Bulletin of Data Science
ISSN 2745-7966 (Media Online)
Vol 2, No 3, June 2023
Hal 107-117
https://ejurnal.seminar-id.com/index.php/bulletinds

Penerapan Algoritma Block Cipher Odd-Even Confusing Key (OE-CK) Pada Aplikasi Pengamanan Video

Dian Wahyuni Kartini*, Garuda Ginting, Eferoni Ndururu

Fakultas Ilmu Komputer Dan Teknologi Informasi, Teknik Informatika, Universitas Budi Darma Medan Indonesia
Email: dianwahyuninababan2104@gmail.com, rondururu@gmail.com

Abstrak−Masalah yang terdapat pada ruang lingkup video adalah dimana video yang bersifat privasi tersebut dapat ditonton oleh orang yang tidak berhak jika file video tanpa pengamanan. Apabila terjadi suatu pembobolan dan pencurian informasi suatu data penting dalam sebuah file video tersebut, maka akan merugikan pihak yang berkepentingan. Oleh karena itu, dibutuhkan suatu sistem aplikasi untuk dapat mengamankan file video tersebut. Untuk meminimalisir hal ini maka diperlukan pengamanan tingkat kedua yaitu dengan mengacak video tersebut sehingga informasi visual dari video tersebut tidak dapat terlihat oleh orang yang tidak memiliki kunci. Maka informasi dalam file video tersebut di ubah dalam bentuk kode atau isyarat dimana kode inilah yang akan dimanipulasi. Melalui proses pengamanan file video menggunakan algoritma block cipher odd-even confusing key (OE-CK), diharapkan kedepannya sistem ini dapat berpengaruh besar terhadap keamanan file video dari pembobolan dari orang yang tidak berkepentingan.

Kata Kunci: Kriptografi, Algoritma Block Cipher Odd-Even, File video

Abstract−The problem that exists in the scope of the video is where the video that is privacy in nature can be watched by unauthorized people if the video file is without security. If there is a breach and theft of information on an important data in a video file, it will be detrimental to the interested parties. Therefore, an application system is needed to be able to secure the video file. To minimize this, a second level of security is needed, namely by scrambling the video so that visual information from the video cannot be seen by people without keys. Then the information in the video file is changed in the form of a code or signal where this code will be manipulated. Through the process of securing video files using the odd-even confusing key (OE-CK) block cipher algorithm, it is hoped that in the future this system can have a major effect on the security of video files from unauthorized breaches.

Keywords: Cryptography, Odd-even block cipher algorithm, video files

1. PENDAHULUAN

Video bukan hanya karya dari sebuah rumah produksi perfilman. Saat ini siapa saja dapat membuat video asalkan memiliki perangkat pembuat video misalnya menggunakan smartphone. Namun, setiap smartphone memiliki kapasitas terbatas sehingga memungkinkan untuk menyimpannya kedalam suatu drive yang memiliki kapasitas lebih besar misalnya kedalam google drive. Seperti yang sudah kita ketahui bahwa setiap smartphone memiliki satu akun google, dimana akun tersebut bisa digunakan untuk masuk ke akun google lainnya seperti google drive, google maps, dan lain sebagainya.

Ada kalanya file video yang dimasukkan dalam google drive tersebut bersifat private atau rahasia sehingga hanya pemilik akunlah yang bisa membuka google drive tersebut dengan password yang telah terdaftar. Akun google menggunakan cara single sign on yaitu sekali login dapat membuka semua akun google yang dimiliki. Oleh karena itu apabila username dan password salah satu akun diketahui oleh pihak lain maka pihak tersebut dapat membuka semua akun yang lainnya. Hal ini sangat merugikan tak terkecuali jika terdapat rekaman video yang bersifat pribadi yang disimpan di drive tersebut. Untuk meminimalisir hal ini maka diperlukan pengamanan tingkat kedua yaitu dengan mengacak video tersebut sehingga informasi visual dari video tersebut tidak dapat terlihat oleh orang yang tidak memiliki kunci.

Untuk itu dibutuhkan pengamanan file video yang berada dalam google drive tersebut supaya tingkat keamanannya lebih terjamin. Maka informasi dalam file video tersebut di ubah dalam bentuk kode atau isyarat dimana kode inilah yang akan dimanipulasi. Dengan demikian file video perlu diamankan dengan pengamanan yang baik. Sehingga perlu membuat enkripsi dan dekripsi pada file video. Salah satu hal yang penting untuk menjamin kerahasiaan data dan informasi adalah enkripsi. Enkripsi menggunakan suatu algoritma yang dapat mengkodekan semua aliran data (stream) bit dari sebuah pesan menjadi kriptogram yang tidak dimengerti (unintelligible).

Dengan permasalahan yang ada, maka dibutuhkan metode pengamanan untuk tujuan diatas adalah menggunakan teknik keamanan Odd-even confusing key, diantaranya adalah algoritma blok cipher odd-even confusing key. Odd-even confusing key merupakan subsitusi struktur dan struktur jaringan Feistel digunakan untuk ekspansi kunci dan enkripsi atau dekripsi. Ketika struktur jaringan Feistel digunakan untuk ekspansi kunci, struktur jaringan SP digunakan untuk enkripsi atau deskripsi. Metode ini menggunakan struktur jaringan untuk melakukan tidak hanya kunci ekspansi tetapi juga enkripsi atau dekripsi; dengan demikian, ekspansi kuncinya lebih maju. Struktur jaringan SP dan struktur jaringan Feistel mengandung beberapa komponen operasi yang berbeda, untuk memastikan kunci perluasan dan operasi enkripsi atau deskripsi sinkronasi kecepatan sejauh mungkin. Kunci utama 32-bit terbaru mengambil sebagai sinyal kontrol untuk memilih satu dari dua struktur untuk mengenkripsi atau mendekripsi sementara yang lain dipilih untuk mengoperasikan ekspansi kunci. Ada 232 = 4.294.697.296 cara berbeda operasi. Bandingkan dengan struktur tetap dalam enkripsi atau dekripsi dan kunci ekspansi, metode enkripsi yang diusulkan dapat meningkatkan kekebalan[1].

Penelitian ini menguraikan proses yang dilakukan untuk mengkombinasikan teknik kriptografi dalam mengamankan video rahasia. Teknik kriptografi digunakan untuk melakukan penyandian video rahasia berdasarkan algoritma blok

Bulletin of Data Science
ISSN 2745-7966 (Media Online)
Vol 2, No 3, June 2023
Hal 107-117
https://ejurnal.seminar-id.com/index.php/bulletinds

cipher odd-even confusing key. Agar proses yang dilakukan lebih mudah. Dari hasil penelitian ini dapat menunjukan bahwa pengamanan video dengan algoritma blok cipher OE-CK yang digunakan dapat berjalan dengan baik dan dapat memudahkan pengguna dalam mengamankan video berdasarkan latar belakang diatas penulis berisiniatif mengangkat judul yaitu Penerapan Algoritma Block Cipher Odd-Even Confusing Key (OE-CK) Pada Aplikasi Pengamanan Video.

2. METODOLOGI PENELITIAN

2.1 Video

Video adalah teknologi untuk menangkap, merekam, memproses, mentransmisikan dan menata ulang gambar bergerak. Biasanya menggunakan film seluloid, sinyal elektronik, atau media digital. Video juga bisa dikatakan sebagai gabungan gambar-gambar mati yang dibaca berurutan dalam suatu waktu dengan kecepatan tertentu. Gambar-gambar yang digabung tersebut dinamakan frame dan kecepatan pembacaan gambar disebut dengan frame rate, dengan satu fps. Pembuatan video sekarang bisa dilakukan dengan perangkat smartphone. Orang yang memiliki smartphone dapat membuat video untuk dokumentasi video pribadinya seperti video kenang-kenangan keluarga[2].

2.2 Kriptografi

Kriptografi berasal dari bahasa Yunani, crypto dan graphi. Crypto berarti secret (rahasia) dan graphi berarti writing (tulisan). Menurut terminologinya, kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat lain. Kriptografi adalah ilmu yang mempelajari teknik matematis yang berhubungan dengan aspek keamanan informasi seperti tingkat keyakinan, integritas data, autentikasi entitas dan autentikasi keaslian data. Seni didefenisikan dengan akta sejarah bahwa setiap orang mempunyai cara masing-masing untuk mengamankan data, sehingga pesan memiliki nilai estetika tersendiri yang berhubungan dengan seni dan kebudayaan, jika diperhatikan secara mendalam grafi di kriprografi memiliki maksa sebuah seni. Keamanan juga membutuhkan teknik dan seni demikian pula dengan halnya keamanan pada data, kehandalan keamanan tergantung dan cara masing-masing dalam memahami penting dari data tersebut. Dalam menjaga kerahasian data, kriptografi mentransformasikan data jelas (plaintext) kedalam bentuk data sandi (chipertext) yang tidak dapat dikenali. Proses pengembalian sebuah chipertext ke plaintext disebut deskripsi [3]. Kriptografi pada awalnya dijabarkan sebagai ilmu yang mempelajari bagaimana menyembunyikan pesan. Namun pada pengertian modern kriptografi adalah ilmu yang bersandarkan pada teknik matematika untuk berusan dengan keamanan informasi seperti kerahasian, keutuhan data dan otentikasi entitas.

2.3 Mode Operasi

Adapun beberapa mode operasi yang tersedia, yaitu: *electronic codebook, chiper block chaining, chiper feedback, output feedback,* dan *counter*. Variasi mode operasi ini dibuat agar sistem sandi blok dapat dipakai sesuai dengan kebutuhan berdasarkan permintaan aplikasi.

2.3.1 *Electronic Codebook* (ECB)

Mode operasi ECB merupakan mode yang paling sederhana. ECB beroperasi dengan memecah teks asli berukuran N x n bit, menjadi N blok dengan tiapblok berukuran n bit (sesuai dengan ukuran blok sistem penyandian), kemudian tiap blok disandi dengan kunci, dan algoritma enkripsi yang sama [4]. Untuk dekripsi dilakukan hal yang sama, hanya saja menggunakan algoritma dekripsi.

Algoritma enkripsi ECB dapat diselesaikan dengan menggunakan persamaan berikut:

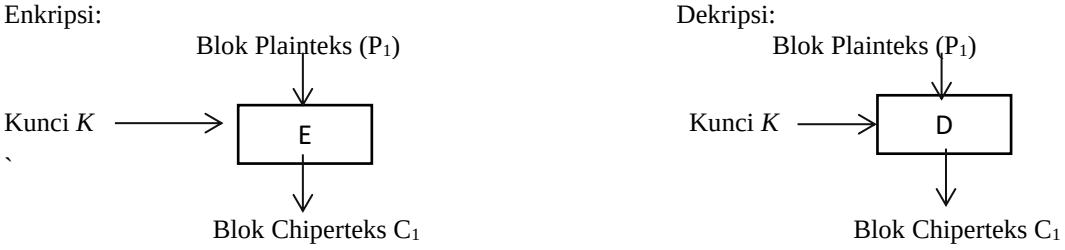
$C_i = E_k(P_i)$ ..... (1)

Sedangkan untuk algoritma dekripsi ECB diselesaikan menggunakan persamaan berikut:

$P_i = D_k(C_i)$ ..... (2)

Keterangan:
C_i = *Ciphertext Index*
E_k = *Enkripsi Key* (Kunci Proses Enkripsi)
D_k = *Dekripsi Key* (Kunci Proses Dekripsi)
P_i = *Plaintext Index*

Untuk lebih jelasnya berikut gambar skema proses enkripsi dan proses dekripsi ECB.



Gambar 1. Skema Enkripsi Dan Dekripsi Pada Cipher Blok
Sumber: Rifki SadiKin2012[7]

Bulletin of Data Science
ISSN 2745-7966 (Media Online)
Vol 2, No 3, June 2023
Hal 107-117
https://ejurnal.seminar-id.com/index.php/bulletinds

Pada mode operasi ECB, jika teks asli memiliki ukuran yang bukan tepat kelipatan ukiran blok sistem penyandian maka diperlukan *padding*. *Padding* merupakan penambahan beberapa byte pada blok terakhir teks asli agar memiliki ukuran yang tepat kelipatan ukuran blok. Larik byte yang digunakan untuk *padding* bias berupa byte kosong atau sebuah larik dengan konstan misalnya byte 80 yang diikuti byte 00. Cara kedua untuk menggenapi panjang teks asli sehingga berukuran tepat kelipatan ukuran blok adalah teknik *chiperteks stealing*. Dengan teknik ini ukuran teks sandi dengan ukuran teks asli tanpa perlu tambahan *padding*. Namun ada 2 yang menjadi kekurangan utama mode operasi ECB, yaitu:

1. Pola teks asli tetap bertahan pada teks sandi. Hal ini disebabkan hasil enkripsi satu blok teks asli yang sama menghasilkan blok teks sandi yang sama.
2. Karena blok teks sandi yang sama memiliki blok teks sandi yang sama, seorang penyadap dapat menggunakan ulang blok teks sandi untuk keperluannya.

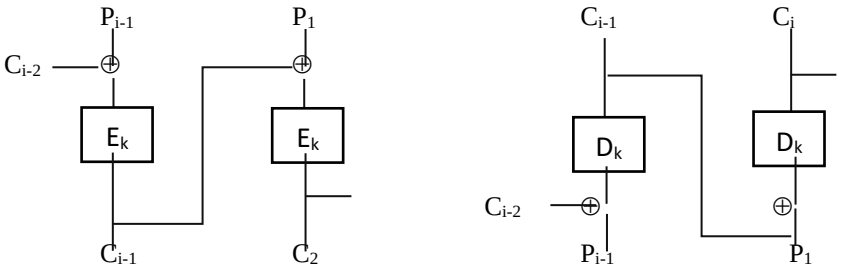
Kelebihan dari mode operasi ECB:

1. Karena tiap blok plainteks dienkripsi secara independen, maka kita tidak perlu mengenkripsi file secara linear. Kita dapat mengenkripsi 5 blok pertama, kemudian blok-blok di akhir, dan kembali ke blok-blok di tengah dan seterusnya.
2. Jika satu atau lebih bit pada blok cipherteks mengalami kesalahan, maka kesalahan ini hanya mempengaruhi cipherteks yang bersangkutan pada waktu dekripsi. Blok-blok cipherteks lainnya bila didekripsi tidak terpengaruh oleh kesalahan bit cipherteks tersebut.

2.3.1 *Chiper Block Chaining* (CBC)

Mode ini menerapkan mekanisme umpan-balik (feedback) pada sebuah blok, yang dalam hal ini hasil enkripsi blok sebelumnya di-umpan-balikkan ke dalam enkripsi blok yang current.Caranya, blok plainteks yang *current* di-XOR-kan terlebih dahulu dengan blok cipherteks hasil enkripsi sebelumnya, selanjutnya hasil peng-XOR-an ini masuk ke dalam fungsi enkripsi. Dekripsi dilakukan dengan memasukkan blok cipherteks yang current ke fungsi dekripsi, kemudian meng-XOR-kan hasilnya dengan blok cipherteks sebelumnya[5]. Dalam hal ini, blok cipherteks sebelumnya berfungsi sebagai umpan-maju *(feedforward)* pada akhir proses dekripsi. Untuk lebih jelasnya dapat dilihat pada gambar berikut:

Enkripsi: Dekripsi:



Gambar 2. Skema Enkripsi dan Dekripsi Mode CBC
Sumber: Sumber: R. Sadikin, 2012[4]

Secara matematis, enkripsi dengan mode CBC dinyatakan dalam persamaan berikut:

$$C_i = E_k (P_i \oplus C_{i-1}) \quad (3)$$

Persamaan dekripsi :

$$P_i = D_k (C_i) \oplus C_{i-1} \quad (4)$$

Adapun yang menjadi kelebihan dari mode CBC yaitu karena blok-blok plainteks yang sama tidak menghasilkan blok-blok cipherteks yang sama, maka kriptanalisis menjadi lebih sulit. Inilah alasan utama penggunaan mode CBC digunakan. Sedangkan yang menjadi kelemahan dari mode CBC ini adalah:

1. Penggunaan IV*(Initialization Vektor)* yang selalu sama mengakibatkan blok teks asli yang sama akan memiliki blok teks sandi yang sama. Direkomendasikan setiap penyandian menggunakan nilai IV yang berbeda misalnya dengan menggunakan *time stamp*.
2. Karena blok cipherteks yang dihasilkan selama proses enkripsi bergantung pada blok-blok cipherteks sebelumnya, maka kesalahan satu bit pada sebuah blok plainteks akan merambat pada blok cipherteks yang berkoresponden dan semua blok cipherteks berikutnya.

2.3.3 *Chiper Feedback* (CFB)

Mode operasi ini untuk mengenkripsi aliran cipher. Dengan cara ini tidak diperlukan lagi *padding* karena jumlah bit data tidak harus merupakan kelipatan blok minimum. Mode ini bekerja pada sistem waktu nyata. Salah satu keistimewaan metode ini adalah bahwa panjang cipher akan tepat sama dengan panjang plainteks.Secara matematis, mode CFB dapat dinyatakan dalam persamaan berikut:

$$C_i = P_i \oplus E_k (C_{i-1}) \quad (5)$$

$$P_i = C_i \oplus E_k (C_{i-1}) \quad (6)$$

Salah satu kerugian dari mode CFB adalah perambatan kesalahan. Jika satu blok cipher mengalami kesalahan ketika di saluran, maka blok-blok berikutnya akan terpengaruh. IV (*Initialization Vektor)* juga harus unik untuk setiap pesan, karena jika IV sama untuk pesan yang berbeda, maka keluaran k, akan juga sama untuk plainteks yang berbeda. Akibatnya

seperti pada sistem OTP, dimana jika kunci yang sama digunakan untuk mengenkrip pesan yang berbeda maka kunci akan mudah ditemukan.

2.3.4 *Output Feedback* (OFB)

Mode operasi OFB hampir mirip dengan mode operasi CFB yaitu harus ada penggunaan IV (*Initialization Vektor)* yang berbeda untuk tiap pengiriman pesan. Selain itu OFB rentan dengan serangan yang disebut dengan serangan *messagen stream,* yaitu mengubah nilai teks sandi tanpa terdeteksi *error correcting code*[4]. Mode OFB tidak mengalirkan error. Satu nit error pada *Chipertext* halnya memperngaruhi satu bit plainteks pada proses dekripsi. Ini berguna untuk sistem analog yang di digitasi seperti *voice* atau video, dimana error satu bit dapat ditoleransi, namun *error* yang mengalir tidak dapat di toleransi[6].

2.4 Algoritma *Odd-even Confusing Key*

Di era perkembangan teknologi informasi saat ini, enkripsi pesan sangat dibutuhkan untuk menjaga kemanan dalam berbagai informasi antar komunikan. Enkripsi harus dibuat serumit mungkin agar sulit untuk dipecahkan oleh penyerang. Algoritma ini adalah algoritma yang bekerja pada 128-bit dengan kunci 128-bit. Algoritma ini menggunakan struktur feistel dengan memanfaatkan operasi subsitusi, pergeseran dan pengecekan fungsi f. Untuk meningkatkan kerumitan, fungsi ekspansi kunci juga memanfaatkan aturan bit ganjil, genap dan pengacakan. Algoritma ini dirancang sedemikian rupa untuk memenuhi prinsip *Confussion* dan *Diffusion*[7]. Algoritma ini memanfaatkan posisi genap dan ganjil pada bit-bit kunci serta pengacakan dengan kotak P untuk meningkatkan *confussion*. Pada fungsi f pada struktur feistelnya. Dilakukan proses subsitusi, penggeseran dan pengacakan. Subsitusi dilakukan dengan kotak S dan pengacakan dilakukan dengan kotak P yang berbeda dengan kotak P pada kunci. Untuk meningkatkan *confussion*, proses *enciphering* juga diulang hingga 10 kali pengulangan.

2.5 Aplikasi

Aplikasi adalah suatu program yang siap untuk digunakan yang dibuat untuk melaksanakan suatu fungsi bagi pengguna jasa aplikasi serta penggunaan aplikasi lain yang dapat digunakan oleh suatu sasaran yang akan dituju. Menurut kamus besar computer eksekutif, aplikasi mempunyai arti yaitu pemecahan masalah yang menggunakan salah satu teknik pemrosesan data aplikasi yang biasanya berpacu pada komputansi yang diinginkan atau diharapkan pemrosesan data yang diharapkan. Pengertian aplikasi menurut Kamus Besar Bahasa Indonesia adalah sebuah penerapan dari rancang sistem untuk mengolah data yang menggunakan aturan atau ketentuan bahasa pemograman tertentu[8].

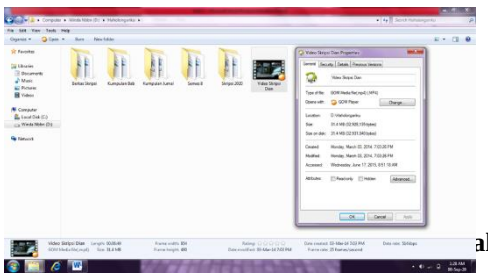
3. HASIL DAN PEMBAHASAN

3.1 Analisa

Masalah yang akan dianalisa adalah bagaimana melakukan pengamanan suatu file video dengan melakukan proses pengecekan atau perbandingan suatu file video yang asli dengan file video yang telah dirubah. File video merupakan suatu sarana transformasi informasi dari satu orang ke orang lain atau dari suatu kelompok ke kelompok lain disimpan didalam sistem file yang dapat diakses dan diatur oleh pengguna. Dalam hal kejahatan file video biasanya dimanipulasi untuk menghilangkan bukti-bukti yang ada didalamnya, oleh sebab itu diperlukan analisis untuk dapat mengamankan file video tersebut. Adanya perubahan yang mengalami perubahan dari bentuk aslinya adalah berupa nama video, perubahan tersebut dapat diklasifikasikan sebagai tindakan sengaja atau tidak sengaja. Perubahan yang disengaja memiliki tujuan yang jahat dengan memodifikasikan konten atau menghapus hak cipta. Disamping itu, perubahan yang tidak disengaja merupakan konsekuensi dari proses operasional digital seperti memperbaiki kecerahan, pengurangan atau penambahan waktu durasi, perubahan format, dll. Untuk membedakan file video yang asli atau sudah dirubah maka diperlukan pendeteksian terhadap file video tersebut. Metode yang digunakan untuk mengamankan video hanya integritas dari video tanpa menunjukan bagian mana pada file video yang telah dimanipulasi. Namun tidak dapat memberikan informasi lokasi mana yang telah dimanipulasi pada file video. Oleh sebab itu maka diperlukan cara mengecek keamanan suatu video dengan memberikan suatu kode atau metadata dari file video.

3.2 Penerapan Algoritma OE-CK

Proses penerapan Algoritma OE-CK dilakukan sesuai dengan langkah yang sudah diuraikan pada sub bab sebelumnya. Sampel video yang digunakan adalah video dengan ekstensi MP4. Lebih jelas dapat dilihat pada gambar berikut ini:



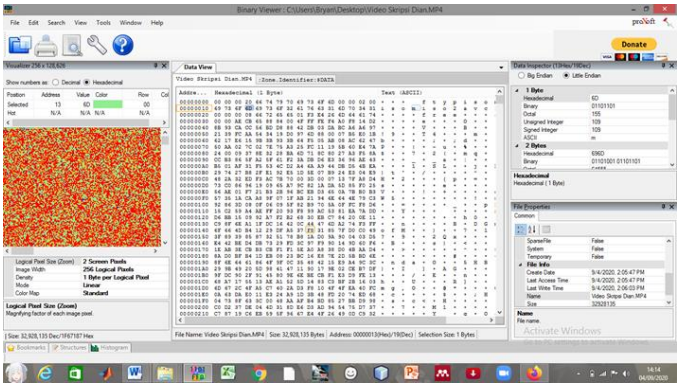
Bulletin of Data Science
ISSN 2745-7966 (Media Online)
Vol 2, No 3, June 2023
Hal 107-117
https://ejurnal.seminar-id.com/index.php/bulletinds

Gambar 3. Gambar File Video sebagai uji coba Algoritma OE-CK

Tabel 1. Informasi *File* video *Sample*

Keterangan	
Jenis File	.MP4
Judul	Video Skripsi Dian
Ukuran	31,4MB
Durasi	06:49 Menit

Dari sample diatas didapatkan nilai *hexadecimal* menggunakan bantuan binary viewer seperti pada gambar dibawah ini:



Gambar 4. Tampilan Nilai Hexadecimal

Nilai piksel pada gambar 3.3, yang digunakan oleh penulis sebagai sampel sebagai berikut: **69 73 6F 6D 69 73 6F 32 61 76 63 31 6D 70 34 31**

3.2.1 Contoh Kasus Algoritma OE-CK

Perhitungan Algoritma OE-CK diketahui yang menjadi pesan adalah **69 73 6F 6D 69 73 6F 32 61 76 63 31 6D 70 34 31,** nilai kunci yang digunakan yaitu " **Dian Nababan**". Langkah pertama yang dilakukan adalah proses pembentukan sub kunci berdasarkan tabel P algoritma OE-CK, sebagai berikut:

Tabel 2. Tabel P algoritma OE-CK

	1	2	3	4	5	6	7	8
1	12	6	46	11	14	50	22	33
2	20	24	19	34	63	25	9	31
3	29	13	54	7	47	28	32	3
4	52	53	61	40	26	41	2	43
5	35	21	39	48	27	44	45	42
6	62	55	10	36	49	58	15	5
7	37	59	38	60	0	8	16	4
8	1	17	23	18	30	56	57	51

Langkah berikutnya membuat kode sub key berdasarkan nilai kunci yang dimasukan nilai kunci yang dimasukan yaitu " **Dian Nababan**", berikut tampilan lengkap tabel kode sub kunci:

Tabel 3. Tabel Kode Sub Kunci

Karakter Kunci	Binner	SubKey Kunci
D	01000100	0
i	01101001	1
a	01100001	2
n	01101110	3
	00100000	4
N	01001110	5
a	01100001	6
b	01100010	7
a	01100001	8
b	01100010	9

a	01100001	10
n	01101110	11
D	01000100	12
i	01101001	13
a	01100001	14
n	01101110	15
	00100000	16
N	01001110	17
a	01100001	18
b	01100010	19
a	01100001	20
b	01100010	21
a	01100001	22
a	01101110	23
D	01000100	24
i	01101001	25
a	01100001	26
n	01101110	27
	00100000	28
N	01001110	29
a	01100001	30
b	01100010	31
a	01100001	32
b	01100010	33
a	01100001	34
n	01101110	35
D	01000100	36
i	01101001	37
a	01100001	38
n	01101110	39
	00100000	40
N	01001110	41
a	01100001	42
b	01100010	43
a	01100001	44
b	01100010	45
a	01100001	46
n	01101110	47
D	01000100	48
i	01101001	49
a	01100001	50
n	01101110	51
	00100000	52
N	01001110	53
a	01100001	54
b	01100010	55
a	01100001	56
b	01100010	57
a	01100001	58
n	01101110	59
D	01000100	60
i	01101001	61
a	01100001	62
n	01101110	63

Langkah berikutnya adalah membuat tabel kotak P untuk kunci perubahan:

Tabel 4. Tabel Kotak P kunci perubahan

	1	2	3	4	5	6	7	8
1	011011 11	010010 00	011000 00	011000 01	011101 01	011101 00	011101 00	001000 00
2	010010	011001	001000	010010	001000	011000	011000	011011

	00	11	00	00	00	01	01	01
3	011000	011011	011011	011101	011001	010011	011000	011011
	01	00	11	01	11	00	01	01
4	011001	011000	001000	010111	011011	011011	011100	011000
	11	01	00	11	11	00	11	01
5	011101	011101	011000	010010	011011	011100	011011	010011
	01	01	01	00	00	11	01	00
6	010010	011011	011001	011101	011101	011100	011000	001000
	00	00	11	00	01	11	01	00
7	011000	011011	110011	011000	010011	011101	011100	011000
	01	01	11	01	00	00	11	01
8	011000	011011	011000	011000	011100	010011	011000	011000
	01	01	01	01	11	00	01	01

Berdasarkan tabel P diatas maka nilai kunci ganjil dan kunci genap yang digunakan pada proses enkripsi OE-CK sebagai berikut:

K1 = 01101111 01001000 01100000 01100001 01110101 01110100 01110100 00100000
K2 = 01001000 01100111 00100000 01001000 00100000 01100001 01100001 01101101
K3 = 01100001 01101100 01101111 01110101 01100111 01001100 01100001 01101101
K4 = 01100111 01100001 00100000 01011111 01101111 01101100 01110011 01100001
K5 = 01110101 01110101 01100001 01001000 01101100 01110011 01101101 01001100
K6 = 01001000 01101100 01100111 01110100 01110101 01110011 01100001 00100000
K7 = 01100001 01101101 11001111 01100001 01001100 01110100 01110011 01100001
K8 = 01100001 01101101 01100001 01100001 01110011 01001100 01100001 01100001

Selanjutnya proses penyandian algoritma OE-CK dilakukan sebanyak 8 kali putaran. Langkah pertama bagi blok menjadi dua blok yaitu Blok L (*Left*) dan Blok R (*Right*) dengan masing-masing jumlah biner perblok sebanyak 64 bit.

M = **69 73 6F 6D 69 73 6F 32 61 76 63 31 6D 70 34 31**

Hasil pembagian blok :

L0 = **69 73 6F 6D 69 73 6F 32**
R0 = **61 76 63 31 6D 70 34 31**

PUTARAN 1 :

Melakukan proses fungsi *round* terhadap R0:

1. Proses XOR R0 dengan Subkey K1

   R0 = 01100001 01110110 01100011 00110001 01101101 01110000 00110100 00110001
   K1 = 01101111 01001000 01100000 01100001 01110101 01110100 01110100 00100000
   = 00001110 00111110 00000010 01010000 00011000 00000100 01000000 00010001

2. Subtitusi biner hasil proses XOR RO dengan Subkey K1, menggunakan kotak S (nilainya sudah menjadi ketetapan).

Tabel 5. Kotak S untuk subtitusi nilai pada blok

Box-S OE-CK			
7	14	4	13
12	1	0	6
9	8	5	3
10	15	11	2

Tabel 6. Kotak P permutasi pesan

5,15,7,2,4,0,9,8,12,1,10,14,3,6,11,13

Lakukan proses subtitusi terhadap nilai biner dari hasil proses XOR RO dengan subkey K1 dengan cara menyusun terlebih dahulu biner kedalam bentuk matriks 4x4. Blok pertama kali diubah ke bentuk matriks 4x4 (yang berarti 1 sel berisi 4 bit pesan) untuk dioperasikan selanjutnya. Pembentukan matriks dilakukan dengan cara yang sederhana dimana pesan dibagi menjadi blok sepanjang 4 bit dan dimasukkan secara sekuensial dari kiri ke kanan pada matriks. Lebih jelasnya dapat dilihat pada tabel berikut ini :

Tabel 7. Blok Matriks Pesan

0000	1110	0011	1110
0000	0010	0101	0000
0001	1000	0000	0100
0100	0000	0001	0001

Tabel 8. HasilSubstitusi dari blok pesan matriks menggunakan kotak S

0111	0000	0111	0011
1100	1100	0101	0110

1000	0000	0101	0111
1110	1111	1010	0011

3. Lakukan pergeseran terhadap matriks dari hasil subtitusi blok pesan
   Selanjutnya dilakukan pergeseran terhadap matriks pergeseran dilakukan terhadap sel pada matriks. Isi sel pada baris pertama dan ketiga digeser ke kanan dan baris kedua dan keempat digeser ke kiri.

Tabel 9. Hasil pergeseran blok

1100	0011	0101	0110
1110	1111	1010	0011
0111	0000	0111	0011
1000	0000	0101	0111

4. Lakukan permutasi dari hasil pergeseran menggunakan Box-P
   Selanjutnya adalah melakukan permutasi dari hasil yang didapat dari pergeseran terhadap sel pada matriks dengan menggunakan Box-P.

Tabel 10. Pergeseran di permutasi menggunakan Box-P

1100	0111	0101	0110
12	7	5	6
1110	1111	1010	0011
14	15	10	3
0111	0000	0111	0011
7	0	7	3
1000	0000	0101	0111
8	0	5	7

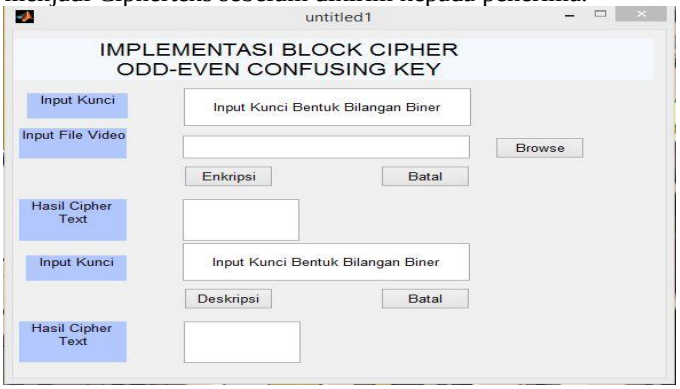
Tabel 11. Permutasi

7	12	6	5
3	15	10	14
7	3	0	7
5	0	8	7

0111 1100 0110 0101
0011 1111 1010 1110
0111 0011 0000 0111
0101 0000 1000 0111
R0 = 01111100 01100101 00111111 10101110 01110011 00000111 01010000 1000 0111
L0 = 01101001 01110011 01101111 01101101 01101001 01110011 01101111 00110010
R1 = 00010101 00010110 01010000 11000011 00011010 01110100 00111111 10110101.
Lakikan putaran hingga mendapatkan hasil yang sesuai, maka putaran ini dilakukan hingga 8 kali putaran.
Maka hasil R adalah : **31 5F 9C F9 CB F2 1C BE**
Maka hasil L adalah : **39 EA FE F8 AE 5D 5C DC**

3.3 Penerapan Algoritma Blok Cipher Odd-Even Confusing Key (OE-CK)

Algoritma Blok Cipher Odd-Even Confusing Key (OE-CK) diterapkan ke File Video yang akan diamankan dengan tujuan merubah *Plainteks* video menjadi Cipherteks sebelum dikirim kepada penerima.

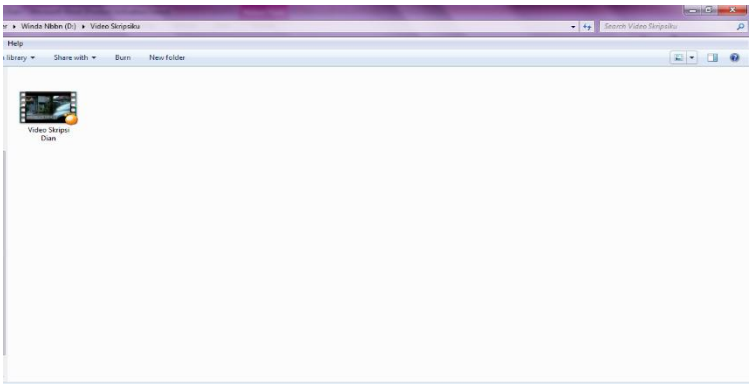


Gambar 5. Tampilan Implementasi Blok Cipher OE-CK

Bulletin of Data Science
ISSN 2745-7966 (Media Online)
Vol 2, No 3, June 2023
Hal 107-117
https://ejurnal.seminar-id.com/index.php/bulletinds

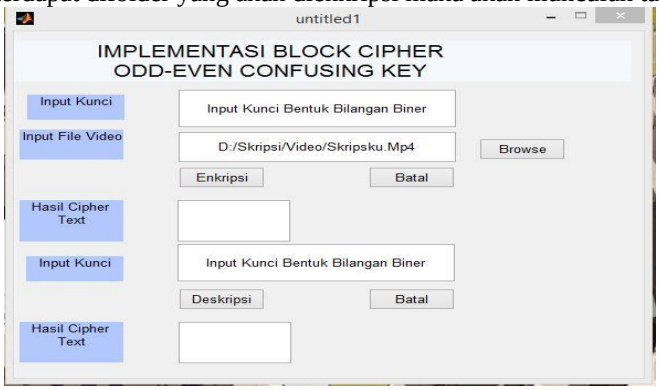
Klik Tombol Browse untuk memilih video yang akan dienkripsi. Lalu pilih file seperti yang bisa dilihat pada gambar di bawah ini.

Bulletin of Data Science
ISSN 2745-7966 (Media Online)
Vol 2, No 3, June 2023
Hal 107-117
https://ejurnal.seminar-id.com/index.php/bulletinds



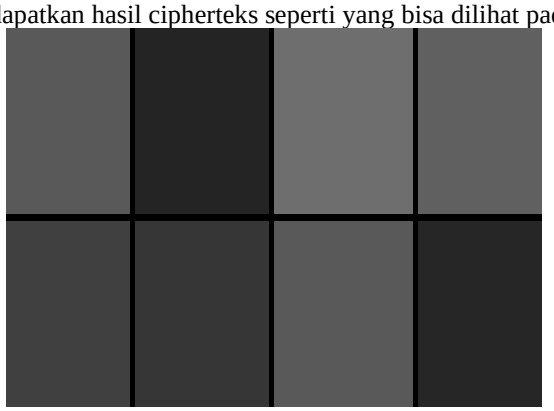
Gambar 6. File yang dipilih

Setelah memilih video yang terdapat difolder yang akan dienkripsi maka akan munculah tampilan sebagai berikut :



Gambar 7. Tampilan Implementasi Blok Cipher OE-CK Setelah File Di Browse

Setelah video di enkripsi maka didapatkan hasil cipherteks seperti yang bisa dilihat pada gambar di bawah ini :



Gambar 8. Hasil Enkripsi Blok Cipher OE-CK

Video yang telah dienkripsi menjadi Cipherteks kemudian dapat langsung didekripsi dengan memasukkan lagi kunci yang didekripsi. Maka dari proses dekripsi didapatlah hasil Video yang seperti semula.

Gambar 9. Hasil Dekripsi Blok Cipher OE-CK

4. KESIMPULAN

Dalam pembahasan sebelumnya penulis bisa membuat beberapa kesimpulan yang dimana dalam penggunaan Algoritma Blok Cipher Odd-Even Confusing Key (OE-CK) dalam pengamanan video. Adapun kesimpulan yang bisa diperoleh. Algoritma Blok Cipher Odd-Even Confusing Key (OE-CK) menggunakan struktur feistel yang bekerja pada kunci sepanjng 128-bit dan blok sepanjang 128-bit. Implementasi pada Algoritma Blok Cipher Odd-Even Confusing Key (OE-CK) untuk mengamankan video terdiri dari proses enkripsi dan dekripsi. Pengujian yang dilakukan melalui aplikasi matlab, karena belum mendapatkan hasil dari pengujian tersebut, maka form yang dirancang terdiri dari form impelementasi algoritma Blok Cipher Odd-Even Confusing Key (OE-CK), dimana form tersebut untuk mengetahui hasil enkripsi dan dekripsi dari Video.

REFERENCES

[1] F. N. Pabokory, I. F. Astuti, and A. H. Kridalaksana, "Implementasi Kriptografi Pengamanan Data Pada Pesan Teks, Isi File Dokumen, Dan File Dokumen Menggunakan Algoritma Advanced Encryption Standard," Inform. Mulawarman J. Ilm. Ilmu Komput., vol. 10, no. 1, p. 20, 2016, doi: 10.30872/jim.v10i1.23.
[2] K. D. Wandani and S. Sinurat, "Implementasi Secure Hash Algoritma Untuk Pengamanan Pada File Video," vol. 13, pp. 165–168, 2018.
[3] Harun Mukhtar, Kriptografi Untuk Keamanan Data. Yogyakarta: Deepublish, 2018.
[4] R. S. Andi, "kriptografi untuk Keamanan Jaringan dan Impelementasinya dalam Bahasa Java," pp. 341–342, 2012.
[5] I. Y. K. Mt, Kriptografi Keamanan Internet dan Jaringan Komunikasi. Bandung: Informatika Bandung, 2004.
[6] Dony Ariyus, Pengantar Ilmu Kriptografi_ Teori Analisis & Implementasi - Dony Ariyus, Universitas Amikom - Google Buku. Yogyakarta: C.V ANDI OFFSET, 2008.
[7] A. Akbar and A. Pangestu, "Algoritma Blok Cipher OE-CK."
[9] J. Andi, "Pembangunan Aplikasi Child Tracker Berbasis Assisted – Global Positioning System (A-GPS) Dengan Platform Android," J. Ilm. Komput. dan Inform., vol. 1, no. 1, pp. 1–8, 2015.