Modifikasi Algoritma Hill Cipher dan Twofish Menggunakan Kode Wilayah Telepon

Hill Cipher and Twofish Algorithm Modification with Phone Region Code

Selviana Yunita *[1], Patmawati Hasan[2], Dony Ariyus[3]
[1,2,3]Universitas Amikom Yogyakarta Jl. Ring Road Utara, Yogyakarta, Tlp (0274) 884201
[1,2,3]Magister Teknik Informatika, Universitas Amikom Yogyakarta
e-mail: [1]selviana.yunita.ax@gmail.com, [2]patmawatihasan@gmail.com, [3]dony.a@amikom.ac.id

Abstrak

Kemudahan pengaksesan media komunikasi oleh semua orang, akan memberikan dampak bagi keamanan informasi atau pesan yang menggunakan media komunikasi tersebut. Informasi menjadi sangat rentan untuk diketahui, diambil dan dimanipulasi oleh pihak-pihak yang tidak bertanggung jawab. Salah satu alternatif yang dapat digunakan untuk menjaga kerahasiaan adalah dengan menyamarkan menjadi bentuk tersandi yang tidak bermakna, yang dapat dilakukan dengan menggunakan kriptografi. Oleh sebab itu dibutuhkan suatu metode atau cara yang dapat menjaga kerahasiaan informasi ini, yang salah satunya dikenal dengan sebutan kriptografi. Dalam kriptografi terdapat banyak algoritma, Twofish salah satu kandidat AES, karena Twofish memenuhi semua kriteria yang dibutuhkan oleh NIST, yaitu 128-bit block, 128 bit, 182 bit, dan 256 bit key. Hasil dari penelitian ini adalah mengaplikasikan modifikasi algoritma hill cipher dengan kode wilayah yang kemudian di enkripsi dengan menggunakan metode Twofish dalam proses enkripsi dan dekripsi file agar kriptanilisis sulit memecahkan chipertextnya sehingga keamanan data tetap terjaga keasliannya. Hasil dari enkripsi dengan algoritma ini adalah file yang dapat diakses melalui aplikasi notepad yang berisi simbol acak. Pengujian dilakukan dengan membandingkan proses beberapa jenis file dari segi kecepatan serta jumlah data yang diproses pada saat enkripsi dan dekripsi.
Kata kunci*— kriptografi, hill cipher, twofish*

Abstract

The ease of accessing communication media by people, of course, will have an impact on the security of information or messages that use these communication media. Information becomes very vulnerable to known, taken and manipulated by irresponsible parties. One alternative that can be used to maintain confidentiality is to disguise these information into an insignificant encrypted form, which can be done using cryptography. Therefore we need a method that can maintain the confidentiality of this information, which one is known as cryptography. In cryptography there are many algorithms, Twofish is one of the AES candidates, because Twofish fulfills all the criteria needed by NIST, namely 128-bit block, 128 bit, 182 nit, and 256 bit key. The results of this study are to apply the modification of the hill cipher algorithm with region codes and then encrypted using the Twofish method in so that cryptanilysis is difficult to solve the ciphertext and data security is maintained. The result of encryption with this algorithm is a file accessable through a notepad application that contains random symbols. Testing is done by comparing the process of several types of files in terms of speed and the amount of data when encryption and decryption process.

Keywords*— cryptography, hill cipher, twofish*

1. PENDAHULUAN

Kemajuan teknologi informasi telah memberikan dampak yang sangat luas, salah satunya sebagai media penyampaian informasi dari suatu tempat ke tempat lainnya, sehingga memudahkan orang dalam mengakses suatu informasi. Kemudahan pengaksesan media komunikasi oleh semua orang, tentunya akan memberikan dampak bagi keamanan informasi atau pesan yang menggunakan media komunikasi tersebut. Informasi menjadi sangat rentan untuk diketahui, diambil dan dimanipulasi oleh pihak-pihak yang tidak bertanggung jawab. Salah satu alternatif yang dapat digunakan untuk menjaga kerahasiaan adalah dengan menyamarkan menjadi bentuk tersandi yang tidak bermakna, yang dapat dilakukan dengan menggunakan kriptografi.

Kriptografi adalah ilmu yang mempelajari bagaimana menjaga agar data tetap aman saat dikirimkan, dari pengirim ke penerima tanpa mengalami gangguan dari pihak ketiga, yang bertujuan untuk menjaga kerahasiaan. Didalam kriptografi terdapat dua konsep utama yaitu enkripsi dan dekripsi [1].

Algoritma kriptografi dapat dibagi ke dalam kelompok algoritma simetris dan algoritma asimetris. Algoritma simetris merupakan algoritma kriptografi yang menggunakan kunci yang sama baik untuk proses enkripsi maupun dekripsi. Algoritma simetris dapat dikelompokkan menjadi dua kategori, yaitu *cipher* aliran dan *cipher* blok. *Cipher* aliran merupakan algoritma kriptografi yang beroperasi dalam bentuk bit tunggal. Sedangkan algoritma kriptografi kategori *cipher* blok beroperasi dalam bentuk blok bit. Saat ini sudah banyak berkembang algoritma kriptografi simetris baik untuk kategori *cipher* aliran maupun *cipher* blok [2]. Beberapa algoritma kriptografi yang dikategorikan ke dalam algoritma simetris adalah DES, AES, Blowfish, IDEA, Saphent, Skipjack, Twofish dan lain-lain.

Beberapa penelitian pada bidang kriptografi terdahulu dibahas mengenai penyelesaian masalah pengamanan file pada perangkat yang menggunakan sistem operasi Android dengan menggunakan AES (Advanced Encryption Standard) algoritma Rijndael. Dalam aplikasi dapat menghasilkan file yang terenkripsi agar tidak dapat dibuka [3]. Penelitian Edy Rahman melakukan pengujian algoritma twofish terhadap estimasi waktu yang diperlukan pada saat proses enkripsi dan dekripsi suatu file dan besar ukuran file pada saat proses enkripsi dan dekripsi [4].

Selanjutnya penelitian Pratiwi menyatakan bahwa algoritma Blowfish dapat digunakan untuk mengamankan data pada aplikasi email dikarenakan algoritma Blowfish dapat berjalan pada jalur komunikasi atau enkripsi file otomatis. Proses enkripsi dan dekripsi menggunakan key yang memiliki panjang maksimum 56 karater dan telah disepakati oleh kedua belah pihak [5]. Penelitian Ratih menyatakan bahwa algoritma twofish merupakan algoritma yang dapat diterapkan untuk enkripsi aliran pesan suara dengan kualitas cukup baik dan lebih efisien. Delay yang dihasilkan meskipun tetap terasa tidak mengganggu dan suara yang dihasilkan dapat didengar tanpa terputus-putus [6]. Selain itu, penelitian yang dilakukan oleh Sayuti melakukan perbandingan performa terhadap algoritma *hill cipher* dan algoritma RSA berdasarkan waktu dan penggunaan memori pada perangkat *mobile* android, dan diperoleh hasil algoritma *hill cipher* lebih baik dalam hasil waktu, sedangkan algoritma RSA lebih baik dalam hal performa memori [7].

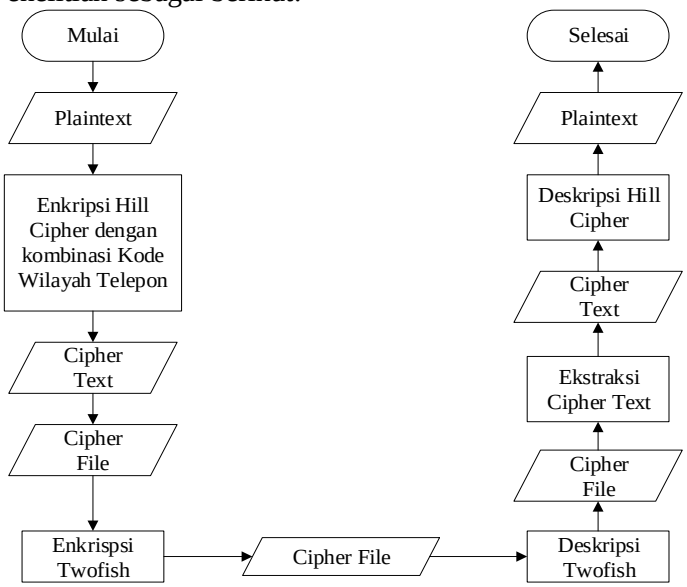
Berdasarkan penelitian yang pernah dilakukan terkait Enkripsi dan Dekripsi pengamanan data atau file, maka akan dilakukan penelitian tentang penerapan modifikasi algoritma *hill cipher* dengan menggunakan kode wilayah telepom sebagai kunci dan setelah diperoleh *cipher text*, kemudian digunakan algoritma twofish pada enkripsi dan dekripsi file dengan kunci 128 bit. File yang dapat diproses adalah file-file yang ada pada Microsoft Office, File berekestensi jpg, pdf. Penelitian ini bertujuan untuk membuat suatu modifikasi algoritma kriptografi yang diharapkan nantinya dapat memberikan alternatif algoritma yang lebih baik dari segi kecepatan enkripsi serta kerumitan dalam pemecahan sandi. Penelitian ini dilakukan dengan menguji enkripsi dan dekripsi file yang dienkripsi menjadi karakter yang acak sehingga menjadi file yang rusak. Data hasil enkripsi dan data hasil dekripsi penelitian yang dilakukan

dapat bermanfaat dalam memberikan keamanan suatu data informasi yang dimiliki, berupa penyandian data dan informasi menjadi sesuatu yang tidak terbaca oleh pihak yang tidak berhak dan juga bermanfaat dalam memberikan tambahan informasi terkait proses enkripsi dan dekripsi yang terjadi pada algoritma twofish. Serta melihat sejauh mana kecepatan eknkripsi dan dekripsi dalam algoritma Twofish. Pengujian dilakukan dengan membandingkan beberapa jenis file yang dienkripsi dengan algoritma tersebut serta bagaimana kecepatan enkripsi menggunakan modifikasi algoritma ini.

2. METODE PENELITIAN

2.1. Alur Penelitian

Alur yang digunakan dalam membuat kombinasi hill cipher dan twofish dapat dilihat pada gambar 1 Alur Penelitian sebagai berikut:



Gambar 1 Alur Penelitian

Penelitian ini terdiri atas beberapa langkah sehingga dapat diperoleh gambaran alur data. Langkah pertama adalah dengan menginput *plain text* pada sistem yang kemudian diproses dengan algoritma *hill cipher* yang dikombinasikan dengan kode wilayah telepon. Setelah *cipher text* diperloeh, file yang berisi *cipher text* tersebut akan di enkripsi kembali dengan menggunakan algoritma *twofish*, dan diperoleh hasil *cipher file* yang berisi kumpulan simbol acak. Selanjutnya, jika dilakukan proses dekripsi, *cipher file* akan di dekripsi dengan menggunakan algoritma *twofish*, setelah diperoleh file hasil dekripsi, dilakukan ekstraksi terhadap file untuk memperoleh *cipher text*. Selanjutnya cipher text akan di dekripsi kembali menggunakan algoritma *hill cipher* yang dikombinasikan dengan kode wilayah telepon. Hasil akhirnya adalah berupa *plain text* seperti input awal sebelum dilakukan proses enkripsi dan dekripsi.

2.2. *Hill Cipher*

Hill Cipher merupakan salah satu algoritma kriptografi *polyalphabeti* yang menggunakan metode subtitusi dengan perhitungan perkalian matriks. Kunci pada *hill cipher* adalah sebuah matriks K berukuran n x n yang digunakan untuk mensubtitusikan n alfabet sekaligus[8]**.**

2.3. Twofish

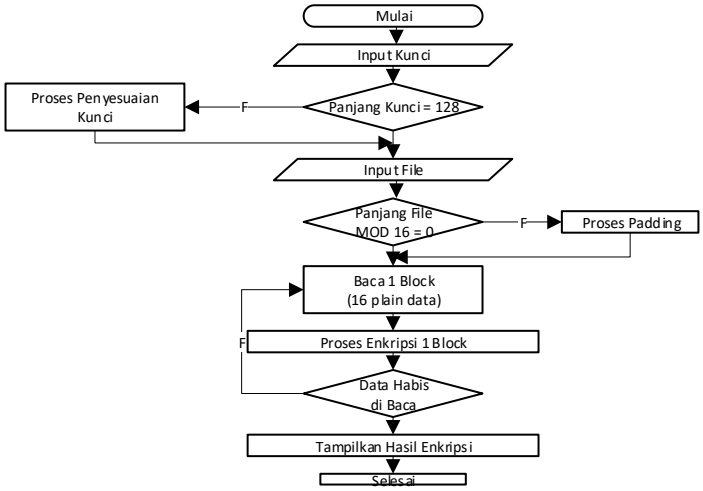
Twofish adalah algoritma kriptografi yang beroperasi dalam mode block cipher. Perancangan Twofish dilakukan dengan memperhatikan kriteria-kriteria yang diajukan National Institute of

Standards and Technology (NIST) untuk kompetisi Advanced Encryption Standard (AES). Twofish adalah block cipher yang berukuran 128 bit yang dapat menerima kunci dengan panjang mencapai 256 bit. Twofish merupakan algoritma yang beroperasi dalam mode blok [9]. Unsur pembangun twofish terdiri dari feistel network (jaringan feistel), s-boxes, matriks MDS, transformasi pseudo-hadamard (PHT), whitening, dan key schedule (penjadwalan kunci). Penjabaran dari unsur unsur pembangun twofish sebagai berikut [4] :

a. *Feistel Network* adalah metode umum untuk mentransformasi fungsi tertentu (biasanya disebut sebagai fungsi F) menjadi permutasi.
b. *S-Boxes* adalah operasi subsitusi *table-driven non linear* yang digunakan dalam *block cipher*. *S-boxes* bervariasi antara setiap ukuran input dan ukuran output, dan dapat diciptakan secara random atau dengan algoritma.
c. *Code Maximum Distance Separable* (MDS) melalui sebuah pemetaan *linear* dari elemen *field* a ke elemen *field* b, menghasilkan campuran dari *vector* a+b elemen, dengan properti jumlah minimum angka tidak nol dalam vector tidak nol paling kurang b+1. Dengan kata lain "*Distance*" adalah jumlah elemen yang berbeda antara dua vector yang berbeda yang dihasilkan oleh MDS paling kurang b+1.
d. *Transformasi Pseudo-Hadamard* adalah operasi sederhana yang bekerja dengan cepat dalam software. Diberikan dua input, a dan b, dan PHT 32 bit didefinisikan sebagai:
   $a' = a + b \bmod 2^{32}$
   $b` = a + 2b \bmod 2^{32}$
   Twofish menggunakan 32 bit PHT untuk mencampur *output* dari dua buah fungsi g 32 bit parallel.
e. *Whitening* merupakan teknik meng-XOR-kan key material kunci sebelum putaran pertama dan sesudah putaran terakhir.
f. Penjadwalan kunci adalah proses dimana pengacakan kunci untuk melakukan proses enkripsi sehingga tingkat kesulitan menjadi tinggi.
g. Fungsi F adalah permutasi yang bergantung pada kunci dengan nilai 64 bit. Fungsi ini menerima 3 (tiga) argumen, dua buah 32 bit R0 dan R1, dan nomor putaran untuk menentukan subkunci mana yang dipakai. R0 akan diserahkan ke fungsi g yang akan mengembalikan T0. R1 akan digeser sejauh 8 bit yang kemudian diberikan juga ke fungsi g yang akan mengembalikan T1. Hasil T0 dan T1 kemudian dikombinasikan ulang menggunakan transformasi *pseudo-Hadamard*, yang kemudian ditambahkan dengan dua buah 32 *bit* dari kunci.
   $T_0 = g(R0)$
   $T_1 = g(\text{shiftLeft}(R1,8))$
   $F0 = (T0+T1+K2r+8) \bmod 2^{32}$
   $F1 = (T0+2T1+K2r+9) \bmod 2^{32}$
   F0 dan F1 adalah hasil dari F, yang masing-masing sepanjang 32 bit. Hasil keluaran ini nantinya akan dipertukarkan dan dimasukkan kembali ke putaran selanjutnya.
h. Fungsi G merupakan jantung dari keseluruhan algoritma twofish. 32 bit masukan X dari fungsi F dipecah menjadi 4 buah yang masing-masing sepanjang 8 bit. Setiap 8 bit kemudian diproses dengan kotak S yang bersesuaian. Setiap kotak S bersifat bijektif, yaitu menerima 8 bit dan mengeluarkan 8 bit pula. 4 buah 8 bit hasil keluaran, kemudian dikalikan dengan matriks Most Distance Separable(MDS) 4x4. Hasil pengalian kemudian diartikan sebagai 32 bit, yang merupakan keluaran dari fungsi g, yang kemudian akan dikembalikan ke fungsi f.

2.4. Proses Enkripsi

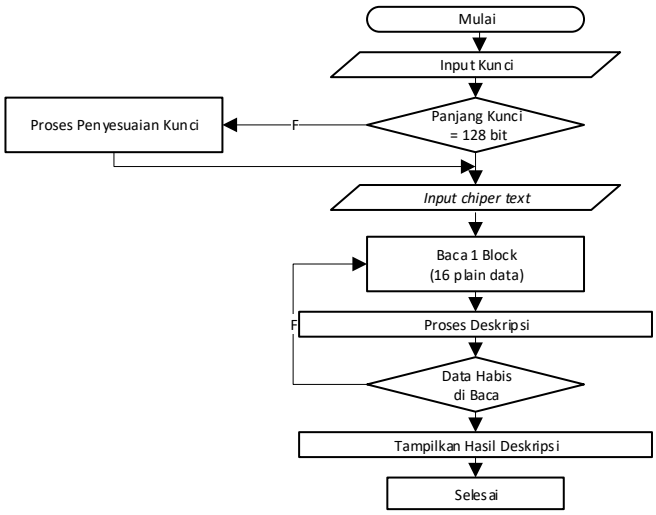
Berikut dijelaskan proses enkripsi data sesuai algoritma twofish, ditunjukan pada Gambar 2 dibawah ini :



Gambar 2 Proses Enkripsi Twofish

Pada gambar 1 dijelaskan langkah-langkah dalam proses enkripsi data, sesuai dengan algoritma twofish yang dapat dijelaskan sebagai berikut : (1) memulai proses enkripsi data (plaintext) dengan ukuran blok 128 bit, (2) setelah itu masukan kunci guna untuk memulai proses enkripsi, (3) apabila panjang kunci kurang dari 128 bit, maka akan melakukan penyesuaian agar dapat mencapai 128 bit, (4) masukan data atau file yang akan kita enkripsi, (5) apabila plaintext berukuran 128 bit, maka tidak akan melakukan proses padding, tetapi plaintext yang ukuranya lebih dari 128 bit otomatis akan melakukan proses padding, (6) langkah selanjutnya proses enkripsi 1 block akan terjadi, apabila data yang dibaca belum habis sampai akhir maka akan berulang hingga data dibaca sampai habis,apabila data sudah dibaca habis oleh sistem maka otomatis akan mengeluarkan hasil enkripsi, (7) selesai

2.5. Proses Dekripsi



Gambar 3 Proses Dekripsi Twofish

Pada gambar 3 dijelaskan langkah-langkah proses dekripsi data sesuai algoritma twofish yang dapat dijelaskan sebagai berikut : (1) memulai proses dekripsi data (chipertext) dengan ukuran blok 128 bit, (2) setelah itu masukan kunci guna untuk memulai proses dekripsi, (3) apabila panjang kunci kurang dari 128 bit, maka akan meakukan penyesuaian agar dapat mencapai 128 bit, (4) masukan data atau file yang akan di dekripsi, (5) setelah itu membaca 1 blok (16 byte

chiper data), (6) langkah selanjutnya proses dekripsi 1 block akan terjadi, apabila data yang dibaca belum habis sampai akhir maka akan berulang hingga data dibaca sampai habis,apabila data sudah dibaca habis oleh sistem maka otomatis akan mengeluarkan hasil dekripsi, (7) selesai.
Langkah-langkah algoritma *Twofish* adalah sebgai berikut:

a. Masukan satu blok plainteks adalah 128 bit. Satu blok tersebut dibagi menjadi 4 buah sub-blok yang masing-masing sepanjang 32 bit (A, B, C, dan D).
b. Masing-masing blok tersebut diputihkan dengan men-XOR-kan dengan kunci K0, K1, K2, dan K3.

Langkah-langkah 1 putaran adalah sebagai berikut:

a. 2 buah 32 bit yang kiri (A dan B) merupaan input dari fungsi g (yang merupakan bagian dari fungsi f), yang salah satunya (B) di geser ke kiri sejauh 8 bit.
b. Fungi g memiliki 4 buah kotak subtitusi yang dibangkitkan oleh kunci.
c. Keluaran fungsi kotak subtitusi dilakukan percampuran linear mengunakan kotak *Most Distance Separable*.
d. Keluaran fungsi g dimasukan ke fungsi transformasi pseudo-Hadamard, kemudian ditambahkan dengan 2 buah 32 bit kunci.
e. Dua buah 32 bit hasilnya kemudian di XOR-kan dengan C dan D. hasil XOR dengan C digeser ke kanan sejauh 1 bit. Dan untuk D sebelum di XOR-kan digeser ke kiri sejau 1 bit.
f. 2 buah 32 bit kiri dan kanan dipertukarkan (A dan B dipertukarkan dengan C dan D).

Langkah diatas dilakukan hingga 16 kali putaran. Kemudian langkah-langkah selanjutnya adalah sebagai berikut :

a. Hasil keluaran setelah diputar sebanyak 16 kali, ditukar lagi (A dan B Pertukarkan dengan C dan D).
b. Hasil dari pertukran tersebut di-XOR-kan dengan 4 buah 32 bit dari kunci menghasilkan cipherteks.

2.6. Kode Wilayah Telepon

Kode Wilayah Telepon digunakan untuk melakukan modifikasi pada kunci *Hill Cipher*. Adapun daftar Kode Wilayah Telepon yang digunakan pada penelitian dapat dilihat pada tabel 1 sebagai berikut:

Tabel 1. Daftar Kode Wilayah Telepon

Kode Wilayah Telepon	Modifikasi	Keterangan Kode Wilayah Telepon
0-4-1-0	1-4-1-1	Makassar, Maros, Sungguminasa
0-4-1-3	1-4-1-3	Bulukumba, Bantaeng
0-4-1-7	1-4-1-7	Malino
0-4-1-9	1-4-1-9	Jeneponto
0-4-2-3	1-4-2-3	Makale, Rantepao
0-4-3-1	1-4-3-1	Manado, Tomohon, Tondano
0-4-3-5	1-4-3-5	Gorontalo, Limboto
0-3-2-5	1-3-2-5	Sangkapura (Bawean)

3. HASIL DAN PEMBAHASAN

3.1. Modifikasi Hill Cipher

a. Enkripsi

Mengenkripsi *plaintext* (KAMI WANITA SOLEHA) dengan menggunakan matriks yang

berdasarkan kepada kode wilayah telepon dengan kunci sebagai berikut:

$$K1 = \begin{matrix}1 & 1\\ 1 & 4\end{matrix} \qquad K5 = \begin{matrix}2 & 1\\ 3 & 4\end{matrix}$$

$$K2 = \begin{matrix}1 & 1\\ 3 & 4\end{matrix} \qquad K6 = \begin{matrix}3 & 1\\ 1 & 4\end{matrix}$$

$$K3 = \begin{matrix}1 & 1\\ 7 & 4\end{matrix} \qquad K7 = \begin{matrix}3 & 1\\ 5 & 4\end{matrix}$$

$$K4 = \begin{matrix}1 & 1\\ 9 & 4\end{matrix} \qquad K8 = \begin{matrix}2 & 1\\ 5 & 3\end{matrix}$$

Berikut langkah penyelesaiannya antara lain:
Langkah Pertama mengubah *plaintext* menjadi deretan angka yang akan ditampilkan pada Tabel 2. *plaintext* menjadi angka

Table 2. *Plaitext* menjadi angka

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Sehingga untuk plaintext terbentuk seperti Tabel 3

Tabel 3. Bentuk baru *plaintext*

K	A	M	I	W	A	N	I	T	A	S	O	L	E	H	A
10	0	12	8	22	0	13	8	19	0	18	14	11	4	7	0

Langkah kedua membagi deretan angka menjadi blok matrix yang sesuai dengan jumlah kolom matriks kunci, seperti pada Tabel 4

Tabel 4. Blok *plaintext*

BLOK 1		BLOK 2		BLOK 3		BLOK 4		BLOK 5		BLOK 6		BLOK 7		BLOK 8	
K	A	M	I	W	A	N	I	T	A	S	O	L	E	H	A
10	0	12	8	22	0	13	8	19	0	18	14	11	4	7	0

Maka didapatkan *plaintext* "K A M I W A N I T A S O L E H A" yang diubah kedalam angka yaitu "10, 0, 12, 8, 22, 0, 13, 8, 19, 0, 18, 14, 11, 4, 7, 0" yang akan di enkripsikan menggunakan algoritma Hill Cipher. Berikut hasil chipertext :

a. Blok 1 (K A)

$$\begin{bmatrix}1 & 1\\ 1 & 4\end{bmatrix}\begin{bmatrix}10\\ 0\end{bmatrix} = \begin{bmatrix}10\\ 0\end{bmatrix} \bmod 26 = \begin{bmatrix}10\\ 10\end{bmatrix} = \begin{bmatrix}K\\ K\end{bmatrix}$$

b. Blok 2 (M I)

$$\begin{bmatrix}1 & 1\\ 3 & 4\end{bmatrix}\begin{bmatrix}12\\ 8\end{bmatrix} = \begin{bmatrix}20\\ 68\end{bmatrix} \bmod 26 = \begin{bmatrix}20\\ 16\end{bmatrix} = \begin{bmatrix}U\\ Q\end{bmatrix}$$

c. Blok 3 (W A)

$$\begin{bmatrix}1 & 1\\ 7 & 4\end{bmatrix}\begin{bmatrix}22\\ 0\end{bmatrix} = \begin{bmatrix}22\\ 154\end{bmatrix} \bmod 26 = \begin{bmatrix}22\\ 24\end{bmatrix} = \begin{bmatrix}W\\ Y\end{bmatrix}$$

d. Blok 4 (N I)

$$\begin{bmatrix}1 & 1\\19 & 4\end{bmatrix}\begin{bmatrix}13\\8\end{bmatrix} = \begin{bmatrix}21\\279\end{bmatrix} \bmod 26 = \begin{bmatrix}21\\19\end{bmatrix} = \begin{bmatrix}V\\T\end{bmatrix}$$

e. Blok 5 (T A)

$$\begin{bmatrix}1 & 1\\23 & 4\end{bmatrix}\begin{bmatrix}19\\0\end{bmatrix} = \begin{bmatrix}19\\437\end{bmatrix} \bmod 26 = \begin{bmatrix}19\\21\end{bmatrix} = \begin{bmatrix}T\\V\end{bmatrix}$$

f. Blok 6 (S O)

$$\begin{bmatrix}3 & 1\\1 & 4\end{bmatrix}\begin{bmatrix}18\\14\end{bmatrix} = \begin{bmatrix}68\\74\end{bmatrix} \bmod 26 = \begin{bmatrix}16\\22\end{bmatrix} = \begin{bmatrix}Q\\W\end{bmatrix}$$

g. Blok 7 (L E)

$$\begin{bmatrix}3 & 1\\5 & 4\end{bmatrix}\begin{bmatrix}11\\4\end{bmatrix} = \begin{bmatrix}37\\71\end{bmatrix} \bmod 26 = \begin{bmatrix}11\\19\end{bmatrix} = \begin{bmatrix}L\\T\end{bmatrix}$$

h. Blok 8 (H A)

$$\begin{bmatrix}3 & 1\\7 & 4\end{bmatrix}\begin{bmatrix}11\\4\end{bmatrix} = \begin{bmatrix}7\\0\end{bmatrix} \bmod 26 = \begin{bmatrix}21\\23\end{bmatrix} = \begin{bmatrix}V\\X\end{bmatrix}$$

Tabel 5. Bentuk *chipertext*

10	10	20	16	22	24	21	19	19	21	16	22	11	19	21	23
K	K	U	Q	W	Y	V	T	T	V	Q	W	L	T	V	X

3.2. Modifikasi Twofish

a. Pembangkitan Kunci

Jumlah kunci internal yang harus dibangkitkan adalah sejumlah 40 kunci masing-masing 32 bit (K0 hingga K39). Dan juga dibutuhkan pembangkitan 4 buah kotak substitusi dari yang bergantung pada kunci. Twofish dapat menerima kunci sepanjang 128, 192 dan 256 bit (N). Kemudian terdefinisi k-N/64. Kunci M terdiri dari 8k byte, m0, ….., mgk-l-. Byte-byte tersebut pertama-tama diubah menjadi 2k buah yang masing-masing terdiri dari 32 bit.

$Mi = \Sigma mm3jj=0\ (4i+j).28j\ i = 0,….,2k - 1$

Hasil fungsi diatas kemudia digolongan menjadi dua buah, ganjil dan genap.

Me = (M0,M2, …, M2k-2)

Mo = (M1,M3, …, M2k-1)

Selanjutnya adalah kotak S. langkah pertama adalah dengan mengelompokkan kunci tersebut dikalikan dengan matriks 4x8 yang diturunkan dari RS. Setiap hasil sepanjang 4 byte diartikan sebagai satu buah 32 bit, menghasilkan kotak S.

Hasil keluaran tahap ini adalah 2 buah matriks, matriks M genap dan matriks M ganjil, dan sebuah matriks kotak substitusi.

b. Pembagian Plaintext

Plaintext dibagai menjadi beberapa blok, setiap blok (P1, …) memiliki panjang 128 bit, kemudian setiap blok dibagi menjadi 4 bagian (K0, K1, K2, K3).

Selanjtnya masing-masing bagian diolah dengan menggunakan proses whitening masukkan terdapat di XOR dengan empat kata kunci. Proses ini akan diikuti oleh 16 putaran.

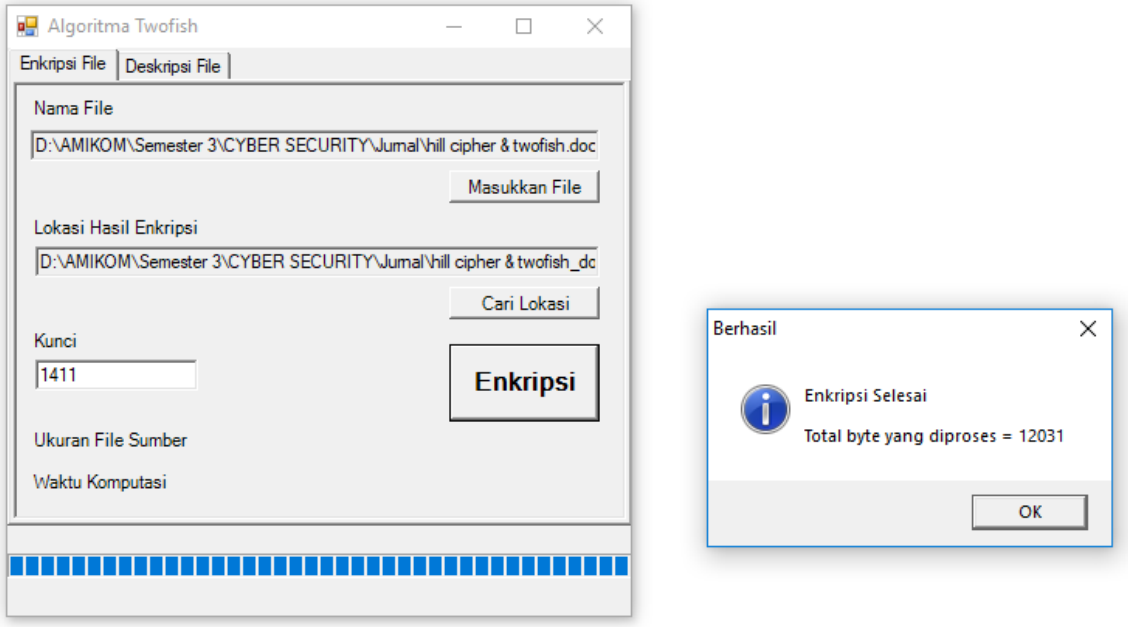
c. Proses Subtitusi

Setelah dibentuk subkey, dilanjutkan dengan melakukan enkripsi plaintext sebanyak 16

putaran dengan operasi :
Li = Ri-1
Ri = Li-1 xor f(Ri-1, Ki)

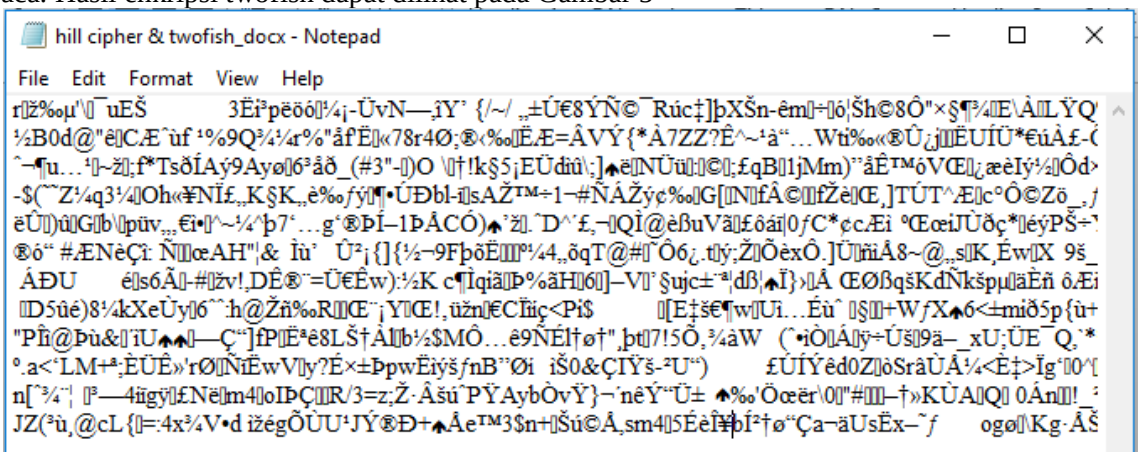
d. Enkripsi

Setelah proses dari awal yaitu enkripsi menggunakan algoritma *hill cipher* selesai dilakukan dengan modifikasi menggunakan kode wilayah telepon, hasil *cipher text* kemudian di enkripsi kembali dengan menggunakan algoritma twofish seperti Gambar 4



Gambar 4 Enkripsi *Twofish*

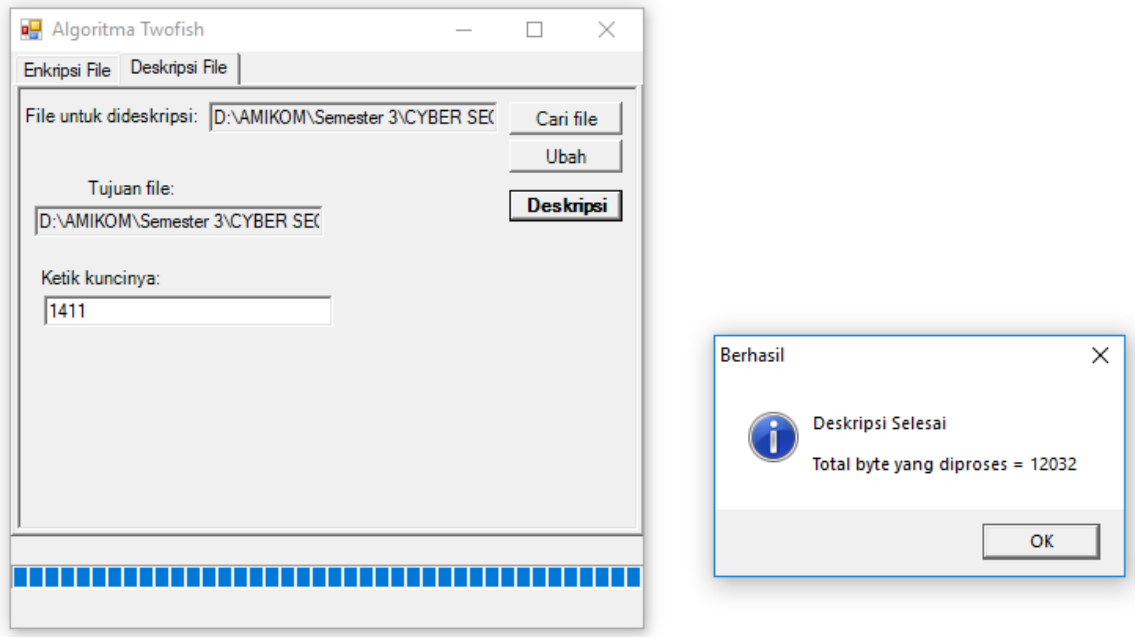
Setelah di enkripsi menggunakan algoritma *Twofish* maka hasil *ciphertext* dari *Hill cipher* akan berubah menjadi file rusak, sehinnga terlindungi dari oleh pihak-pihak yang tidak bertanggung jawab. Hasil enkripsi berupa file rusak ini akan menyulitkan pihak yang tidak berhak dalam membaca informasi yang ada karena simbol yang dihasilkan bersifat acak dan tidak terbaca. Hasil enkripsi twofish dapat dilihat pada Gambar 5



Gambar 5 Hasil Enkripsi *Twofish*

e. Hasil Dekripsi Twofish

Hasil enkripsi dari twofish di dekripsikan kembali untuk mendapatkan file enkripsi dari hill cipher menggunakan algoritma twofish seperti Gambar 6 yang menunjukkan jika dekripsi file berhasil dilakukan dengan memasukkan kembali kunci yang tepat dan *cipher file* yang dihasilkan pada dekripsi ini dapat di ekstraksi *cipher text* untuk kemudian di dekripsi kembali dengan algoritma *hill cipher.*



Gambar 6 Dekripsi *Twofish*

3.3. Proses Dekripsi Hill Cipher

Setelah mendapatkan hasil dekripsi dari twofish " K K U Q W Y V T T V Q W L T V X" kemudian di dekripsikan lagi kedalam Hill Cipher sebagai berikut:

a. Blok 1 (K K)

K1 = $\begin{bmatrix}1 & 1\\ 1 & 4\end{bmatrix}$

1. Det K = (1 x 4) – (1 x 1) = 3
2. Nilai invers Modulo 3^{-1} mod 26

   K = 1 =>> $\frac{26\,(1)+1}{3} = 9$
3. Invers Kunci

   $K^{-1} = \begin{bmatrix}4 & -1\\ -1 & 1\end{bmatrix}$
4. Matriks kunci Hill Cipher

$$9\begin{bmatrix}4 & -1\\ -1 & 1\end{bmatrix} = \begin{bmatrix}(9x4) & (3x(-1))\\ (9x(-1)) & (3x1)\end{bmatrix} \text{Mod } 26$$

$$= \begin{bmatrix}36 & -9\\ -9 & 9\end{bmatrix} \text{ Mod } 26$$

$$= \begin{bmatrix}10 & 17\\ 17 & 9\end{bmatrix}$$

5. Dekripsi

$$\begin{bmatrix}10 & 17\\ 17 & 9\end{bmatrix}\begin{bmatrix}10\\ 10\end{bmatrix} = \begin{bmatrix}(10\ x\ 10) + (17x\ 10)\\ 17\ x\ 10 + (9x\ 10)\end{bmatrix} \text{ Mod } 26$$

$$= \begin{bmatrix}270\\ 260\end{bmatrix} \text{ Mod } 26$$

$$= \begin{bmatrix}10\\ 0\end{bmatrix} = \begin{bmatrix}K\\ A\end{bmatrix}$$

b. Untuk blok 2 – 8 dilakukakan pehitungan yang sama seperti blok 1, sehingga didapatkan hasil dekripsi pada table 6

Tabel 6. Hasil Dekripsi Hill Cipher

Hill Cipher	**BLOK 1**		**BLOK 2**		**BLOK 3**		**BLOK 4**		**BLOK 5**		**BLOK 6**		**BLOK 7**		**BLOK 8**	
Enkripsi	K	K	U	Q	W	Y	V	T	M	F	Q	W	L	T	0	J
	10	10	20	16	22	24	21	19	12	5	16	22	11	19	14	9
Dekripsi	K	A	M	I	W	A	N	I	T	A	S	O	L	E	H	A
	10	0	12	8	22	0	13	8	19	0	18	14	11	4	7	0

Setelah proses dekripsi menggunakan algoritma *Hill Cipher* pada semua blok maka akan didapatkan *plain text* yaitu “KAMI WANITA SHOLEHA”.

3.4. Pengujian Enkripsi dan Dekripsi

Hasil uji coba enkripsi dan dekripsi menggunakan file asli (file sebelum dienkripsi) dokumen dengan *extention *.docx, *.xlsx, *.pptx *.pdf*, yang terdiri dari 8 file. Untuk mengukur kecepatan proses enkripsi dan dekripsi dari Modifikasi Algoritma Hill Cipher dan Twofish Menggunakan Kode Wilayah Telepon yaitu ditujukan pada Tabel 7.

Table 7. Hasil Pengujian Enkripsi dan Dekripsi

No	Nama File	Ukuran File Asli	Hasil Enkripsi		Hasil Dekripsi	
		(Byte)	Ukuran Data (b)	Waktu Proses (s)	Ukuran Data (b)	Waktu Proses (s)
1	Hill cipher & twofish.docx	12,288	12,031	0.05	12.032	0.06
2	Paper Sisfotenika.doc	2,637,824	2,634,752	15.35	2.634.768	15.40
3	Hill Cipher.xlsx	24,576	22,813	1.02	22.816	1.05
4	RTM1_2.xlsx	204,800	201,075	3.08	201.088	3.10
5	Kel.7 Data.pptx	1,024,000	1,023,382	8.25	1.023.392	8.30
6	Tugas RTM2.pptx	565,248	561,346	5.25	561.360	5.27
7	CS_T1A_3A.pdf	135,168	132,282	2.29	132.288	2.31
8	CS_T1B_3A.pdf	331,776	331,381	3.85	331.392	3.90

Berdasarkan tabel 7 dapat telihat bahwa file dengan ukuran yang lebih besar akan diproses lebih lama dibandingkan dengan file yang berukuran lebih kecil.

Keceptan komputasi dalam proses enkripsi dan dekripsi kadang-kadang terdapat perbedaan meskipun di uji dalam satu computer. Hal ini dikarenakan kecepatan computer tidak persis sama dalam setiap detik.

4. KESIMPULAN

Adapun kesimpulan yang diperoleh adalah:

1. Dengan melalui modifikasi algoritma *hill cipher* dan *twofish,* proses enkripsi dan dekripsi *file* sangat bergantung dengan besarnya ukuran *file,* dimana ukuran *file* akan mempengaruhi kecepatan dan jumlah data yang diproses. Semakin besar ukuran *file,* maka akan semakin lama proses enkripsi dan dekripsinya.
2. Twofish memiliki algoritma enkripsi dan penjadwalan kunci yang dibuat berpasangan, perubahan pada satu bagian mempengaruhi bagian lainnya. Hal ini disebabkan tidak cukup jika hanya mendesain fungsi round yang kuat dan menerapkan penjadwalan kunci yang kuat pada fungsi tersebut, keduanya harus dikerjakan bersama.

5. SARAN

Dalam penelitian selanjutnya, dapat diimplemetasikan kombinasi algoritma *hill cipher* yang dimodifikasi dengan menggunakan kode wilayah telepon, dan ditambahkan dalam algoritma *twofish* dalam bentuk aplikasi enkripsi dan dekripsi dengan menggunakan bahasa pemrograman visual basic ataupun bahasa pemrograman lainnya. Aplikasi dapat melakukan enkripsi terhadap file bertipe jpg, mp3, pdf, serta doc.

DAFTAR PUSTAKA

[1] Dony Ariyus, 2008, Pengantar Ilmu Kriptografi: Teori Analisis & Implementasi, Andi Offset.

[2] Donzilio, A. M, 2018, Perbandingan Algoritma DES, AES, IDEA Dan Blowfish dalam Enkripsi dan Dekripsi Data, *Jurnal Teknologi Terpadu*, vol. 4, hal 8-15.

[3] Langit, D. S. P, Dessyanto B. P, Heriyanto, 2013, Aplikasi Enkripsi Dan Dekripsi File Dengan Menggunakan Aes (Advanced Encryption Standard) Algoritma Rijndael Pada Sistem Operasi Android, *TELEMATIKA*, vol.10.

[4] Syahputra, E. R, 2015, Analisa Pengujian Estimasi Waktu Dan Besar Ukuran File Menggunakan Algoritma Twofish Pada Proses Enkripsi Dan Dekripsi, *Jurnal TIMES*, vol IV, hal 14–19.

[5] Pratiwi, Apriyanti E., Lhaksmana, Kemas M., Rizal, Setia, 2011, Implementasi Enkripsi Data Dengan Algoritma Blowfish Pada Aplikasi Email, Jurnal PA : Politeknik Telkom Bandung, vol 1.

[6] Ratih, 2007, Study dan Implementasi Enkripsi Pengiriman Pesan Suara Menggunakan Algoritma Twofish, *Jurnal Teknik Informatika*, vol 3.

[7] Sayuti, A., Habibi, H., Widhiarso, W, 2019, Perbandingan Performa Algoritma Hill cipher dengan RSA dalam proses Enkripsi dan Dekripsi Text.

[8] Hidayat, M. H., Gerhana, Y. A., & Syaripudin, U. 2018. Kombinasi Algoritma Kriptografi Vigenere Chiper dan Hill Cipher untuk Penyandian Pesan Rahasia pada Metode Steganografi, vol 1, hal 125–131.

[9] Imelda, I., Prawira, E., Informatika, T., Informasi, F. T., & Luhur, U. B. 2018. Pengamanan Disposisi Dokumen secara online menggunakan Kriptografi Twofish dan Kompresi Huffman pada CV . TMU, 363–369.