dan *binary cipherfile* yang dihasilkan pada file pdf yang sama menggunakan variasi panjang kunci 1 sampai 8 karakter dapat dilihat pada Tabel 2.

Pada Tabel 2 menunjukkan bahwa nilai rata-rata korelasi antara *binary plainfile* yang diambil dan *binary cipherfile* yang dihasilkan termasuk kategori rendah yaitu 0, 24692765. Hal ini menunjukkan bahwa *binary cipher* tersebut menghasilkan *binary cipherfile* yang acak.

Tabel 2 Korelasi *binary* berdasarkan panjang kunci

No	*Plainfile*	Kunci	*Binary Plainfile* Yang Diambil	*Binary Chiperfile* Yang Dihasilkan	Korelasi
1	FILE1.pdf	N	%PDF-1-.5..%.....	….g…v.o….E	0,195441501
2	FILE1.pdf	NU	%PDF-1-.5..%.....	‘<`.D.n.1N.s…=	0,316467722
3	FILE1.pdf	NUE	%PDF-1-.5..%.....	xXs…Q2%..I>IK.	0,015160866
4	FILE1.pdf	NUEL	%PDF-1-.5..%.....	.2)T../”…..5.( )	0,115488997
5	FILE1.pdf	NUELB	%PDF-1-.5..%.....	|.q…….7IV…	0,388159377
6	FILE1.pdf	NUELBE	%PDF-1-.5..%.....	.E.).C(..U..(.2.	0,39840967
7	FILE1.pdf	NUELBEL	%PDF-1-.5..%.....	….YUC~.(..”Om.	0,207790283
8	FILE1.pdf	NUELBELO	%PDF-1-.5..%.....	2…m….1…m.L	0,35284226
TOTAL					1,97542122
RATA-RATA					**0,24692765**

c. Pengujian Sensitivitas Kunci

Pengujian sensitivitas kunci bertujuan untuk mengetahui sensitivitas kunci yang diperoleh dari korelasi antara 2 *cipherfile* hasil enkripsi dengan kunci yang berbeda pada 1 karakternya, jika hasilnya mendekati 0 maka sensitivitas kunci sangat baik, namun jika mendekati 1 maka kunci tidak sensitif. Pengujian dilakukan pada 5 file pdf yang telah di enkripsi dengan kunci asli dan dengan perubahan 1 karakter pada kunci Setelah dilakukan 3 kali percobaan lalu dicari nilai rata-ratanya untuk menentukan sensitivitas kunci. Hasil pengujian ini dapat dilihat pada Tabel 3.

Tabel 3 Pengujian sensitivitas dengan perubahan 1 karakter pada kunci

No.	Kunci	*Plainfile*	*Binary Chiperfile* Kunci “NUELBELO”	*Binary Chiperfile* Perubahan 1 Karakter Kunci	Korelasi
1	**M**UELBELO	FILE1.pdf	2…m….1…m.L	/....h[....I/G`.	0,34398279
		FILE2.pdf	2...0.j..1..b.Y.	/.....l....I..d;	0,56353244
		FILE3.pdf	}..N<spasi>x5...`p...:	:J.E.s....1.;.H.	0,10160593
		FILE4.pdf	....b,@..#>U..nm	q*#,....":....3.	0,39376093
		FILE5.pdf	$..evH.....	.....`...i.../.G	0,09454627
Rata-rata					**0,29948567**
2	NUEL**A**ELO	FILE1.pdf	2…m….1…m.L	.j..Il.&./.O~.S.	0,27239524
		FILE2.pdf	2...0.j..1..b.Y.	.j..Iy!../.O....	0,27078199
		FILE3.pdf	}..N<spasi>x5...`p...:	.z..{.b..9..Q...	0,41533555
		FILE4.pdf	....b,@..#>U..nm	..a'..=.}.....	0,02500331
		FILE5.pdf	$..evH.....	.a.v....r..ET...	0,10120856
Rata-rata					**0,21694493**
3	NUELBEL**N**	FILE1.pdf	2…m….1…m.L	P...H.....&Oc.*	0,11250439
		FILE2.pdf	2...0.j..1..b.Y.	P...H.s....&P...	0,09260749
		FILE3.pdf	}..N<spasi>x5...`p...:	.]2.g...n....W.H	0,31957203
		FILE4.pdf	....b,@..#>U..nm	9....3...Y....2.	0,03225044
		FILE5.pdf	$..evH.....	.c.T.....2	0,22419549
Rata-rata					**0,15622597**
Rata-rata keseluruhan					**0,22421886**

Pada Tabel 3 menunjukkan bahwa rata-rata keseluruhan dari korelasi antara *binary cipherfile1* (hasil enkripsi dengan kunci awal tanpa perubahan karakter) dan *binary cipherfile2* (hasil enkripsi dengan kunci awal yang telah diubah 1 karakternya) yang dihasilkan termasuk kategori rendah yaitu 0, 22421886. Dari rata-rata koefisien di atas menujukkan bahwa metode yang digunakan sensitif pada perubahan 1 karakter pada kunci karena kunci yang diinput tidak langsung digunakan tetapi masih dicampurkan dengan kunci internal S[] yang dibentuk dari konstanta P dan Q yang hasilnya digunakan untuk enkripsi maupun dekripsi.

3.2 Pembahasan

Dari hasil pengujian enkripsi dan dekripsi yang telah dilakukan**,** diketahui bahwa algoritma MD5 dan RC5 yang digunakan pada aplikasi yang dibangun dapat mengenkripsikan *plainfile* dan mendekripsikan *chiperfile* dengan baik.

Pada pengujian aplikasi yang dilakukan dengan membuka file pdf yang terenkripsi dengan mengubah ekstensi file secara manual. Hal ini dikarenakan struktur *binary* dari file pdf tersebut yang diacak dan disimpan dengan tambahan ekstensi *.ncx. Jadi, ketika ingin membuka file pdf yang terenkripsi, *user* harus mengdekripsi terlebih dahulu file pdf yang terenkripsi dengan aplikasi yang ada.

Pada pengujian perbandingan korelasi koefisien mengunakan kunci yang sama pada 5 file pdf berbeda, diketahui bahwa *binary chiperfile* yang dihasilkan berbeda. Rata-rata koefisien keseluruhan yang dihasilkan termasuk kategori rendah yaitu 0,205795252. Hasil dari pengujian ini diketahui bahwa struktur *binary plainfile* yang diambil pada masing-masing file pdf berbeda maka penggunaan kunci yang sama tidak akan menghasilkan *binary chiperfile* yang sama pada 5 file pdf tersebut.

Pada pengujian perbandingan korelasi koefisien penggunaan panjang kunci 1 sampai 8 karakter pada 1 file pdf yang sama, diketahui bahwa *binary chiperfile* yang dihasilkan berbeda. Rata-rata koefisien keseluruhan yang dihasilkan termasuk kategori rendah yaitu 0,24692765. Hasil dari pengujian ini diketahui bahwa panjang kunci tidak terlalu berpengaruh pada keamanan file yang dienkripsi.

Pada pengujian sensitivitas kunci, diketahui bahwa metode yang digunakan sensitif pada perubahan 1 karakter pada kunci. Hasil ini didapat dari rata-rata korelasi pada pengujian sensitivitas kunci(Tabel 3.3) yang menunjukkan bahwa tingkat kesamaan data rendah/kecil yaitu 0,22421886.

IV PENUTUP

4.1 Kesimpulan

Pada pengujian sistem, disimpulkan bahwa sistem dapat melakukan proses enkripsi dan dekripsi file pdf dengan baik dan praktis penggunaannya.

Pada pengujian aplikasi yang dilakukan dengan membuka file pdf yang terenkripsi dengan mengubah ekstensi file secara manual, disimpulkan bahwa *user* harus mendekripsi terlebih dahulu file pdf yang terenkripsi dengan aplikasi yang ada bila ingin membuka file pdf yang terenkripsi.

Pada pengujian perbandingan korelasi koefisien penggunaan kunci yang sama pada file pdf yang berbeda, disimpulkan bahwa penggunaan kunci yang sama tidak akan berpengaruh pada keamanan file pdf yang dienkripsi. Hal ini dikarenakan struktur *binary* setiap file berbeda dan rata-rata korelasi yang dihasilkan termasuk kategori rendah yaitu 0,205795252.

Pada pengujian perbandingan korelasi koefisien penggunaan panjang kunci 1 sampai 8 karakter pada file pdf yang sama, disimpulkan bahwa panjang kunci tidak terlalu berpengaruh pada keamanan file yang dienkripsi. Hal ini dikarenakan rata-rata koefisien yang dihasilkan termasuk kategori rendah yaitu 0,24692765.

Pada pengujian sensitivitas kunci dengan merubah 1 karakter pada kunci disimpulkan atau didapati bahwa metode yang digunakan sensitif pada perubahan 1 karakter pada kunci. Hasil ini didapat dari rata-rata korelasi pada pengujian sensitivitas kunci yang menunjukkan bahwa tingkat kesamaan data rendah/kecil yaitu 0,22421886.

4.2 Saran

Berdasarkan pembahasan sebelumnya, maka saran untuk pengembangan penelitian selanjutnya adalah:

1. Perbaikan pada file input dan output yang diproses tidak hanya berformat pdf saja namun dapat dikembangkan untuk format lain juga.
2. Perbaikan pada aplikasi yang masih berbasis offline menjadi online.
3. Pengujiaan korelasi ketika panjang kunci inputan(c) > banyaknya kunci internal S[] awal yang dibentuk(t).
4. Pencarian kunci terbaik dari 1 sampai banyaknya kunci internal S[] awal yang dibentuk(t).

DAFTAR PUSTAKA

[1] Alyas, R. 2014. “Hybrid Cryptosystem Untuk Pengamanan E-Dokumen Menggunakan Algoritma RC4, RSA Dan MD5”.

[2] Fanggidae A, Polly Y. T. 2015. “Analisis Pembangkit Kunci Dengan Tent Map, Session Key Dan Linear Congruential Generator Pada Cipher Aliran

[3] Munir, R. 2006, Kriptografi, Informatika, Bandung.

[4] Munir, R. 2012, Analisis Keamanan Algoritma Enkripsi Citra Digital menggunakan Kombinasi Dua Chaos Map dan Penerapan Teknik Selektif, Bandung, http://informatika.stei.itb.ac.id/~rinaldi.munir/Penelitian/Makalah_JUTI_ITS_2012.pdf diakses tanggal 20 Maret 2019.

[5] Rivest, R.L. 1997. The RC5 Encryption Algorithm*. Cambridge : MIT Laboratory for Computer Science 545 Technology Square
[6] Sugiono, 2007, Metode Penelitian Administrasi, Alfabeta, Bandung.-