Journal of Computer System and Informatics (JoSYC)
Volume 1, No. 4, Agustus 2020, Page 337-345
ISSN 2714-8912 (media online)
ISSN 2714-7150 (media cetak)

Kombinasi Algoritma Cipher Block Chaining (CBC) dan Mars Pada Penyandian File PDF

Ridha Ismadiah, Muhammad Syahrizal, Putri Ramadhani

Program Studi Teknik Informatika, STMIK Budi Darma, Medan, Indonesia
Email: ridha@gmail.com
Submitted: **28/06/2020**; Accepted: **21/08/2020**; Published: **21/08/2020**

Abstrak−Pada lingkungan kompetitif sekarang ini memungkinkan manusia dapat berkomunikasi dan dapat bertukar informasi data atau pun file secara jarak jauh. Oleh sebab itu perlu dilakukan perlindungan terhadap informasi. Salah satu cara yang dapat dilakukan adalah dengan melakukan pertukaran informasi dalam bentuk file Portable Document Format (PDF). Perkembangan ilmu pengetahuan yang sangat pesat saat ini menyebabkan informasi menjadi hal yang sangat berharga, oleh sebab itu perlu dilakukan perlindungan terhadap informasi. Dalam penelitian ini menggabungkan dua buah algoritma antara algoritma yaitu algoritma Cipher Block Chaining (CBC) dan Mars. Untuk membangun aplikasi yang terkomputerisasi ini dengan menggunakan Visual Basic 2008 sebagai aplikasi pendukung nya. Aplikasi ini dibuat untuk implementasi enkripsi dan deskripsi file teks sebagai komunikasi yang aman.

Kata Kunci: File PDF, Kriptografi, CBC, Mars.

Abstract−In today's competitive environment allows humans to communicate and can exchange data information or files remotely. Therefore it is necessary to protect information. One way that can be done is to exchange information in the form of Portable Document Format (PDF) files. The development of science that is very fast now causes information to be very valuable, therefore protection of information is needed. In this study combining two algorithms between algorithms namely Cipher Block Chaining (CBC) and Mars algorithms. To build this computerized application using Visual Basic 2008 as its supporting application. This application is made for the implementation of encryption and description of text files as secure communication.

Keywords: PDF Files, Cryptography, CBC, Mars

1. PENDAHULUAN

Teknik kriptografi merupakan salah satu teknik pengamanan data dengan melakukan proses penyandian terhadap data yang ingin diamankan sehingga makna asli dari data tidak lagi dapat dimengerti. Kriptografi merupakan salah satu teknik yang dapat digunakan dalam menjaga dan mengamankan informasi yang sangat penting untuk dijaga agar informasi tersebut tetap utuh dan terjamin pada saat di distribusikan dari suatu tempat ke tempat lain[1].

Perkembangan teknologi komputerisasi saat ini sudah sangat meningkat bagi pengguna komputer. Semakin tinggi teknologi komputer semakin tinggi tingkat ancaman keamanan bagi pengguna komputer. Pengguna perlu untuk menyimpan data berupa file text yang berisi informasi. Salah satunya adalah file PDF atau *(Portable Document Format)* adalah sebuah format file yang diciptakan oleh *Adobe System*. File jenis ini sangat populer dan banyak digunakan terutama dalam bentuk *ebook* karena dapat dengan mudah dibuka menggunakan berbagai aplikasi gratis. Jika dibandingkan dengan format dokumen lain seperi MS Word, PDF tentu lebih aman dan dapat didistribusikan atau dibuka di PC manapun dengan tampilan yang sama asalkan sudah terinstall *software* PDF *reader.*

Walaupun melalui data digital disebut sebagai sarana yang paling aman untuk saling menyimpan informasi. Namun nyatanya tidak demikian, banyak sekali orang yang memiliki kemampuan untuk menyusup ke dalam jaringan informasi yang menyebabkan informasi dapat dibaca, diambil, atau bahkan diubah dan dipublikasikan. Informasi yang dimiliki oleh pemilik bisa dirugikan apabila ada kegiatan mengambil bahkan membaca isi informasi yang ada tanpa seijin pihak yang bersangkutan. Hal seperti itulah yang menjadi ancaman yang perlu dilindungi karena dapat merugikan pihak yang bersangkutan.

Berdasarkan penelitian sebelumnya yang dilakukan oleh R.Kurniawan, Jurnal Ilmu Komputer dan Informasi, tahun 2017, volume 01, no 1, November, menyatakan bahwa keamanan dokumen merupakan salah satu hal yang sangat penting dalam penukaran data, khusunya pertukaran data didunia maya yang di dalamnya terdapat banyak ancaman pada saat proses itu dilakukan. Keamanan data, khususnya untuk dokumen atau file teks bagi suatu organisasi yang mengasumsikan bahwa dokumen tersebut bernilai rahasia (*private and confidential)*. Salah satu aspek keamanan dalam dokumen teks adalah keaslian, bentuk dan isinya harus sesuai dengan yang dimaksud oleh pembuat. Hingga saat ini sistem kriptografi merupakan salah satu solusi untuk menjamin keutuhan dan keamanan dari suatu data yaitu dengan menyandikan isi atau *content file* dokumen tersebut menjadi isi yang sulit bahkan tidak dapat dipahami melalui proses enkripsi dan untuk memperoleh kembali informasi yang asli dilakukan[2].

A.M Hara Pardede Jurnal Jurnal Teknik Informatika Kaputama (JTIK), tahun 2017, volume 1, no1 ,Januari. Juga menyatakan dalam penelitiannya, bahwa dalam sistem keamanan data dikenal sebuah metode enkripsi yang mempunyai kode-kode pengamanan untuk mengacak data dan juga mempunyai kode-kode dan kunci yang akan di gunakan untuk mengembalikan data yang teracak dan tidak beraturan ke dalam bentuk data yang sebenarnya.

Journal of Computer System and Informatics (JoSYC)
Volume 1, No. 4, Agustus 2020, Page 337-345
ISSN 2714-8912 (media online)
ISSN 2714-7150 (media cetak)

Enkripsi bisa diartikan dengan *chiper* atau kode, dimana pesan asli (*plaintext*) diubah menjadi kode-kode tersendiri sesuai metode yang disepakati oleh kedua belah pihak, baik pihak pengirim pesan maupun penerima pesan[3].

Salah satu metode kriptografi yang dapat digunakan untuk mengkombinasikan pengamanan data file adalah algoritma C*ipher Block Chaining* dan *Mars.* dimana algoritma ini dapat menyelesaikan proses enkripsi dan dekripsi dengan cepat. Konsep pengkombinasian dua algoritma menghasilkan algoritma yang sulit terpecahkan. Maka penulis mencoba menggabungkan konsep kriptografi modern berupa algoritma *Cipher Block Chaining* dan *Mars*.

2. METODOLOGI PENELITIAN

2.1 Kriptografi

Kriptografi (*cryptography*) berasal dari bahasa yunani, yaitu dari kata *cypto* dan *graphia* yang berarti penulisan rahasia. Kriptografi adalah ilmu ataupun seni yang mempelajari bagaimana membuat suatu pesan yang dikirim oleh pengirim dapat disampaikan kepada penerima dengan aman. Kriptografi juga merupakan studi terhadap teknik matematis yang terkait dengan aspek keamanan suatu sistem informasi seperti kerahasiaan, integritas data, autentikasi dan ketiadaan penyangkalan[4].

2.2 Algoritma CBC *(Cipher Block Chaining)*

Ada dua ide utama di balik *Cipher Blok Chaining* (CBC). Pertama, enkripsi semua blok adalah "dirantai bersama-sama". Kedua, enkripsi secara acak dengan menggunakan inisialisasi vektor. Mode ini menerapkan umpan-balik (*feedback*) pada sebuah blok, dalam hal ini hasil enkripsi blok sebelumnya diumpanbalikan ke dalam enkripsi blok yang *current*. Blok plainteks yang current di-XOR-kan terlebih dahulu dengan blok cipherteks hasil enkripsi sebelumnya, selanjutnya hasil peng-XORan masuk ke dalam fungsi enkripsi. Pada mode CBC, setiap blok cipherteks tidak hanya tergantung pada blok plainteks tetapi juga pada seluruh blok plainteks sebelumnya[8].

Enkripsi adalah proses dari penyandian pesan asli menjadi pesan yang tidak dapat diartikan seperti aslinya. Dekripsi adalah merubah pesan yang sudah disandikan menjadi pesan aslinya. Pesan asli biasanya disebut plaintext, sedangkan pesan yang sudah disandikan disebut ciphertext. Perhatikan kelemahan yang dimiliki metode ini yaitu kesalahan satu bit pada sebuah blok plaintext akan merambat pada blok ciphertext yang berkoresponden dan semua blok ciphertext berikutnya. Adapun cara kerja Enkripsi dan Dekripsi dari algoritma di atas adalah :

1. Secara matematis, enkripsi dengan mode CBC dinyatakan sebagai Ci = EK (Pi⊕Ci–1) dan dekripsi sebagai Pi = DK (Ci) ⊕ Ci–1,
2. Blok plaintext pertama menggunakan C0 sebagai vector awal (initialization vector atau IV).
3. Blok-blok plaintext yang identik di enkripsi menjadi blok-blok ciphertext yang berbeda hanya jika blok-blok plaintextnya sebelumnya berbeda.
4. Pada skema ini setiap block n-bit plaintext di XOR-kan dengan block n-bit ciphertext. Kecuali blok plaintext pertama di-XORkan dengan suatu konstanta awal atau initialization vector (IV), sebesar n-bit. Hasil dari proses XOR tersebut yang kemudian di enkripsi.
5. Untuk proses dekripsi, hasil dekripsi blok ciphertext di-XOR-kan dengan blok ciphertext sebelumnya untuk menghasilkan blok plaintext. Untuk blok pertama, hasil dekripsi blok ciphertext pertama di-XOR-kan dengan IV untuk menghasilkan blok plaintext pertama.[10].

2.3 Algoritma Mars

Multivariate Adaptive Regression Splines (MARS) merupakan metode dengan pendekatan regresi nonparametrik yang pertama kali diperkenalkan oleh Friedman pada tahun 1991. Model mars berguna untuk mengatasi permasalahan data berdimensi tinggi dan menghasilkan prediksi variabel respon yang akurat, dan menghasilkan model kontinue dalam knot berdasarkan nilai Generalized Cross Validation (GCV) terkecil. Meskipun algoritma MARS tidak terpilih sebagai algoritma AES, tetapi algoritma MARS dapat dijadikan sebagai salah satu allematif untuk enkripsi data dalarn berbagai aplikasi.

Permasalahan berdimensi tinggi adalah suatu permasalahan dengan jumlah variabel yang banyak serta ukuran sampel yang besar sehingga memerlukan perhitungan yang rumit. Data berdimensi tinggi yang dimaksud adalah data dengan ukuran $3 \leq v \leq 20$, dimana v adalah banyak variabel prediktor dan sampel data yang berukuran $50 \leq N \leq 1000$, dimana N untuk ukuran sampel (Friedman, 1991)[6]. Notasi yang digunakan dalam chiper adalah:

1. D[ ] adalah suatu array dari 4 32 bit data word. Array ini berisikan plaintext dan pada akhir proses enkripsi berisikan chipertext.
2. K[ ] adalah array untuk expended key, terdiri dari 40 32 bit.
3. S[ ] adalah array yang berisikan S-box, terdiri dari 512 bit word.

Perluasan kunci berfungsi untuk membangkitkan sub kunci dari kunci yang diberikan yakni K[ ] terdiri dari n 32 bit dan diperluas menjadi 64 bit sub kunci K[ ][11]. Tahapan yang dilakukan untuk membangkitkan sub kunci menggunakan modifikasi dari algoritma DES pada perluasan kunci adalah.

1. Konversi karakter kunci menjadi biner
2. Lakukan Permutation Commpresiton 1 (PC-1) terhadap biner kunci sesuai dengan ketentuan tabel PC-1.

Journal of Computer System and Informatics (JoSYC)
Volume 1, No. 4, Agustus 2020, Page 337-345
ISSN 2714-8912 (media online)
ISSN 2714-7150 (media cetak)

3. Biner kunci hasil PC-1 dibagi menjadi 2 kelompok yaitu C_0 dan D_0.
4. Lakukan proses Shift left terhadap C_0 dan D_0 sebanyak 16 kali berdasarkan aturan jumlah perpindahan bit disetiap putaran
5. Gabungkan kembali setiap Ci dan Di hasil Shift left .
6. Masing-masing hasil penggabungan Ci dan Di di Permutation Commpresion 2 (PC-2) sesuai dengan tabel PC-2 untuk menghasilkan internal key (subkey).

3. HASIL DAN PEMBAHASAN

Masalah keamanan data atau sebuah *file* harus menjadi hal yang penting untuk dilihat, dan penyandian berdasarkan teknik kriptografi memberikan hasil yang signifikan untuk mengurangi penyalah gunaan isi dari *file* tersebut. Pengamanan *file* pdf berdasarkan kombinasi algoritma *CBC* dan *Mars* meliputi tahap, yaitu proses perluasan kunci (*key expansion*), proses *enkripsi* dan *dekripsi*.

Blok *plaintext* pertama menggunakan C_0 sebagai vector awal, Blok-blok *plaintext* yang identik di enkripsi menjadi blok-blok *ciphertext*, yang berbeda hanya jika blok-blok *plaintext* sebelumnya berbeda. Pada skema ini setiap *block* n-bit *plaintext* di XOR-kan dengan *block* n-bit *ciphertext*. Kecuali blok *plaintext* pertama di-XORkan dengan suatu konstanta awal atau *initialization vector* (IV), sebesar n-bit. Hasil dari proses XOR tersebut yang kemudian di enkripsi. Dari Algoritma Mars ini proses yang akan di jalan kan terdiri dari ekspansi atau pembangkit kunci, pembangkit kunci disini menggunkan modifikasi dari Algoritma DES.

Plaintext **: JURNAL_ILMIAH_01**
Key **: STMIK_BD**
C_0 / IV **: ISMA_2**
Lakukan SHIFT / Pergeseran 4 bit dari kiri ke kanan.
*Plaintext :

Char	J	U	R	N	A	L
Des	74	85	82	78	65	76
Bin	01001010	01010101	01010010	01001110	01000001	01001100

Char	-	I	L	M	I	A
Des	95	73	76	77	73	76
Bin	01011111	01001001	01001100	01001101	01001001	01000001

Char	H	-	0	1
Des	72	95	0	1
Bin	01001000	01011111	00000000	00000001

*Key :

Char	S	T	M	I	K
Des	83	84	77	73	75
Bin	01010011	01010100	01001101	01001001	01001011

Char	_	B	D
Des	95	66	68
Bin	01010000	01000010	01000100

*C0/ VI :

Char	I	S	M	A	_	2
Des	73	83	77	65	95	2
Bin	01001001	01010011	01001101	01000001	01010000	00000010

Proses pembangkitan kunci karena ada 16 putaran, maka dibutuhkan kunci internal sebanyak 16 buah, yaitu K1, K2, …, K16. Kunci-kunci internal ini dapat dibangkitkan sebelum proses enkripsi atau bersamaan dengan proses enkripsi. Kunci internal dibangkitkan dari kunci eksternal yang diberikan oleh pengguna. Kunci eksternal panjangnya 64 bit atau 8 karakter. Lakukan Permutation Commpression (PC-1) terhadap biner kunci seseai dengan tabel PC-1. Hal ini di lakukan untuk mengkompresikan 64 bit kunci eksternal menjadi 56 bit.

Tabel 1. Permutation Commpression (PC-1)

57	49	41	33	25	17	9
1	58	50	42	34	26	18

Journal of Computer System and Informatics (JoSYC)
Volume 1, No. 4, Agustus 2020, Page 337-345
ISSN 2714-8912 (media online)
ISSN 2714-7150 (media cetak)

10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	45	38	30	22
14	6	61	53	45	37	29
21	13	5	20	20	12	4

Cara melakukan nya cari bit pada posisi ke-57 dan pindahkan pada posisi ke-1, cari bit ke 49 dan pindah kan pada posisi ke-2 cari posisi ke 41 dean pindah kan pada posisi ke-3, dan seterusnya. Gabungkan semua biner kunci kemudian lakukan Permutasi Compresi-1 (PC-1) untuk mendapatkan 56 bit pra kunci
*Biner Kunci:
0101001101010100010011010100100101001011010100000100001001000100
*Hasil PC-1
00000000111111110000000000100101000110000110000111000011

Hasil PC-1 di bagi menjadi 2 kelompok yang terdiri dari C_0 dan D_0 yang masing-masing terdiri dari 28 bit:
C_0 : 00000000111111110000000000010
D_0 : 0101000110000110000111000011

Lakukan proses *Shift left* terhadap C_0 dan D_0 sebanyak 16 kali berdasarkan aturan jumlah perpindahan bit disetiap putaran

Tabel 2. Generate key (Pembangkit Kunci)

Putaran	Jumlah Putaran	C_0	D_0
		00000000111111110000000000010	0101000110000110000111000011
1	1	00000001111111100000000000100	1010001100001100001110000110
2	1	00000011111111000000000001000	0100011000011000011100001101
3	2	00001111111100000000000100000	0001100001100001110000110101
4	2	00111111110000000000010000000	0110000110000111000011010100
5	2	11111111000000000001000000000	1000011000011100001101010001
6	2	11111100000000000100000000011	0001100001110000110101000110
7	2	11110000000000010000000001111	0110000111000011010100011000
8	2	11000000000010000000000111111	1000011100001101010001100001
9	1	10000000000100000000001111111	0000111000011010100011000011
10	2	00000000010000000000111111110	0011100001101010001100001100
11	2	00000001000000000011111111000	1110000110101000110000110000
12	2	00000100000000001111111100000	1000011010100011000011000011
13	2	00010000000001111111110000000	0001101010001100001100001110
14	2	01000000000111111111000000000	0110101000110000110000111000
15	2	00000000011111111000000000001	1010100011000011000011100001
16	1	00000000111111110000000000010	0101000110000110000111000011

Proses generate key (pembangkit kunci) penggabungan kembali C_0 & D_0 hasil left shift operation dan lakukan PC-2. Cara melakukan nya cari bit pada posisi ke-14 dan pindahkan pada posisi ke-1, cari bit ke 17 dan pindah kan pada posisi ke-2 cari posisi ke 11 dan pindahkan pada posisi ke-3, dan seterusnya.

Tabel 3. Permutation Commpression (PC-2)

14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

Setelah di lakukan Generate key maka di hasilkan kunci internal untuk proses Enkripsi :

Tabel 4. Kunci Internal

Journal of Computer System and Informatics (JoSYC)
Volume 1, No. 4, Agustus 2020, Page 337-345
ISSN 2714-8912 (media online)
ISSN 2714-7150 (media cetak)

Round	Biner Kunci
K[1]	101000001001001011000010101011000001010000010110
K[2]	101000000001001001010010100010111101000111100000
K[3]	001001000101101001010000010000001110101100100001
K[4]	000001100111000101010000011100100000110000011100
K[5]	000011100100010101010001110010010001000110011010
K[6]	010011110100000100001001000001010111001000101001
K[7]	000010111000000110001001011100100001100001100100
K[8]	000110010000100010001011100000001000100110111110
K[9]	000110010000101010001000100001010110010110001000
K[10]	000100000011100010001100101010000011001001000001
K[11]	000100000010110001000100111100101100001000100110
K[12]	010000000110110000100100000101000000111110001010
K[13]	110000001010010100100100100111000011000001010001
K[14]	110000001000011000100011011000111110001001100000
K[15]	111000011001001000100010001100001010110100001010
K[16]	101000001001001000101010000101100001010100011101

Setelah didapatkan pembangkit kunci, selanjutnya melakukan proses enkripsi yang dapat dilihat pada dibawah ini:

Lngkah 1
P1 : 01001010 00000000 00000000 00000000 00000000 00000000 ⊕
C0 : 01001001 01010011 01001101 01000001 01011111 00000010
P1' : 00000011 01010011 01001101 01000001 01011111 00000010 ⊕
Key : 10100000 10010010 11000010 10101100 00010100 00010110
Hasil : 10100011 11000001 10001111 11101101 01001011 00010100
Shift 4 dari kiri ke kan
C1 : 00111100 00011000 11111110 11010100 10110001 01001010

Langkah 2
P2 : 01010101 00000000 00000000 00000000 00000000 00000000 ⊕
C1 : 00111100 00011000 11111110 11010100 10110001 01001010
P2' : 01101001 00011000 11111110 11010100 10110001 01001010 ⊕
Key : 10100000 00010010 01010010 10001011 11010001 11100000
Hasil : 11001001 00001010 10101100 01011111 01100000 10101010
Shift 4 dari kiri ke kanan
C2 : 10010000 10101010 11000101 11110110 00001010 10101100

Langkah 3
P3 : 01010010 00000000 00000000 00000000 00000000 00000000 ⊕
C2 : 10010000 10101010 11000101 11110110 00001010 10101100
P3' : 11000010 10101010 11000101 11110110 00001010 10101100 ⊕
Key : 00100100 01011010 01010000 01000000 11101011 00100001
Hasil : 11100110 11110000 10010101 10110110 11100001 10001101
Shift 4 dari kiri ke kanan
C3 : 01101111 00001001 01011011 01101110 00011000 11011110

Langkah 4
P4 : 01001110 00000000 00000000 00000000 00000000 00000000 ⊕
C3 : 01101111 00001001 01011011 01101110 00011000 11011110
P4' : 00100001 00001001 01011011 01101110 00011000 11011110 ⊕
Key : 00000110 01110001 01010000 01110010 00001100 00011100
Hasil : 00100111 01111000 00001011 00011100 00010100 11000010
Shift 4 dari kiri ke kanan
C4 : 01110111 10000000 10110001 11000001 01001100 00100010

Langkah 5
P5 : 01000001 00000000 00000000 00000000 00000000 00000000 ⊕
C4 : 01110111 10000000 10110001 11000001 01001100 00100010
P5' : 00110110 10000000 10110001 11000001 01001100 00100010 ⊕
Key : 00001110 01000101 01010001 11001001 00010001 10011010
Hasil : 00111000 11000101 11100000 00001000 01011101 10111000

Journal of Computer System and Informatics (JoSYC)
Volume 1, No. 4, Agustus 2020, Page 337-345
ISSN 2714-8912 (media online)
ISSN 2714-7150 (media cetak)

Shift 4 dari kiri ke kanan
C5 : 10001100 01011110 00000000 10000101 11011011 10000011

Langkah diatas dilakukan berlanjut hingga sampai pada langkah ke 16, sehingga hasil akhir yang didapatkan adalah

C1 : 00111100 00011000 11111110 11010100 10110001 01001010
C2 : 10010000 10101010 11000101 11110110 00001010 10101100
C3 : 01101111 00001001 01011011 01101110 00011000 11011110
C4 : 01110111 10000000 10110001 11000001 01001100 00100010
C5 : 10001100 01011110 00000000 10000101 11011011 10000011
C6 : 11110001 11110000 10011000 00001010 10011010 10101000
C7 : 01010111 00010001 00010111 10001000 00101100 11001010
C8 : 01110001 10011001 11000000 10001010 01010111 01000000
C9 : 01001001 00110100 10000000 11110011 00101100 10000010
C10 : 01000000 11000000 11000101 10110001 11101100 00110001
C11 : 10011110 11001000 00010100 00110010 11100001 01110001
C12 : 11111010 01000011 00000010 01101110 11101111 10111001
C13 : 00101110 01100010 01101111 00101101 11111110 10000111
C14 : 00011110 01000100 11000100 11100001 11001110 01111011
C15 : 11111101 01101110 01101101 00010110 00110111 00011111
C16 : 11001111 11000100 01111111 00000010 00100000 00100101

Masing-masing block cipher di kelompokan 8 bit perkelompok agar dapat di konversikan menjadi karakter ambil 8 bit kelompok pertama.

Maka Ciphertext yang di hasilkan adalah : **< ' o w Œ ñ W q I @ ž ú . ← ŷ Ï**

Bin	00111100	10010000	01101111	01110111	10001100	11110001
Des	60	144	111	119	140	241
Char	<	'	o	w	Œ	ñ

Bin	01010111	01110001	01001001	01000000	10011110	11111010
Des	87	113	73	64	158	250
Char	W	q	I	@	ž	ú

Bin	00101110	00011110	11111101	11001111
Des	46	30	253	207
Char	.	←	ŷ	Ï

Kemudian setelah proses enkripsi selesai, dilakukan kembali proses dekripsi untuk membaca pesan yang disampaikan.

Block Cipher Asli :
C1 : 00111100 00011000 11111110 11010100 10110001 01001010
C2 : 10010000 10101010 11000101 11110110 00001010 10101100
C3 : 01101111 00001001 01011011 01101110 00011000 11011110
C4 : 01110111 10000000 10110001 11000001 01001100 00100010
C5 : 10001100 01011110 00000000 10000101 11011011 10000011
C6 : 11110001 11110000 10011000 00001010 10011010 10101000
C7 : 01010111 00010001 00010111 10001000 00101100 11001010
C8 : 01110001 10011001 11000000 10001010 01010111 01000000
C9 : 01001001 00110100 10000000 11110011 00101100 10000010
C10 : 01000000 11000000 11000101 10110001 11101100 00110001
C11 : 10011110 11001000 00010100 00110010 11100001 01110001
C12 : 11111010 01000011 00000010 01101110 11101111 10111001
C13 : 00101110 01100010 01101111 00101101 11111110 10000111
C14 : 00011110 01000100 11000100 11100001 11001110 01111011
C15 : 11111101 01101110 01101101 00010110 00110111 00011111
C16 : 11001111 11000100 01111111 00000010 00100000 00100101

Hasil Pengembalian 4 bit kanan ke kiri :
C1 : 10100011 11000001 10001111 11101101 01001011 00010100
C2 : 11001001 00001010 10101100 01011111 01100000 10101010
C3 : 11100110 11110000 10010101 10110110 11100001 10001101
C4 : 00100111 01111000 00001011 00011100 00010100 11000010
C5 : 00111000 11000101 11100000 00001000 01011101 10111000
C6 : 10001111 00011111 00001001 10000000 10101001 10101010

Journal of Computer System and Informatics (JoSYC)
Volume 1, No. 4, Agustus 2020, Page 337-345
ISSN 2714-8912 (media online)
ISSN 2714-7150 (media cetak)

C7 : 10100101 01110001 00010001 01111000 10000010 11001100
C8 : 00000111 00011001 10011100 00001000 10100101 01110100
C9 : 00100100 10010011 01001000 00001111 00110010 11001000
C10 : 00010100 00001100 00001100 01011011 00011110 11000011
C11 : 00011001 11101100 10000001 01000011 00101110 00010111
C12 : 10011111 10100100 00110000 00100110 11101110 11111011
C13 : 01110010 11100110 00100110 11110010 11011111 11101000
C14 : 10110001 11100100 01001100 01001110 00011100 11100111
C15 : 11111111 11010110 11100110 11010001 01100011 01110001
C16 : 01011100 11111100 01000111 00000000 00100010 00000010

Langkah 1
P1 : $C_1 \oplus C_{1-1}$
: $C_1 \oplus C_0$
C1 : 10100011 11000001 10001111 11101101 01001011 00010100 ⊕
C0 : 01001001 01010011 01001101 01000001 01011111 00000010
P1' : 11101010 10010010 11000010 10101100 00010100 00010110 ⊕
Key : 10100000 10010010 11000010 10101100 00010100 00010110
P1 : 01001010 00000000 00000000 00000000 00000000 00000000

Langkah 2
P2 : $C_2 \oplus C_{2-1}$
: $C_2 \oplus C_1$
C2 : 11001001 00001010 10101100 01011111 01100000 10101010 ⊕
C1 : 00111100 00011000 11111110 11010100 10110001 01001010
P2' : 11110101 00010010 01010010 10001011 11010001 11100000 ⊕
Key : 10100000 00010010 01010010 10001011 11010001 11100000
P2 : 01010101 00000000 00000000 00000000 00000000 00000000

Langkah 3
P3 : $C_3 \oplus C_{3-1}$
: $C_3 \oplus C_2$
C3 : 11100110 11110000 10010101 10110110 11100001 10001101 ⊕
C2 : 10010000 10101010 11000101 11110110 00001010 10101100
P3' : 01110110 01011010 01010000 01000000 11101011 00100001 ⊕
Key : 00100100 01011010 01010000 01000000 11101011 00100001
P3 : 01010010 00000000 00000000 00000000 00000000 00000000

Langkah 4
P4 : $C_4 \oplus C_{4-1}$
: $C_4 \oplus C_3$
C4 : 00100111 01111000 00001011 00011100 00010100 11000010 ⊕
C3 : 01101111 00001001 01011011 01101110 00011000 11011110
P4' : 01001000 01110001 01010000 01110010 00001100 00011100 ⊕
Key : 00000110 01110001 01010000 01110010 00001100 00011100
P4 : 01001110 00000000 00000000 00000000 00000000 00000000

Langkah 5
P5 : $C_5 \oplus C_{5-1}$
: $C_5 \oplus C_4$
C5 : 00111000 11000101 11100000 00001000 01011101 10111000 ⊕
C4 : 01110111 10000000 10110001 11000001 01001100 00100010
P5' : 01001111 01000101 01010001 11001001 00010001 10011010 ⊕
Key : 00001110 01000101 01010001 11001001 00010001 10011010
P5 : 01000001 00000000 00000000 00000000 00000000 00000000

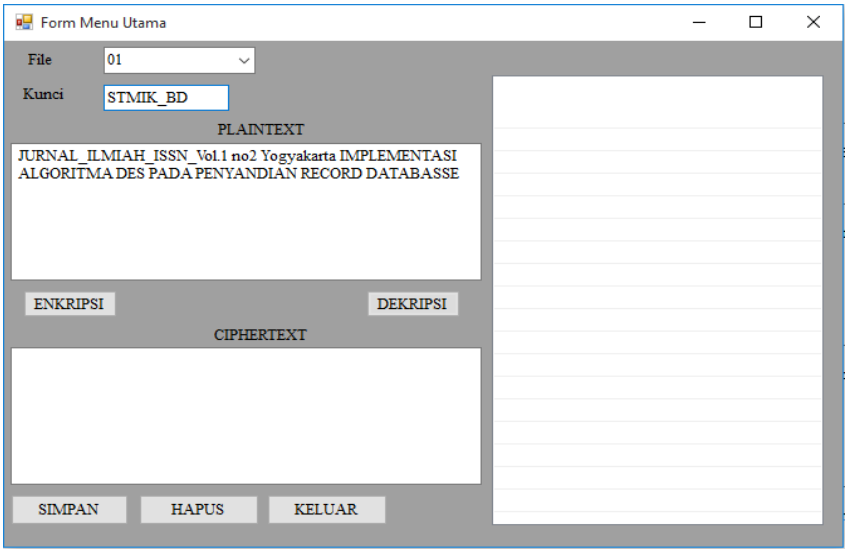
Masing-masing block cipher di kelompokan 8 bit perkelompok agar dapat di konversikan menjadi karakter, ambil 8 bit kelompok pertama. Maka Plaintext yang di hasilkan adalah : **JURNAL_ILMIAH_01**

3.1 Implementasi Program

Pada gambar 1 tampilan *form* menu utama ini didesain minimalis agar pengguna aplikasipentandian text file pdf tidak sulit memahami bagaimana cara menggunakan maupun mengoperasikan aplikasi ini. Bentuk tampilan *input*

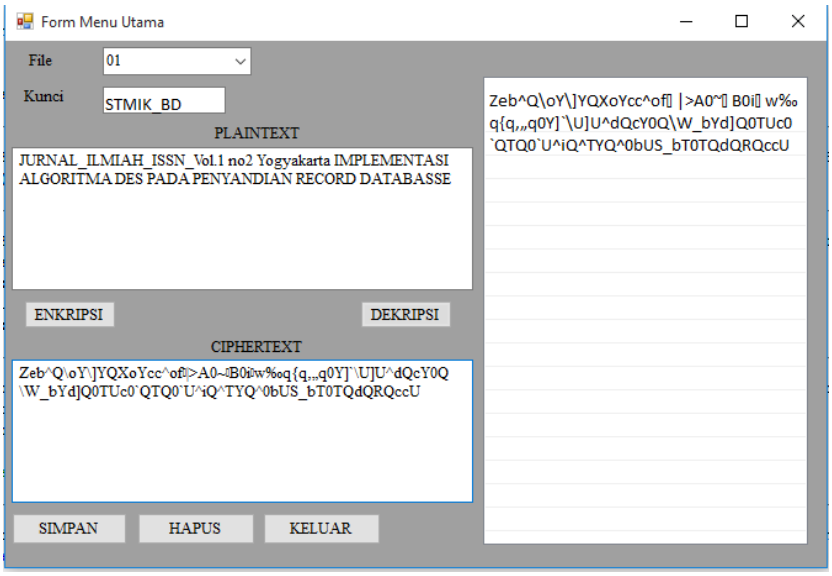
Journal of Computer System and Informatics (JoSYC)
Volume 1, No. 4, Agustus 2020, Page 337-345
ISSN 2714-8912 (media online)
ISSN 2714-7150 (media cetak)

dan *output* penyandian text file pdf yang akan tampil pada menu utama yang akan di menjalankan proses enkripsi dan dekripsi.



Gambar 1. Tampilan *Input Plaintext* PDF

Pada gambar 1 untuk pertama pengguna harus memilih file mana yang akan di enkripsi kan kemudian pengguna mengisi kotak kunci lalu menekan tombol enkripsi agar text dapat tersandikan.



Gambar 2. Tampilan *Output Ciphertext* PDF

Pada gambar 2 pada proses ini text file yang sudah terenkripsi yang berbentuk kode-kode dapat di simpan ke dalam kotak *listview*, dan jika ingin mengembalikan text ke bentuk semula dapat mengunakan tombol dekripsi.

4. KESIMPULAN

Berdasarkan uraian dari bab-bab sebelumnya, maka penulis dapat memberikan kesimpulan sebagai berikut:

1. Proses enkripsi dan dekripsi penyandian *text file* pdf dapat dilakukan dengan kombinasi kedua algoritma sehingga *text* asli atau informasi tidak dapat dibaca dan dimengerti oleh sembarang pihak.
2. Penerapan kedua algoritma *Cipher Block Chaining* (CBC) dan *Mars* dalam proses penyandian *text file* pdf dalam penyisipan kata kunci yang ingin disisipkan dapat merubah pertukaran informasi menjadi berbentuk karakter-karakter, simbol dan huruf yang tidak sesuai dengan text aslinya.
3. Perancangan aplikasi dengan menggunakan *Visual Basic* 2008 yang telah selesai dirancang dengan desain minimalis diharapkan dapat berguna dalam penyandian *text.*

REFERENCES

[1] Hara Pardede, A. M., Manurung, H., & Filina, D. (2017) Algoritma Vigenere Cipher Dan Hill Cipher Dalam Aplikasi Pengamanan Data Pda File Dokumen Jurnal Teknik Informatika Kaputama(JTIK), 1 (Januari), 26-33. Retrieved from
[2] Kurniawan, R. RANGCANG BANGUN APLIKASI PENGAMANAN IIS FILE DOKUMEN. Jurnal Ilmu Komputer Dan Informatika, 01 n0 1 (November). 46-52. Retrieved from, 2017
[3] Zebua, T., & Ndruru, E. Pengamanan Citra Digital Berdasarkan Modifikasi Algoritma Rc4 Jurnal Teknologi Informasi Dan Ilmu Komputer (JTIK), 4 (December), 275-282. 2017
[4] Algoritma, C. Ketepatan Klasifikasi Status Pemberian Air Susu Ibu (ASI) Menggunakan Multivariate Adaptive Regression Splines (MARS) dan, 5,229-238. 2006
[5] Setyaningsih S.Si., M.Kom, E. Kriptografi Dan Implementasinya Menggunakan Matlab. (N. WK,Ed.) (1st ed.). Yogyakarta : Andi Publiser. 2015
[6] Sartika, D. Pengembangan Perangkat Lunak Penyembunyian Pesan Terenkripsi Dengan Menggunakan Algoritma Mars Pada Citra Digital Dengan Metode adaktif, 7(1), 1-6. 2016.
[7] Nugroho, P. S., & Aribowo, E. PENGEMBANGAN MODUL ENKRIPSI DAN DEKRIPSI PADA PHP DENGAN MODIFIKASI METODE KRIPTOGRAFI VIGENERE CIPHER DAN CIPHER BLOCK CHAINING (Studi Kasus pada geekybyte.com) Universitas Ahmad Dahlan, 2(1), 1004-1012. 2014
[8] Kadir, A. Pengenalan Algoritma Pendekatan Secara Visual dan Interaktif Menggunakan RAPTOR. (D. Hardjono, Ed.). Yogyakarta : Andi Publiser. 2013
[9] Maulana, G. G. Pembelajaran Dasar Algoritma Dan Pemograman Menggunakan El-GoritmaBerbasis Web. In Jurnal Teknik Mesin (JTM) (Vol.06, pp. 69 73). 2017
[10] Nugroho, A. Belajar Sendiri Mengimplementasikan SQL Server 2008. Jakarta : PT.Alex Media Komputindo. 2008
[11] Dharwiyanti, S., & Wahono, R. S. Pengantar Unified Modeling Langguage (UML). Ilmu Komputer.Com, 1-13. 2003.