KONSEP PENGGABUNGAN ALGORITHMA VIGENERE DENGAN XTEA BLOK CIPHER UNTUK MENINGKATKAN KEAMANAN DOKUMEN DALAM MATAKULIAH KRIPTOGRAFI

Fathirma'ruf
Dosen Program Studi Pendidikan Teknologi Informasi, STKIP Yapis Dompu
Email: fathir.ntb@gmail.com

Abstract: Security and confidentiality of documents or information has become a very important concern, in this modern era of computing speed increases dramatically, certainly considered threatening for some algorithms that are used to secure documents or information, it spawned an option to increase the security of documents by combining two cryptographic algorithms are Vigenére cipher with XTEA. Selection Vigenére cipher because it is not so vulnerable to solving method code is called frequency analysis, but some cryptanalyst has found security flaws of this algorithm, for it Vigenére cipher in this research carried out modifications to operations of mathematics, the results of these modifications will be combined with the algorithm-based XTEA block cipher, because his strength has been proven to secure the document (text). Based on the results of research conducted, the merger of the two algorithms are (VixTEA) can improve the security of ciphertext, it is measured by various indicators, namely, a visual comparison of encryption (frequency analysis), entropy value analysis, and analysis of bruteforce attacks. The results also showed that the VixTEA concept does not change the performance of the algorithm and the integrity of the digital documents can secured.

Keywords: *Cryptography, Ciphertext, Vigenere cipher, Block cipher, XTEA, VixTEA.*

Abstrak: Keamanan dan kerahasiaan sebuah dokumen atau informasi telah menjadi perhatian yang sangat penting, di jaman modern ini kecepatan komputasi meningkat drastis, tentu dianggap mengancam bagi beberapa algoritma yang digunakan untuk mengamankan dokumen /informasi, hal ini melahirkan opsi untuk meningkatkan keamanan dokumen dengan cara menggabungkan dua algoritma kriptografi yaitu Vigenere cipher dengan XTEA. Pemilihan Vigenere cipher karena dianggap tidak begitu rentan terhadap metode pemecahan sandi yang disebut analisis frekuensi, akan tetapi beberapa kriptanalis telah menemukan celah keamanan dari algoritma ini, untuk itu vigenere cipher dalam penelitian ini dilakukan modivikasi pada operasi matematikanya, hasil modivikasi tersebut akan digabungkan dengan algoritma berbasis blok cipher XTEA karena kekuatannya telah terbukti untuk mengamankan dokumen (text). Dari hasil penelitian yang dilakukan, penggabungan dari kedua algoritma tersebut (VixTEA) dapat meningkatkan keamanan dari ciphertext, hal ini diukur dari beberapa indicator yaitu, perbandingan enkripsi secara visual (analisis frequensi), analisis nilai entropy, dan analisis serangan bruteforce. Hasil penelitian juga menunjukan bahwa penggabungan tersebut tidak merubah performa dari algoritma dan integritas dokumen digital yang diamankan.

Kata kunci*: Kriptografi, Ciphertext, Vigenere cipher, Block cipher, XTEA, VixTEA.*

I. PENDAHULUAN

Bagi sebuah organisasi ataupun setiap individu, keamanan dari sebuah dokumen atau informasi telah menjadi sesuatu yang sangat penting, pengiriman dan penerimaannya dalam suatu jaringan, baik jaringan local maupun jaringan internet akan menimbulkan sebuah resiko terancamnya dokumen tersebut, baik dari pencurian maupun akses illegal dari pihak yang tidak berhak, hal ini dapat merugikan pihak yang mengirim atau yang menerima dokumen tersebut, kerugian yang dimaksud dapat berupa hilang dan bocornya informasi yang bersifat rahasia maupun kerugian secara material. Menurut (Irfan, 2015) Perkembangan teknologi informasi saat ini telah membuat penyimpanan dan transmisi dokumen digital seperti citra, dokumen, video, dan lain-lain menjadi lebih mudah dan efisien, Persoalan yang timbul dari kemudahan ini adalah terdapatnya celah keamanan bagi pihak–pihak yang tidak bertanggung jawab untuk melakukan pencurian terhadap data, baik yang tersimpan dalam harddrive atau yang ditransmisikan. Terkait dengan keamanan dan kerahasiaan dokumen /informasi tersebut memberikan pilihan apakah setiap individu atau organisasi akan melakukan pengamanan terhadap dokumen yang mereka miliki atau tidak, tentunya resiko yang diterima dari setiap pilihan tersebut akan berbeda, teknik dan aktivitas pencurian dokumen memang kerap terjadi terutama di

jaringan internet, aktivitas tersebut secara tidak langsung mengharuskan kepada setiap orang untuk melakukan pengamanan terhadap informasi atau dokumen yang hendak disimpan maupun ditransmisikan.

Menurut (Bhateja, 2015) Algoritma Vigenere cipher adalah algoritma yang termasuk dalam kriptografi simetri klasik dan termasuk dalam cipher abjad-majemuk *(polyalpabetic substitution cipher)*, dan menurut (Niladre, 2012), XTEA adalah algoritma yang termasuk kedalam kriptografi berbasis blok cipher, dan merupakan turunan dari TEA, XTEA memiliki prinsip yang menonjol yaitu *small, secure, simple, and fast*, dan salah satu alasan yang membuat algoritma ini dianggap aman karena dalam penerapannya tidak menggunakan fungsi s-boxes dan permutasian, sehingga terbebas dari analisis frekuensi, dalam penelitian yang ditulis oleh (Youngdai, 2007) mengatakan bahwa XTEA

dengan menggunakan 27 ronde telah dipecahkan, maka penerapan dari XTEA dengan menggunakan 27 ronde sudah tidak direkomendasikan dalam penggunaanya karena telah ditemukan celah pada keamanannya.

Penelitian yang dilakukan oleh Menurut (Irfan, 2015) mengatakan bahwa dengan menggabungkan 2 algoritma dapat meningkatkan keamanan pada dokumen digital khususnya keamanan pada citra, Untuk meningkatkan keamanan yang dimiliki oleh algoritma Vigenere cipher maka dalam penelitian ini akan dilakukan modivikasi dengan menambahkan fungsi matematika dalam operasinya, pada penerapannya untuk mengamankan dokumen, ciphertext yang dihasilkan oleh algoritma Vigenere cipher hasil modivikasi akan dilakukan pengamanan kembali dengan menggunakan XTEA 32 ronde, dengan demikian ciphertext yang diperoleh dapat ditingkatkan keamanannya karena telah di enkripsi sebanyak 2 kali menggunakan dua algoritma, dalam konsep penggabungan algoritma yang diusulkan (VixTEA) akan memiliki 3 keamanan utama yaitu kunci Vigenere, nilai integer Z dan kunci XTEA.

A. Vigenere Chiper

Dalam penelitian yang dilakukan oleh (Hatipoglu, 2008), mengatakan bahwa algoritma kriptografi klasik Vigenere cipher termasuk dalam abjad majemuk *(Polyalphabetic substitution Cipher)* yang dipublikasikan oleh diplomat sekaligus seorang kriptologis yang berasal dari Prancis, Blaise de Vigenere pada abad 16 (tahun 1586), para peneliti telah menerapkan sebuah konsep yang terinspirasi dari alam untuk pembacaan sandi dari kriptografi klasik dan mengklaim keberhasilan, menurut (Spillman, 1993) penggunaan algoritma genetika dapat dilakukan untuk pembacaan sandi sederhana pada cipher substitusi, Proses enkripsi dan dekripsi plaintext yang dilakukan, menggunakan rumus sebagai berikut:

Enkripsi

$$C_i = P_i + K_{i(\mathrm{mod}\ n)} \ (\mathrm{mod}\ 26) \quad (1)$$

Dekripsi

$$P_i = C_i - K_{i(\mathrm{mod}\ n)} \ (\mathrm{mod}\ 26) \quad (2)$$

Contoh: plaintext “CRYPTOGRAPHY” dengan kunci “KLASIK”.

Plaintext	: C R Y P T O G R A P H Y
Key	: K L A S I K
Ciphertext	: L C A H B Y Q C A H P I

Menurut (Stallings, 2006) In Vigenere cipher each plaintext letter has multiple corresponding ciphertext letters, which makes cryptanalysis harder with more alpha ets to guess and flatter frequency distribution, Rumus enkripsi dan dekripsi yang disampaikan diatas, merupakan rumus dasar dari algoritma Vigenere cipher yang menggunakan modulo 26, akan tetapi dalam penelitian ini menggunakan modifikasi dari rumus tersebut dan menggunakan kode ASCII yang berjumlah 256 yang diadopsi dari source code algoritma berbasis *Polyalphabetic cipher*, yaitu:

Enkripsi

$$C_i = P_i + K_i - Z \ (\mathrm{mod}\ 256)$$

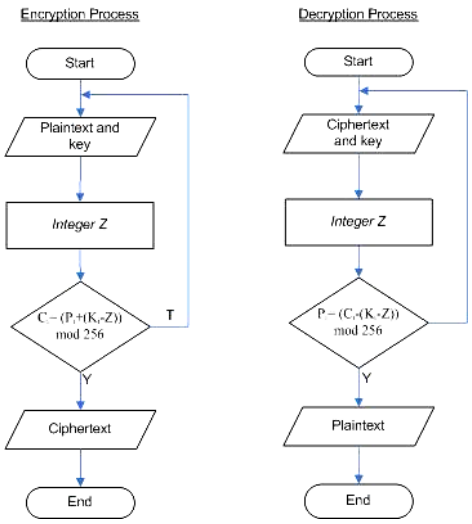
Dekripsi

$$P_i = C_i - K_i - Z \ (\mathrm{mod}\ 256)$$

Contoh: plaintext “CRYPTOGRAPHY” dengan kunci “KLASIK”.

Plaintext	: C R Y P T O G R A P H Y
Key	: K L A S I K
Z	: 29
Ciphertext	: V f n f k g ` l \ l [m

Implementasi dari vigenere cipher hasil modivikasi tersebut menunjukan bahwa, jangkauan karakter menjadi luas sesuai dengan kode ASCII, keamanan yang dimiliki bukan hanya terletak pada kunci, tetapi berada pada nilai Z juga, berikut ini alur dari enkripsi/dekripsi dari vigenere cipher yang telah di modivikasi:



Gambar 1. Proses Enkripsi dan Dekripsi Vigenere Cipher

Keterangan:

P_i = Plaintext ke-*i*

C_i = Ciphertext ke-*i*

K = Kunci ke-*i*

Z = Nilai integer positif yang diberikan untuk kunci ke-*i*

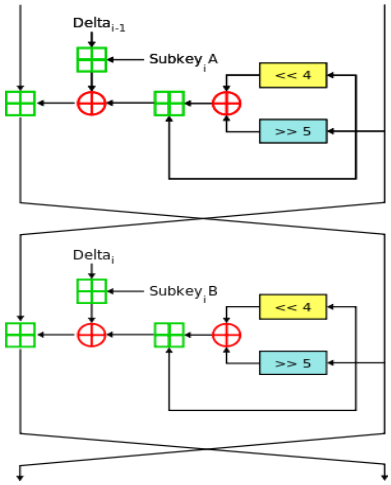
Mod 256 = Jumlah dari Kode ASCII standar

Berdasarkan alur pada proses enkripsi yang ada pada gambar diatas, menjelaskan tahapan dalam mengubah sebuah dokumen (plaintext) menjadi sebuah ciphertext yaitu dimulai dari meng-inputkan plaintext dan kunci, lalu menentukan nilai integer positif Z yang diberikan untuk sub-kunci sebelumnya, selanjutnya masuk kepada tahapan inti dari algoritma ini yaitu menerapkan rumus Ci = Pi + Ki – Z mod 256, dimana, hasil yang diperoleh dari implementasi rumus tersebut adah berupa sebuah ciphertext.

Proses enkripsi yang dilakukan diatas adalah proses dimana bertujuan untuk merusak sebuah text agar tidak dapat diketahui oleh orang lain, Sedangkan untuk melakukan perbaikan terhadap text yang telah di rusak tersebut, maka dilakukan sebuah tahapan dekripsi terhadap ciphertext tersebut (Stallings, 2006) yaitu, dengan meng-inputkan ciphertext dan kunci awal yang sebelumnya dilakukan untuk enkripsi, lalu memberikan nilai integer positif Z untuk sub-kunci sebelumnya, dan tahapan selanjutnya yaitu menerapkan rumus dekripsi yaitu: Pi = Ci – Ki - Z mod 256, dimana hasil yang diperoleh dari proses implementasi rumus tersebut adalah berupa sebuah plaintext awal sebelum dilakukan enkripsi.

B. eXtended Tiny Encryption Algorithm (XTEA)

XTEA adalah algoritma blok cipher simetris yang dirancang untuk memperbaiki kelemahan yang terdapat pada TEA, algoritma ini beroperasi dalam ukuran blok 64 bit dan panjang kunci 128 bit (Wheeler, 2009), dalam implementasinya XTEA akan membagi kedalam 2 blok plaintext masing-masing bernilai 32 bit untuk blok z dan 32 bit untuk blok y, sedangkan untuk kunci yang bernilai 128 bit akan dibagi kedalam 4 blok sub kunci K[0]=32 bit, K[1]=32 bit, K[3]=32 bit dan K[4]= 32 bit [9], bentuk dari jaringan Feistel milik XTEA hampir sama dengan jaringan Feistel milik TEA, menurut (Niladree, 2012) yang membedakan antara XTEA dengan TEA adalah fungsi Feistel dan penjadwalan kunci yang digunakan. pada round ganjil digunakan K[sum & 3], sedangkan pada round genap digunakan K[sum >> 11 & 3], seperti yang ditunjukan pada gambar berikut (Gaba, 2012):



Gambar 2. Satu Rounde Model Enkripsi XTEA

Penelitian yang dilakukan oleh [4] Dalam implementasinya XTEA menggunakan nilai $delta\ (\sqrt{5} - 1)2^{31}$ dan secara konstan nilai delta tersebut di rubah ke nilai Heksadesimal yaitu: 9E3779B9, berikut ini adalah operasi matematika pada proses enkripsi XTEA:

Round 0:

y+= (z << 4 ^ z >> 5) + z ^ sum + k[sum & 3];
sum += delta;

Round I:

z+= (y << 4 ^ y >> 5) + y ^ sum + k[sum >> 11 & 3];

Tahapan yang dilalui untuk melakukan dekripsi terhadap *ciphertext* hasil enkripsi yaitu menggunakan tahapan yang sama dengan proses enkripsi diatas dengan ketentuan 32 kali putaran atau 64 round, dengan menggunakan operasi sebagai berikut:

Round 0:

z-= (y << 4 ^ y >> 5) + y ^ sum + k[sum >> 11 & 3];
sum -= delta;

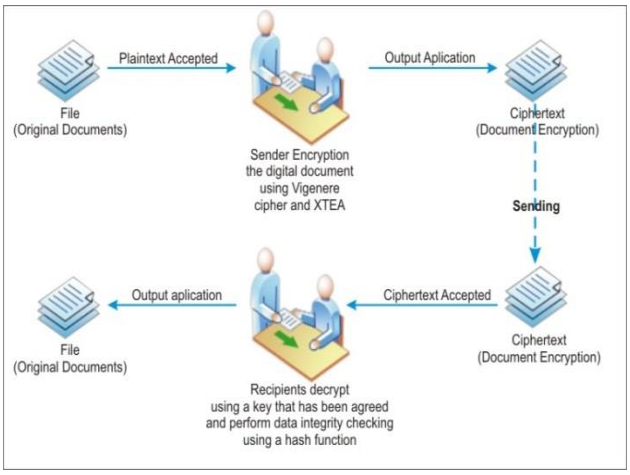
Round I:

y-= (z << 4 ^ z >> 5) + z ^ sum + k[sum & 3];

Dalam tulisan yang dilakukan oleh (Wheller, 2009) putaran yang direkomendasikan dalam penggunaan XTEA adalah 32 siklus atau 64 round, karena beberapa kriptanalis telah menemukan celah keamanan dari penggunaan XTEA dengan round dibawah 32 siklus.

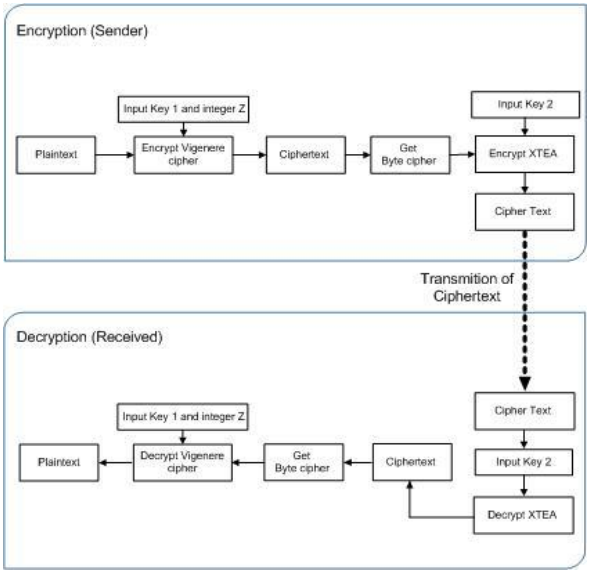
II. METODE PENELITIAN

Contoh dari pentingnya pengamanan dari sebuah dokumen digital adalah ketika terdapat sebuah dokumen yang bersifat pribadi atau sangat rahasia dari seseorang atau sebuah institusi yang tidak menginginkan dokumen tersebut diketahui oleh orang lain atau pihak yang tidak berkepentingan, baik dalam penyimpanannya maupun dalam mentransmisikannya. Gambaran umum penggunaan enkripsi ganda pada sebuah dokumen dalam dunia nyata dapat dilihat pada skenario penggunaan enkripsi seperti pada gambar berikut:



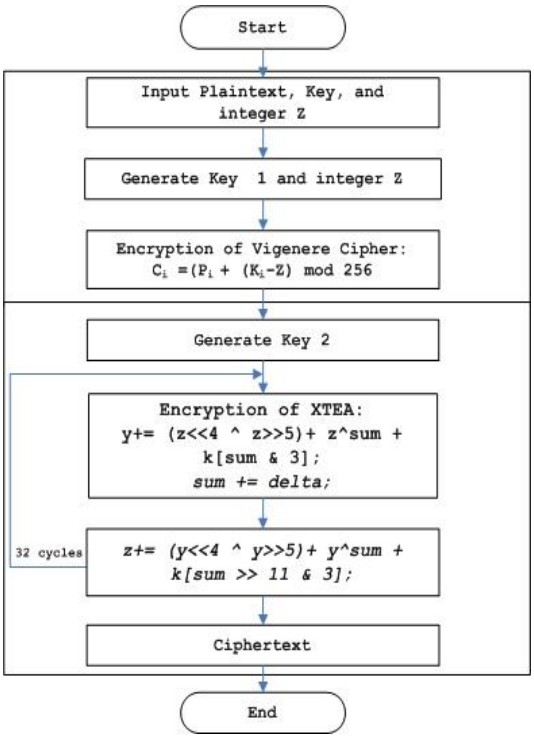
Gambar 3. Skenario Enkripsi Ganda VixTEA

Pada gambar 3 diatas diberikan sebuah contoh, dimana seorang pengguna ingin mengirimkan sebuah dokumen digital yang memiliki informasi penting kepada rekan kerjanya melalui jaringan publik yang tentunya rawan terhadap penyadapan atau pengaksesan oleh pihak lain. Untuk menjaga kerahasiaan dan keamanan pada dokumen yang dikirim, maka perlu dilakukan enkripsi ganda pada dokumen tersebut sehingga dokumen digital yang dikirimkan tidak dapat dikenali sebagai sebuah informasi penting melainkan sebuah ciphertext yang tidak memiliki makna, karena telah dilakukan pengacakan yang menyertakan kode-kode aneh yang terdapat pada kode ASCII yang berjumlah 256 karakter dan tentunya informasi yang terdapat pada dokumen digital yang dikirim akan aman dari pengaksesan oleh pihak yang tidak berwenang. Rancangan enkripsi ganda hasil penggabungan dari algoritma Vigenere cipher dan XTEA yang akan dibangun pada penelitian ini secara umum dijelaskan pada gambar 4 berikut:



Gambar 4. Desain Proses Enkripsi dan Dekripsi VixTEA

Rancangan diatas akan diimplementasikan kedalam sebuah aplikasi enkripsi/dekripsi, atau dalam konsep baru yang diberi nama VixTEA, dan secara khusus untuk rancangan skema enkripsi dan dekripsi dari konsep VixTEA akan dijelaskan kembali pada gambar 5 dan 6 berikut:

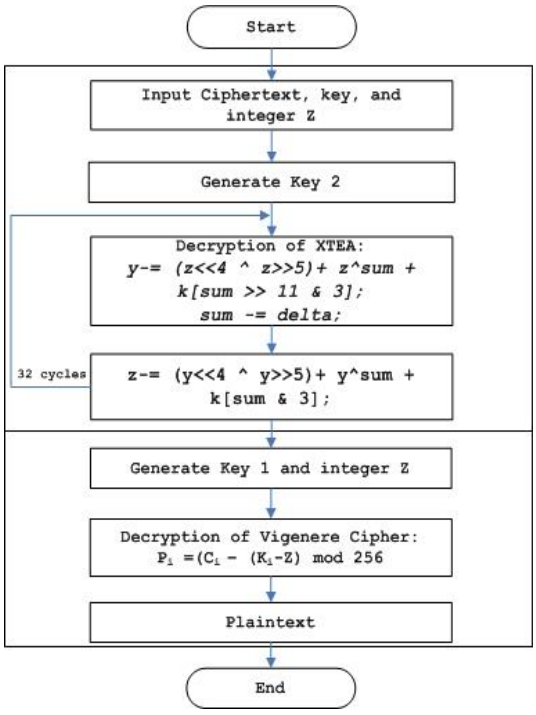


Gambar 5. Desain Proses Enkripsi VixTEA

Penjelasan dari proses enkripsi pada gambar 5 diatas yaitu:

1. Input plaintext (dokumen), kunci 1 (Kunci vigenere) dengan panjang n≤256, kunci 2 (Kunci XTEA) dengan panjang 16 karakter, atau 128 bit, dan nilai Z.
2. Generate kunci 1 dan nilai Z.
3. Enkripsi Vigenere cipher dengan rumus $C_i = P_i + K_i – Z \bmod 256$.
4. Generate kunci 2.
5. Sebelum melakukan enkripsi dengan XTEA terlebih dahulu melakukan pembagian hasil enkripsi dari Vigenere cipher kedalam 2 blok plaintext yaitu blok y dan blok z, yang masing-masing berisi 32 bit, dan membagi kunci kedalam 4 blok kunci yaitu K[0], K[1], K[2], K[3], yang juga masing-masing bernilai 32 bit.
6. Enkripsi *XTEA* dengan rumus: *y+= (z << 4 ^ z >> 5) + z ^ sum + k[sum & 3]; sum += delta;* untuk setiap round genap dan menggunakan rumus: *z+= (y << 4 ^ y >> 5) + y ^ sum + k[sum >> 11 & 3];* untuk setiap round ganjil.
7. Tahapan nomor 6 dan 7 dilakukan pengulangan sebanyak 32 kali, untuk mendapatkan ciphertext.

Sedangkan untuk rancangan dari skema dekripsi yang akan di bangun secara khusus kembali digambarkan pada gambar 6 berikut:



Gambar 6. Desain Proses Dekripsi VixTEA

Penjelasan dari proses dekripsi pada gambar 6 diatas yaitu:

1. Input ciphertext (dokumen), kunci 2 (Kunci XTEA) dengan panjang 16 karakter, atau 128 bit, dan nilai Z.
2. Generate kunci 2.
3. Sebelum menerapkan rumus dekripsi XTEA terlebih dahulu melakukan pembagian plaintext kedalam 2 blok plaintext yaitu blok y dan blok z, yang masing-masing bernilai 32 bit, dan membagi kunci kedalam 4 blok kunci yaitu K[0], K[1], K[2], K[3], yang juga masing-masing bernilai 32 bit.
4. Dekripsi XTEA dengan rumus: *z-= (y << 4 ^ y >> 5) + y ^ sum + k[sum >> 11 & 3]; sum -= delta;* untuk setiap round genap dan menggunakan rumus: *y-= (z << 4 ^ z >> 5) + z ^ sum + k[sum & 3];* untuk setiap round ganjil.
5. Generate kunci 1 dan nilai Z.
6. Dekripsi Vigenere cipher dengan rumus: $P_i = C_i – K_i - Z \bmod 256$.

Tahapan nomor 3 dan 4 dilakukan pengulangan sebanyak 32 kali, untuk mendapatkan kembali plaintext

Untuk berbagai alasan, keamanan dan kerahasiaan sebuah informasi sangatlah dibutuhkan dalam komunikasi data, terdapat berbagai cara untuk menjamin keamanan dan kerahasiaan dalam komunikasi data, diantaranya adalah dengan seni pengacakan data atau disebut juga dengan kriptografi, menurut (Hatipoglu, 2008) Bidang ilmu kriptografi memiliki sejarah yang sangat menarik, bidang ilmu ini sudah digunakan sejak 4000 tahun yang lalu, diperkenalkan oleh bangsa mesir untuk mengirimkan pesan kepada pasukan militer yang berada di medan perang. dalam konsep kriptografi terdapat istilah enkripsi atau pengacakan data, yang bertujuan untuk melakukan pengamanan data yang dapat memberikan layanan untuk memenuhi beberapa aspek keamanan.

III. HASIL DAN PEMBAHASAN

Percobaan yang dilakukan menggunakan konsesp hasil penggabungan algoritma, (VixTEA), jenis file dokumen digital yang digunakan yaitu berupa file dengan berbagai ekstensi, diantaranya .pdf, .mp4, .docx, .pptx, .jpeg, dan .txt. Tahapan ini akan dilakukan beberapa hal terkait dengan ujicoba dan analisis pada masing-masing algoritma dan hasil penggabungan, diantaranya yaitu:

- Memberikan perbandingan hasil enkripsi secara visual dari setiap algoritma
- Melakukan enkripsi pada beberapa file dokumen dengan menggunakan aplikasi yang mengadopsi konsep algoritma Vigenere cipher, XTEA dan VixTEA untuk mengetahui nilai hasil analisis Entropy, hasil analisis serangan bruteforce, performa algoritma dan pengujian terhadap integritas dari dokumen digital hasil dekripsi.

Untuk mengetahui perbandingan antara hasil enkripsi secara visual dari masing-masing algoritma sebelum dan setelah dilakukan penggabungan disajikan dalam tabel berikut ini:

Tabel 1. Komparasi Hasil Enkripsi VixTEA

Original File	Vigenere	XTEA	VixTEA
1.....Ê.2.. .....ø..... ...‡i..... .....'..t° ê.....	×ØÏãÑÒÔÎ×é×ÛÏÐÑÓ ÓÕÕ^ÃÎÔÑÒÓÕÕÕàä ¹iÑÛÓÔÝã×ØÏÞÑÒG„ ñÃ×ØÏØÑÒÓÕÕ×ØÏÐ ÑÒÓÕÕ×ØÏÐÑÒÓÕÕ ×ØÏÐÑÒÓÕÕ×ØÏÐÑÒ	Nò¨)Åá‡ôÐ[×:ø„'´ .hiûœ£»´fáŠ#i,…· >¤Ã–äKdi{ÚûBŽ7%Ï ÝYÛwý5Ÿ.gDQ/þè«– gDQ/þè«–gDQ/þè«– gDQ/þè«–gDQ/þè«– gDQ/þè«–gDQ/þè«–	ÿ:.?ž`ªÿ¤°Îþ–Ál[' dW¾Æ…:…^&.%S.E ïtgíŸé¼.“d § @!X •Ð9.Ä¤.è.SA$…–¾M *8².¶ªLÿä .fB.öŒ OBŠ(”)E¦.o,=úO ì t6)V').÷ Xô JÍ,9

Tabel perbandingan hasil enkripsi diatas menjelaskan bagaimana ciphertext yang dihasilkan dari masing-masing algoritma sebelum dan setelah dilakukan penggabungan, dalam percobaan yang dilakukan diatas menggunakan sebuah file dokumen yang berekstensi .txt, dokumen yang dijadikan sebagai contoh tersebut adalah sebuah dokumen yang berisi banyak karakter yang sama, karakter yang dimaksud yaitu adalah karakter (titik), dari ujicoba secara visual tersebut, terlihat ciphertext yang dihasilkan oleh algoritma Vigenere cipher dan XTEA mengulang beberapa karakter yang sama di (tiga baris terakhir), sedangkan ciphertext yang dihasilkan dari konsep VixTEA tersebut tidak terdapat pengulangan karakter yang sama di setiap barisnya, hal ini menunjukan bahwa tingkat pengacakan yang dilakukan oleh konsep penggabungan (VixTEA) lebih baik dari pada ciphertext yang dihasilkan dari masing-masing algoritma tersebut. Sedangkan untuk mengetahui tingkat keamanan dan performa dari hasil penggabungan algoritma, dilakukan beberapa analisis sebagai berikut:

A. Analisis Entropy

Menurut penelitian yang dilakukan oleh [12], Nilai entropy ideal jika sebuah informasi dienkripsi dan dalam kondisi teracak sempurna adalah 7,99902 (~8). Dengan demikian sistem yang dirancang aman dari serangan entropy. Namun jika nilai entropy lebih kecil dari 8, dapat dikatakan sistem enkripsi masih dapat ditebak, entropy dari ciphertext dapat dihitung menggunakan rumus berikut:

$$H_e = -\sum_{k=0}^{G-1} P(k) \log_2\big(P(k)\big)$$

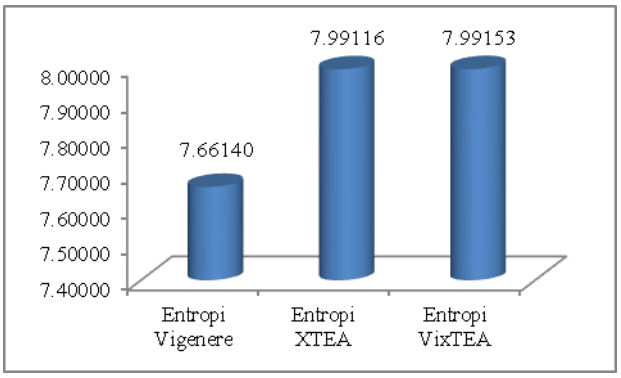
Dimana:

H_e : Nilai entropy
G : Jumlah karakter yang digunakan (kode ASCII)
P(k) : Peluang kemunculan symbol ke-*k*

Tabel 2. Perbandingan Nilai Entropy antar Algorithma

No	File	Size	Vigenere	XTEA	VixTEA
1	Begin.pdf	31.6 MB	7.99045	7.99981	7.99995
2	Dual.mp4	33.6 MB	7.99999	7.99999	7.99999
3	Mtra.docx	17.8 MB	7.97496	7.99927	7.99993
4	Mod.pptx	23.5 MB	7.99944	7.99999	7.99999
5	Mou.jpeg	1.90 MB	7.99344	7.99915	7.99984
6	Cont.txt	3.59 KB	6.01011	7.94875	7.94946
Average			**7.66140**	**7.99116**	**7.99153**

Tabel 2 diatas memperlihatkan bahwa nilai entropy sebelum dan setelah dilakukan penggabungan algoritma, terjadi peningkatan dari rata-rata entropy untuk algoritma Vigenere cipher yaitu **7.66140**, XTEA **7.99116**, dan nilai entropy VixTEA menjadi **7.99153,** Nilai entropy yang terdapat pada table II diatas digambarkan kembali dalam grafik berikut:



Gambar 7. Grafik Analisis Entropy

Dalam grafik yang ditunjukan pada gambar 7 diatas terlihat nilai entropy dari Vigenere cipher begitu rendah, sedangkan nilai entropy dari XTEA hampir memiliki kesamaan dengan entropy VixTEA, akan tetapi antara keduannya memiliki nilai yang berbeda walaupun tidak meningkat secara signifikan, dari data yang disajikan diatas dapat dipetik kesimpulan bahwa setelah dilakukan penggabungan antara kedua algoritma tersebut dapat meningkatkan nilai entropy dari ciphertext yang dihasilkan, dan tentu hal ini dianggap hasil penggabungan lebih siap untuk menghadapi serangan entropy, Berdasarkan teori yang disampaikan oleh (Wheller, 2009), konsep enkripsi ganda yang dirancang ini dianggap aman dari serangan entropy atau sulit ditebak oleh kriptanalis karena nilai entropy yang terdapat pada dokumen hasil enkripsi mengalami peningkatan dari

sebelum dilakukan penggabungan, dan berada dalam keadaan teracak sempurna.

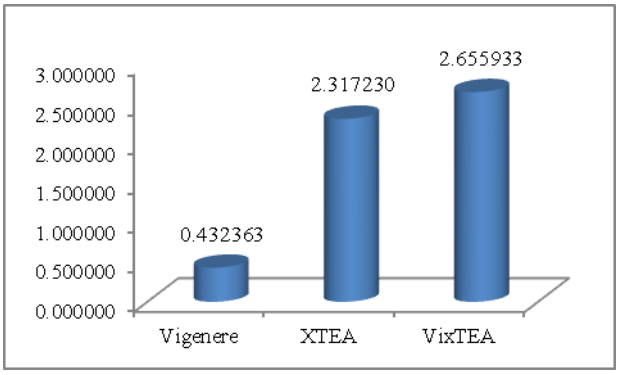
B. Analisis Waktu Enkripsi

Untuk mengetahui performa antar algoritma baik sebelum, maupun setelah dilakukan penggabungan terkait dengan waktu enkripsi jelaskan dalam tabel III berikut:

Tabel 3. Hasil Analisa Waktu Enkripsi Antar Algorithma

No	File	Size	Encrypt time (in seconds)		
			Vigenere	*XTEA*	*VixTEA*
1	Begin.pdf	31.6 MB	0.610179	3.992444	4.845577
2	Dual.mp4	33.6 MB	0.640530	4.331984	4.720395
3	Mtra.docx	17.8 MB	0.550764	2.378419	2.708127
4	Mod.pptx	23.5 MB	0.708328	2.954658	3.355831
5	Mou.jpeg	1.90 MB	0.084031	0.245188	0.304957
6	Cont.txt	3.59 KB	0.000346	0.000687	0.000708
Rata-rata			**0.432363**	**2.317230**	**2.655932**

Tabel 3 diatas menjelaskan bahwa rata-rata waktu yang dibutuhkan untuk melakukan enkripsi dengan jumlah dan kapasitas file yang sama menggunakan algoritma Vigenere cipher membutuhkan waktu 0.432363 detik, dan XTEA 2.317230 detik, sedangkan waktu enkripsi dari *VixTEA* yaitu 2.655932 detik, Informasi pada table III diatas digambarkan kembali dalam grafik berikut ini:



Gambar 8. Grafik Waktu Enkripsi Antar Algorithma

Jika di skenariokan, pengguna melakukan enkripsi secara terpisah dari masing-masing algoritma dan aplikasi, dengan enkripsi pertama menggunakan Vigenere cipher dan kemudian enkripsi yang kedua menggunakan XTEA berarti waktu enkripsi yang diperoleh akan lebih lambat yaitu 2.749593 detik (waktu tersebut diperoleh dari penjumlahan rata-rata waktu enkripsi Vigenere cipher dan XTEA) dengan jumlah dan ukuran file yang sama, dibandingkan dengan menggabungkan keduanya didalam satu aplikasi seperti pada konsep *VixTEA*, Berdasarkan data hasil analisis waktu enkripsi diatas, diperoleh kesimpulan bahwa setelah dilakukan penggabungan, tidak merubah performa algoritma menjadi lebih lambat dalam melakukan enkripsi, terbukti dari hasil pengujian diatas waktu enkripsi yang diperoleh dari *VixTEA* hanya membutuhkan 2.52517 detik.

C. Analisis Serangan Bruteforce

Rumus yang digunakan adalah sebagai berikut (Irfan, 2015).

Jumlah Kunci = $r \wedge n$

Dimana:

r : Jumlah kemungkinan kunci
n : Jumlah karakter yang digunakan

Untuk melakukan bruteforce pada Vigenere cipher, parameter kunci yang digunakan untuk melakukan enkripsi bernilai n (tidak diketahui jumlah karakternya), Semua karakter kunci yang digunakan berupa huruf dan angka sesuai dengan kode ASCII yang berjumlah 256 karakter, maka rincian dari rumus diatas yaitu:

r = (Jumlah kemungkinan kunci = 12 karakter (dimisalkan))
n = (Jumlah karakter yang digunakan = 256)
Jumlah Kombinasi Kunci = 256^{12}
= 25.106.405.242 tahun

Setelah dilakukan modifikasi pada algoritma Vigenere cipher, maka diketahui bahwa, dalam penerapannya kekuatan dari algoritma ini bukan hanya terdapat pada panjang kunci 256^n tetapi juga terdapat pada nilai integer untuk setiap kunci ke-i dengan jumlah kemungkinan $Z=10^3$, sedangkan untuk melakukan *bruteforce* pada XTEA, parameter kunci yang digunakan untuk melakukan enkripsi bernilai 128 bit, Semua karakter kunci yang digunakan berupa huruf dan angka sesuai dengan kode ASCII yang berjumlah 256 karakter, maka rincian dari rumus diatas yaitu:

r = (Jumlah kemungkinan kunci = 16 karakter (128 bit))
n = (Jumlah karakter yang digunakan = 256)
Jumlah Kombinasi Kunci = 256^{16}
= 1.078.311.894.384 tahun

Setelah dilakukan penggabungan terhadap dua algoritma tersebut maka kriptanalis yang melakukan serangan *bruteforce* haruslah terlebih dahulu menembus 3

(tiga) pertahanan yang terdapat pada ciphertext, seperti yang dikatakan oleh rumus berikut:

Jumlah kemungkinan: $256^n + 10^3 + 256^{16}$
Lama waktu yang dibutuhkan: $26{,}2 \times 10^{12}$

Dari data percobaan perhitungan diatas, terlihat waktu yang dibutuhkan untuk melakukan percobaan dekripsi menggunakan metode bruteforce sangat lama atau tidak mungkin untuk dilakukan. Sehingga dapat diambil kesimpulan bahwa penerapan algoritma ganda pada dokumen digital (Plaintext) dapat menghasilkan ciphertext yang aman dari serangan bruteforce.

D. Uji Integritas data

Pengujian integritas terhadap dokumen hasil dekripsi, dilakukan dengan tujuan untuk mengetahui apakah terdapat perubahan terhadap sebuah file yang yang di dekripsi atau tidak, pengujian integritas dari dokumen digital dengan konsep enkripsi ganda masih tetap terjaga, hal ini ditunjukan dengan pencocokan nilai *hash* dari dokumen hasil dekripsi dengan nilai *hash* dari dokumen original, setelah dilakukan uji perbandingan dapat disimpulkan bahwa pengacakan (enkripsi) yang dilakukakan oleh algoritma hasil penggabungan ini dapat mengembalikan file kedalam bentuk semula tanpa terdapat perubahan asalkan keseluruhan dari kunci yang digunakan tidak mengalami perubahan

IV. KESIMPULAN DAN SARAN

A. Simpulan

Konsep pengamanan dokumen digital yang diusulkan yaitu dengan melakukan enrkipsi/dekripsi ganda dari dua algoritma yaitu Vigenere cipher dan XTEA. Implementasi penggabungan dari dua algoritma tersebut akan diterapkan pada sebuah aplikasi yang dibangun dengan bahasa pemrograman C#. konsep VixTEA dapat meningkatkan keamanan dokumen hasil enkripsi menjadi lebih baik, dibuktikan dari indicator hasil analisis entropy, analisis serangan bruteforce. Sedangkan untuk hasil pengujian terhadap performa algoritma yang di dasarkan dari parameter waktu enkripsi diperoleh kesimpulan bahwa setelah dilakukan penggabungan tidak merubah performa algoritma, dan hasil penelitian juka menunjukan, bahwa konsep VixTEA tidak merubah integritas dari dokumen.

B. Saran

Konsep penggabungan antar algoritma klasik Vigenere cipher dan XTEA dirasakan masih terdapat kekurangan, karena terbatasnya penggunaan kunci dari masing-masing algorithma, untuk itu diharapkan pengembangan lebih lanjut dapat digabungkan dengan algorithma modern seperti halnya ELGAMAL.

DAFTAR RUJUKAN

A. Jolfaei A, and A. Mirghadri, “Image Encryption Using Chaos and Block Cipher,” Computer and Information Science. 4:1, 2011.

A. K. Bhateja. A, A. Bhateja, S. Chaundhury, and P. K. Saxena, “Cryptanalysis of Vigenere cipher using Cuckoo Search,” Applied Soft Computing, vol. 26, pp. 315-324, 2015.

B. Hatipoglu, (2008). A Wireless Entryphone System Implementation With MSP430 and CC1100. Faculty of Engineering and Architecture Department of Komputer Engineering. Yetipede University, Unpublished.

D. J. Wheeler, and R. Needham, “TEA Extensions”, Unpublished.

D. J. Wheeler, and R. Needham, TEA, “a tiny encryption algorithm,” Unpublished.

D. Tom. St, “Extended TEA Algorithms, Unpublished.

J. Niladree. D, “A Modified XTEA,” International Journal of Soft Computing and Engineering (IJSCE), Vol. 2 (2), pp 461-464, 2012.

K. Youngdai, H. Seokhie, L. Wonil, L. Sanjin, and K. Ju-sung, “Related Key Differential Attacks on 27 rounds of XTEA anf Full-round GOST,” Unpublished.

P. Irfan, Y. Prayudi. and I. Riadi. “Image Encryption using Combination of Chaotic System and Rivers Shamir Adleman (RSA),” International Journal of Computer Applications, Vol. 123 (6), pp. 0975-8887, 2015.

R. Spillman, M. Janssen, B. Nelson, and M. Kepner, “Use of a genetic algorithm in the cryptanalysis of simple substitution ciphers,” Cryptologia, vol. 17 (1), pp. 31–44, 1993.

S. Gaba, I. Aggarwal, and S. Pandey, “Design of Efficient XTEA Using Verilog” IJSRP, vol. 2 (6), pp. 1-5, 2012.

W. Stallings, Cryptography and Network Security : Principles and Practices, Prentice-Hall, Upper Saddle River, New Jersey, 2006..