MODIFIKASI NEW PDAC (*PARALLEL ENCRYPTION WITH DIGIT ARITHMETIC OF COVER TEXT*)

Widiyanto Tri Handoko[1], Eka Ardhianto[2], Edy Supriyanto[3]
[1,2,3]Program Studi Teknik Informatika, Fakultas Teknologi Informasi, Universitas Stikubank
e-mail: [2]ekaardhianto@edu.unisbank.ac.id

Abstrak

Teknik pengamanan data merupakan hal penting dalam proses enkripsi. Salah satu hal yang menjadikan penting adalah aspek jumlah kapasitas data yang mampu diamankan. Semakin besar jumlah data yang dapat diamankan maka akan lebih banyak informasi yang akan disembunyikan dari pihak yang tidak berhak. Tujuan dari penelitian ini adalah bagaimana meningkatkan kapasitas penyembunyian informasi dengan menambah jumlah kunci dan meminimalkan stego kunci dalam New PDAC. Dalam penelitian ini pembangkitan kunci digunakan operasi matematika penjumlahan, pengurangan, perkalian dan nilai maksimum dari kode ASCII stego kunci. Hasil dari penelitian ini adalah adanya peningkatan kapasitas informasi yang dapat diamankan dengan menggunakan satu stego kunci.

***Kata Kunci**: data security, data hiding, steganography, pdac, new pdac.*

1. PENDAHULUAN

Informasi hingga saat ini masih terus masih ditingkatkan model kemananannya pada berbagai bidang. Dalam melakukan pengamanan data teknik kriptografi menerapkan proses enkripsi dan dekripsi untuk mengubah data menjadi sesuatu yang tidak dapat dikenali dan mengembalikan kembali menjadi keadaan semula [1]. Meskipun demikian serangan terhadap sebuah informasi masih dapat terjadi. Seharusnya sebuah mekanisme keamanan memberikan rasa aman kepada pengguna dalam mengamankan informasi baik dalam masa penyimpanan maupun dalam pengiriman informasi tersebut kepada pihak penerima. Steganography adalah sebuah ilmu, teknik atau seni menyembunyikan sebuah pesan rahasia dengan suatu cara sehingga pesan tersebut hanya akan diketahui oleh si pengirim dan si penerima pesan rahasia tersebut. Steganografi berasal dari Bahasa Yunani yaitu Stegano yang berarti "tersembunyi atau menyembunyikan" dan graphy yang berarti "Tulisan", jadi Steganografi adalah tulisan atau pesan yang disembunyikan [2]. Steganografi kebalikannya kriptografi yang menyamarkan arti dari sebuah pesan rahasia saja, tetapi tidak menyembunyikan bahwa ada sebuah pesan. Kelebihan Steganografi dibandingkan dengan Kriptografi adalah pesan-pesannya akan dibuat tidak menarik perhatian dan tidak menimbulkan kecurigaan, berbeda dengan Kriptografi yang pesannya tidak disembunyikan, walaupun pesannya sulit untuk di pecahkan akan tetapi itu akan menimbulkan kecurigaan pesan tersebut.

Secara umum terdapat empat jenis file yang diperlukan pengamanan yaitu gambar, audio, video dan teks [3]. Dalam penggunaan data yang banyak, file teks adalah yang paling membutuhkan lebih sedikit penyimpanan dalam memori dan dalam pentransmisian data [3]. Sehingga dalam penelitian ini akan memfokuskan teks sebagai informasi yang akan diamankan.

Sebuah penelitian penggunakan operasi XOR untuk melakukan pengamanan teks secara sederhana yang dikenal sebagai ECR (Encryption with Cover Text and Reordering) [4]. Dalam ECR penggunaan operasi XOR diperuntukkan mengenkripsi dan mendekripsi informasi dengan membangkitkan teks cover secara random dan menggabungkan cover dan enchiper teks menjadi sebuah kesatuan file. Pendekatan lain adalah PDAC (Parallel Encryprtion with Digit Arithmetic of Cover Text) yang diterapkan pada file berbasis teks [5]. Pada proses pengamanan data berbasis teks ini memanfaatkan operasi tambah dan kurang untuk menciptakan sebuah kunci yang digunakan untuk melakukan proses enkripsi dan dekripsi. Pengembangan dari PDAC adalah New PDAC yang memanfaatkan operator perkalian untuk menciptakan kunci tambahan sehingga akan memperbanyak kapasitas proses karakter yang dapat diamankan [3]. Pada keduanya menggunakan proses XOR sebagai inti proses pengamanan informasi yang disembunyikan.

Dalam penelitian ini akan dilakukan pengembangan New PDAC dengan berkonsentrasi pada penambahan kapasitas pembangkitan kunci sehingga akan berimbas pada penambahan kapasitas karakter yang dapat diamankan dengan menggunakan stego kunci yang lebih sedikit.

2. TINJAUAN PUSTAKA

PDAC dikenalkan pada tahun 2013, [5] teknik ini menyajikan perhitungan matematika dan konsep paralel untuk melakukan pendekatan steganografi berbasis teks. Dalam pendekatan ini operasi perhitungan menggunakan operator penjumlahan dan pengurangan dengan pada digit kode ASCII dari setiap karakter teks sampul sehingga mengasilkan angka baru. Angka baru ini akan digunakan dalam proses enkripsi plaintext. teknik ini satu karakter teks sampul akan memproses empat karakter plaintext. Pendekatan ini akan menghasilkan dua kunci untuk satu karakter kunci stego. Dalam pendekatan teknik ini memerlukan maksimal n byte teks sampul untuk

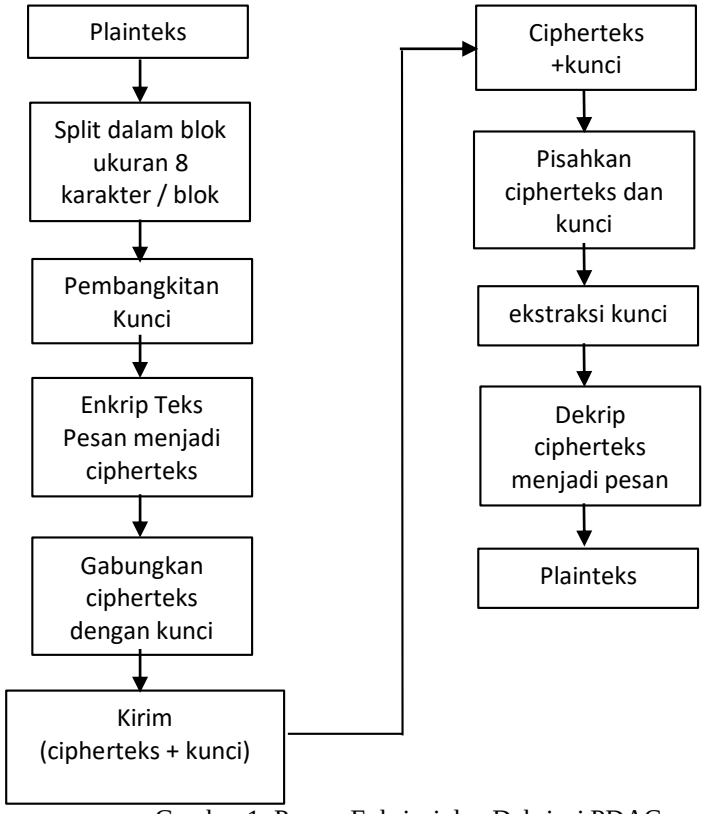
menyembunyikan 4n byte teks biasa karena satu karakter teks sampul dapat menyembunyikan empat karakter teks biasa.

Pengembangan PDAC dilakukan dalam penelitian [3]. Dalam pengembangan PDAC dilakukan pendekatan baru yang berguna dari steganografi berbasis teks untuk keamanan data cloud. Pengembangan yang dilakukan adalah dengan menggunakan operator, penjumlahan, pengurangan dan peperkalian digit kode ASCII dari setiap karakter teks sampul dilakukan dan nilai numerik yang dihasilkan baru ini digunakan untuk mengenkripsi nilai ASCII dari teks data. Karena, dalam pengembangan PDAC terdapat tiga operasi aritmatika dasar yang dilakukan pada setiap karakter teks sampul, oleh karena itu, setelah perhitungan masing-masing dan setiap karakter akan menghasilkan tiga nilai numerik sehingga, setiap nilai numerik akan mengenkripsi dua nilai ASCII dari teks biasa secara paralel. Satu dari awal array nilai ASCII dari teks biasa dan satu lagi dari akhir array yang sama. Dalam pendekatan kami, satu karakter teks sampul menyembunyikan paling banyak enam karakter teks biasa. Dengan demikian masalah alokasi memori untuk teks sampul dan waktu eksekusi keduanya berkurang.

3. METODE PENELITIAN

Pada bagian ini akan dijelaskan mengenai pengembangan New PDAC untuk bagian pengirim dan penerima. Gambar 1 menunjukkan alur proses enkripsi dan dekripsi PDAC.

Pengembangan New PDAC yang dilakukan adalah pada bagian pembangkitan kunci. Pada New PDAC untuk membangkitkan kunci digunakan operator penjumlahan penguran dan perkalian serta menggunakan angka 10 untuk menghindari hasil kunci berupa angka negatif. Pada pengembangan ini akan digukanan empat proses matematika dan tetap menggunakan angka 10 untuk membangkitkan kunci. Supaya lebih jelas proses New PDAC dijelaskan pada sub bab selanjutnya.



Gambar 1. Proses Enkripsi dan Dekripsi PDAC.

3.1 Pembagian Plainteks Kedalam Blok

Plainteks yang diakan diproses perlu dibagi menjadi beberapa blok dengan ukuran 8 karakter per blok. Sebagai contoh plainteks yang akan diproses adalah "BHARATUSESPORTAL", plainteks ini memiliki panjang 16 karakter sehingga akan dibagi menjadi 2 blok dengan ukuran masing masing 8 karakter. Blok pertama akan berisi : BHARATUS dan blok ke dua berisi : ESPORTAL seperti terlihat pada gambar 2. Apabila terjadi kekurangan jumlah karakter dalam blok, untuk memenuhi menjadi 8 blok perlu ditambahkan karakter sembarang yang tidak bermakna untuk memenuhi ukuran blok menjadi 8 karakter.

3.2 Pembangkitan Kunci

Untuk mendapatkan kunci, setiap block diperlukan kunci masing masing. Pada contoh terdapat 2 blok, sehingga diperlukan 2 kunci yang berbeda. Kunci yang diperlukan adalah sebuah karakter bebas dengan ukuran 8 bit. Dalam kasus ini sebagai kunci untuk blok 1 adalah huruf "R" dan huruf "E" untuk blok 2. Kunci ini yang

disebut dengan stego-key. Setelah mendapatkan kunci untuk setiap blok, kunci dikodekan menjadi kode ASCII yang kemudian dikenakan operasi matematika.

Plainteks :	B	H	A	R	A	T	U	S	E	S	P	O	R	T	A	L
		.....Blok 1.....								.....Blok 2.....							

Gambar 2. Blok Plainteks

Stego Kunci :	R	E
Kode ASCII :	82	69

Operasi	8+2	8-2	8*2	Max	6+9	6-9	6*9	Max
Matematika	10	6	16	8	15	-3	54	9
+ 10								
Kunci	20	16	26	18	25	7	64	19

Gambar 3. Proses Pembangkitan Kunci

Dalam penelitian ini operator matematika yang digunakan adalah penjumlahan, pengurangan, perkalian dan max yang diterapkan pada setiap digit angka pada kode ASCII. Max digunakan untuk mengambil nilai yang lebih besar pada code ASCII. Hal ini berbeda dengan penelitian sebelumnya yang hanya menggunakan operator penjumlahan, pengurangan dan perkalian saja [3]. Setelah mendapatkan hasil operasi operator matematika, ditambahkan dengan angka 10. Penambahan dengan angka 10 ini adalah digunakan untuk menghindari hasil negatif dari proses sebelumnya. Sehingga pada akhir proses ini akan terdapat 8 buah kunci yang dibangkitkan dari 2 stego kunci yang dipilih sebelumnya, dengan kata lain 1 stego key akan menghasilkan 4 buah kunci. Dalam contoh kunci yang akan digunakan untuk proses selanjutnya adalah : 20, 16, 26, 18, 25, 7, 64, 19. Proses pembangkitan kunci digambarkan pada gambar 3.

3.3 Proses Enkripsi

Pada fase pengkodean plainteks menjadi cipherteks, operator XOR diperlukan dalam proses utamanya. Dalam proses ini setiap kunci yang dibangkitkan dari stego key akan mengenkripsi 2 karakter cipherteks. Hasil dari operasi XOR ini adalah berupa angka dala kode ASCII yang kemudian diterjemahkan dalam bentuk karakter yang dapat dikenali. Gambar 4 menunjukkan proses XOR plainteks dengan kunci.

Plainteks	B	H	A	R	A	T	U	S	E	S	P	O	R	T	A	L
ASCII	66	72	65	82	65	84	85	83	69	83	80	79	82	84	65	76

Kunci	20	16	26	18	25	7	64	19
XOR								

Plainteks	66	72	65	82	65	84	85	83	69	83	80	79	82	84	65	76
Cipherteks	86	88	91	64	83	78	69	71	92	84	16	92	65	20	70	85
Simbol Karakter	V	X	[	@	S	N	E	G	\	T		\	A		F	U

Gambar 4. Proses Enkripsi

Dari proses XOR, di dapatkan hasil kode ASCII cipherteks yaitu 86, 88, 91, 64, 83, 78, 69, 71, 92, 84, 16, 92, 65, 20, 70, 85. Pada proses XOR alur yang dibuat adalah kunci pertama akan mengenkripsi karakter ke-1 dan ke-8, kunci kedua mengenkripsi karakter ke-2 dan ke-7, kunci ke tiga mengenkripsi karakter ke-3 dan ke-6, kunci keempat mengenkripsi karakter ke-4 dan ke-5, begitu juga berlaku untuk blok selanjutnya.

3.4 Penggabungan Cipherteks dan Kunci

Setelah didapatkan cipherteks, selanjutnya adalah menggabungkan cipherteks dan stego kunci yang kemudian dikirimkan secara bersamaan kepada penerima. Gambar 5 menunjukkan penggabungan cipherteks dan stego kunci. Pada proses ini stego kunci ditempatkan pada awal blok setiap cipherteks.

Pengembangan pada New PDAC dalam penelitian ini adalah dengan menempatkan stego kunci di awal block untuk blok ganjil dan stego kunci pada akhir blok untuk blok genap. hal ini digunakan untuk lebih mempersulit orang yang tidak berhak atas pesan melakukan analisa.

Dalam penelitian ini, satu stego kunci mampu mengenkripsi 8 karakter plainteks, hal ini lebih meningkat dari proses penelitian sebelumnya. Tabel 1 menunjukkan perbedaan dari penelitian sebelumnya. Dengan demikian jumlah kunci yang ikut dikirimkan kepada penerima dapat dikurangi.

Stego Kunci	82									69								
Cipherteks		86	88	91	64	83	78	69	71	92	84	16	92	65	20	70	85	
Penggabungan Kunci Stego + Cipherteks																		
	82	86	88	91	64	83	78	69	71	92	84	16	92	65	20	70	85	**69**

Gambar 5. Proses Penggabungan Stego Kunci dan Cipherteks

Tabel 1. Perbedaan PDAC, New PDAC dan Modifikasi New PDAC

	PDAC	New PDAC	Modifikasi New PDAC
Stego Key	1	1	1
Operator Pembangkitan Kunci	+, -	+. -, *	+, - , *, max
Proses Enkripsi	XOR	XOR	XOR
Kemampuan proses per 1 Stego Kunci	1 stego kunci mengenkripsi 4 karakter plainteks	1 stego kunci mengenkripsi 6 karakter plainteks	1 stego kunci mengenkripsi 8 karakter plainteks

3.5 Proses Dekripsi

Proses dekripsi dilakukan oleh pihak penerima pesan. Proses ini merupakan balikan dari proses enkripsi. Untuk melakukan penguraian cipherteks menjadi plainteks beberapa langkah perlu dilakukan yaitu 1) memisahkan stego kunci dari pesan, 2) membangkitkan kunci dari stego kunci, 3) melakukan proses XOR antara kunci dengan cipherteks.

Untuk memisahkan cipherteks dan stego kunci, digunakan blok dengan ukuran 9 karakter per blok dari pesan yang diterima. Karakter pertama dari setaip blok ganjil adalah stego kunci dari blok dan karakter terkhir dari blok genap adalah stego kunci. Dan tahapan selanjutnya adalah mendapatkan kunci dari stego kunci yang di pisahkan.

Untuk mendapatkan kunci, proses yang dilakukan adalah sama seperti yang dilakukan oleh pengirim. Yaitu dengan menggunakan operasi matematika penjumlahan, pengurangan, perkalian dan nilai maksimal dari stego kunci. Langkah selanjutnya adalah proses dekripsi yang menggunakan logika XOR. Sehingga nantinya akan mendapatkan hasil yang ekivalen dengan plainteks.

4. HASIL DAN PEMBAHASAN

Teknik yang dilakukan dalam penelitian ini adalah mengadopsi dari penelitian sebelumnya dengan melakukan beberapa perubahan. Perubahan pertama yang diusulkan adalah dengan menambah operator matematika dalam menghasilkan kunci enkripsi. Pada penelitian ini digunakan empat operator yaitu penjumlahan, pengurangan, perkalian dan nilai maksimum dari kode ASCII kunci stego. Dengan menambahkan operator dalam melakukan pembangkitan kunci, maka operasi enkripsi terhadap jumlah karakter plainteks akan juga meningkat, yang mana setiap kunci enkripsi akan memproses dua karakter plainteks. Sehingga dalam penelitian ini satu kunci stego akan menghasilkan 4 kunci enkripsi dan akan memproses 8 karakter plainteks.

Dalam proses enkripsi digunakan logika XOR untuk memproses plainteks menjadi cipherteks. Dalam penelitian ini alur proses XOR antara kunci enkripsi dengan karakter plainteks tidak dilakukan perubahan. Hal ini dikarenakan proses XOR adalah kunci pertama akan mengenkripsi karakter ke-1 dan ke-8, kunci kedua mengenkripsi karakter ke-2 dan ke-7, kunci ke tiga mengenkripsi karakter ke-3 dan ke-6, kunci keempat mengenkripsi karakter ke-4 dan ke-5, begitu juga berlaku untuk blok selanjutnya. Asumsi lain jika dilakukan perubahan alur XOR maka akan berakibat lebih sulitnya cipherteks yang dihasilkan untuk dianalisa, karena proses akan semakin acak.

Dalam proses penggabungan kunci stego dengan cipherteks, dalam penelitian ini juga dilakukan perubahan. Untuk blok dengan nilai ganjil, penempatan kunci stego diberikan pada awal blok, dan penempatan kunci stego untuk blok dengan urutan genap ditempatkan pada akhir blok. Hal ini berbeda dengan teknik sebelumnya yang menempatkan kunci stego pada awal blok. Dengan demikian proses pengacakan akan semakin rumit untuk dideteksi oleh pihak yang tidak berhak.

5. KESIMPULAN

Dari proses yang sudah dilakukan dapat ambil kesimpulan bahwa penggunaan jumlah operator matematika pada pembangkitan kunci akan mempengaruhi jumlah kunci yang dihasilkan dari stego kunci. Semakin banyak operator yang digunakan dalam pembangkitan kunci maka akan semakin banyak jumlah kunci yang akan dihasilkan dari proses tersebut. Dengan demikian, jika jumlah kunci menjadi semakin banyak maka akan berimbas kepada proses enkripsi. Dengan menggunakan kunci yang banyak maka jumlah karakter plainteks yang dapat di enkripsikan akan menjadi semakin bertambah. Dengan demikian akan menjadikan reduksi stego kunci menjadi meningkat. Pada proses enkripsi menggunakan logika XOR dengan jalur yang telah ditentukan, dengan mengubah

jalur XOR antara kunci dengan plainteks maka akan mengakibatkan pesan dalam cipherteks menjadi lebih acak, sehingga akan meningkatkan keamanan plainteks saat dikirim kepada penerima.

Proses pengamanan data adalah menjadi penting saat sebuah algoritma diusulkan, dengan demikian perlunya pengembangan dalam bentuk yang lebih baik. Pendekatan pendekatan secara soft computing mungkin akan menjadikan perhatian dalam pengembangan selanjutnya.

DAFTAR PUSTAKA

[1] Bobade, S. dan Goudar, R., 2015, Secure Data Communication Using Protocol Steganography in IPv6, *IEEE 2015 International Conference on Computing Communication Control and Automaton*.

[2] Ardhianto, E., Warnars, H. L. H. S., Soewito, B., Gaol, F. L. dan Abdurachman, E., 2020, Improvement of Steganography Technique: A Survey, *1st International Multidisciplinary Conference on Education, Technology, and Engineering (IMCETE 2019)*, Serang, Banten, Indonesia.

[3] Gaur, M. dan Sharma, M., 2015, A New PDAC (Parallel Encryption with Digit Arithmetic of Cover Text) Based Text Steganography Approach for Cloud Data Security, *International Journal on Recent and Innovation Trends in Computing and Communication*, Vol. 3, No. 3, 344 – 1352.

[4] Kataria, S., Singh, K., Kumar, T. dan Nehra, M. S., 2013, ECR (Encryption with Cover Text and Reordering) based Text Steganography, *IEEE Second International Conference on Image Information Processing*, Waknaghat, Shimla, Himachal Pradesh, INDIA.

[5] Kataria, S., Singh, B., Kumar, T. dan Shekhawat, H. S., 2013, PDAC (Parallel Encryption with Digit Arithmetic of Cover Text) Based Text Steganography, *Fourth International Conference on Advances in Computer Science-AETACS2013*.

[6] Pressman, R. S., 2002, *Rekayasa Perangkat Lunak (Pendekatan Praktis)*, Andi, Yogyakarta.