Jurnal Informatika Universitas Pamulang **ISSN: 2541-1004**
Penerbit: Program Studi Teknik Informatika Universitas Pamulang **e-ISSN: 2622-4615**
Vol. 7, No. 2, Juni 2022 (308-312) **10.32493/informatika.v7i2.13921**

Modifikasi Parallel Encryption with Digit Arithmetic and Covertext (PDAC) Menggunakan Kunci Berulang

Eka Ardhianto[1], Khristma M. A. Pamungkas[2], Edy Supriyanto[3], Endang Lestariningsih[4]

Fakultas Teknologi Informasi dan Industri, Universitas Stikubank, Jl. Tri Lomba Juang No. 1, Semarang
e-mail: [1]ekaardhianto@edu.unisbank.ac.id, [2]khristmap@gmail.com, [3]edysup4@edu.unisbank.ac.id, [4]endang_lestariningsih@edu.unisbank.ac.id

Submitted Date: October 20th, 2021 Reviewed Date: January 08th, 2022
Revised Date: January 09th, 2022 Accepted Date: August 16th, 2022

Abstract

The encryption process is the most important security technique, because it is used to hide information from unauthorized partiesWith the capability to secure large quantities of data, encryption is of the most importance. This research aims to be able to hide a large amount of information by using a repetitive key to the solution for an odd number of plaintext characters for smooth encryption in PDAC. In this study, the mathematical operations of addition and subtraction are used to generate keys from ASCII codes. This research results increase the capacity of information that can be secured.

Keywords: PDAC; Enkripsi; Enkripsi PDAC; padding

Abstrak

Proses enkripsi adalah teknik keamanan yang paling penting, karena digunakan untuk menyembunyikan informasi dari pihak yang tidak berwenang Dengan kemampuan untuk mengamankan data dalam jumlah besar, enkripsi adalah yang paling penting. Penelitian ini bertujuan untuk dapat menyembunyikan sejumlah besar informasi dengan menggunakan kunci berulang untuk solusi jumlah karakter plaintext ganjil untuk kelancaran enkripsi di PDAC. Dalam penelitian ini, operasi matematika penjumlahan dan pengurangan digunakan untuk membangkitkan kunci dari kode ASCII. Hasil penelitian ini meningkatkan kapasitas informasi yang dapat diamankan.

Kata kunci: PDAC; Enkripsi; Enkripsi PDAC; padding

1. Pendahuluan

Keamanan informasi sangat penting untuk menjaga keamanan informasi dari orang yang tidak berwenang. Keamanan informasi dicapai dengan mengenkripsi informasi sehingga keaslian isi informasi tetap terjaga, dan dekripsi adalah pengembalian informasi ke bentuk aslinya, hanya dapat diakses oleh pihak yang berwenang. (Aditya, 2010: G-32)

Pengenkripsian suatu informasi terus berkembang dengan menggunakan berbagai macam teknik penyembunyian pesan contohnya seperti Steganografi dan Kriptografi, keduanya berasan dari Bahasa Yunani, untuk Steganografi berasa dari kata steganos, artinya "tersembunyi", dan graphien, "menulis" (Eka Ardhianto, 2019:289), sementara Kriptografi berasal dari kata kryptos, artinya "tersembunyi, rahasia" dan graphein, "menulis", meskipun memiliki fungsi yang sama namun memiliki tujuan yang berbeda, Steganografi menyembunyikan pesan dengan mengganti tiap digit pesan tersebut menjadi pesan yang tidak memiliki arti selain penerima, tak seorang pun tahu bahwa ada pesan rahasia pada tulisan tersebut, sementara kriptografi menyembunyikan pesan dengan menyamarkan pesan yang memiliki arti lain, kelebihan dari steganografi dibandingkan kriptografi yaitu hasil dari pengubahan pesan yang tidak menimbulkan kecurigaan. (Handoko, 2020:55)

Model enkripsi *Parallel Encryption with Digit Arithmetic of Cover Text (PDAC)* adalah teknik perhitungan matematika dan konsep paralel untuk pendekatan steganografi berbasis

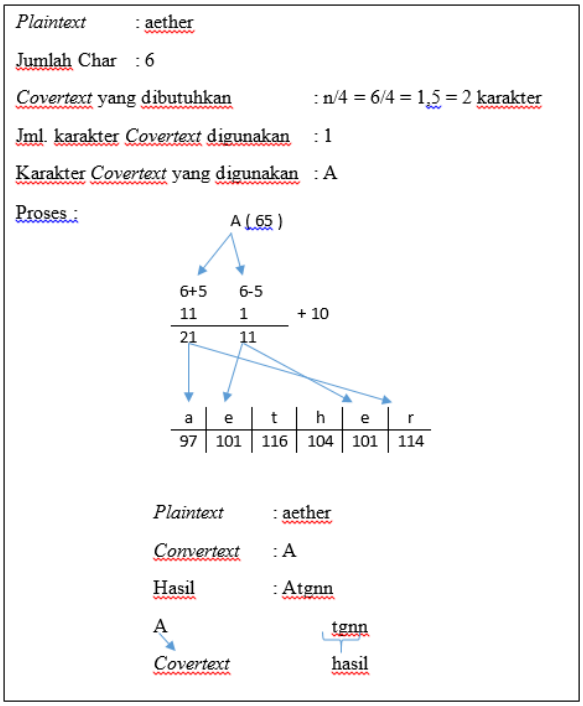
teks (Handoko, 2020:55). PDAC menggunakan Steganografi untuk mengenkripsi pesan, dengan tahap pengubahan digit karakter pada pesan menjadi digit kode ASCII, kode ASCII diubah menjadi kode biner, begitu pula dengan karakter covertext yang digunakan. PDAC membutuhkan sebuah covertext untuk membangkitkan 2 buah kunci enkripsi. Sehingga satu covertext mampu mengenkripsi sebanyak 4 karakter, setelah mengubah covertext menjadi kode ASCII selanjutnya dengan proses penghitungan matematika SUM (penjumlahan) antara 2 digit angka pada kode ASCII dan SUB (pengurangan) antara 2 digit angka pada kode ASCII lalu hasil dari SUM dan SUB masing – masing ditambah 10 untuk menghasilkan kunci enkripsi. (Sahil Kataria, 2013)

Proses enkripsi PDAC menggunakan operasi XOR antar tiap digit karakter plaintext dengan kunci. Pada percobaan awal yang dilakukan, sebagai pengguna akan merasa nyaman dengan penggunaan PDAC yang digunakan untuk mengenkripsi plaintext dengan jumlah karakter yang relatif sedikit. Hal ini berkaitan dengan penerbitan covertext yang dipilih selayaknya password. Namun saat jumlah karakter plaintext berjumlah banyak, maka pengguna perlu menerbitkan covertext dengan jumlah n/4, dengan n adalah jumlah karakter dalam plaintext. Proses PDAC menggunakan satu covertext untuk mengenkripsi 4 karakter, hal ini adalah berupa angka genap.

Penelitian ini dilakukan berdasar pada penelitian yang sebelumnya: PDAC, metode tersebut masih memiliki kekurangan, proses enkripsi akan tidak berjalan saat ukuran covertext yang dibutuhkan kurang dari n/4 karakter. Maka pada artikel ini akan membahas tentang perbaikan untuk menutup celah tersebut pada PDAC.

2. Metode

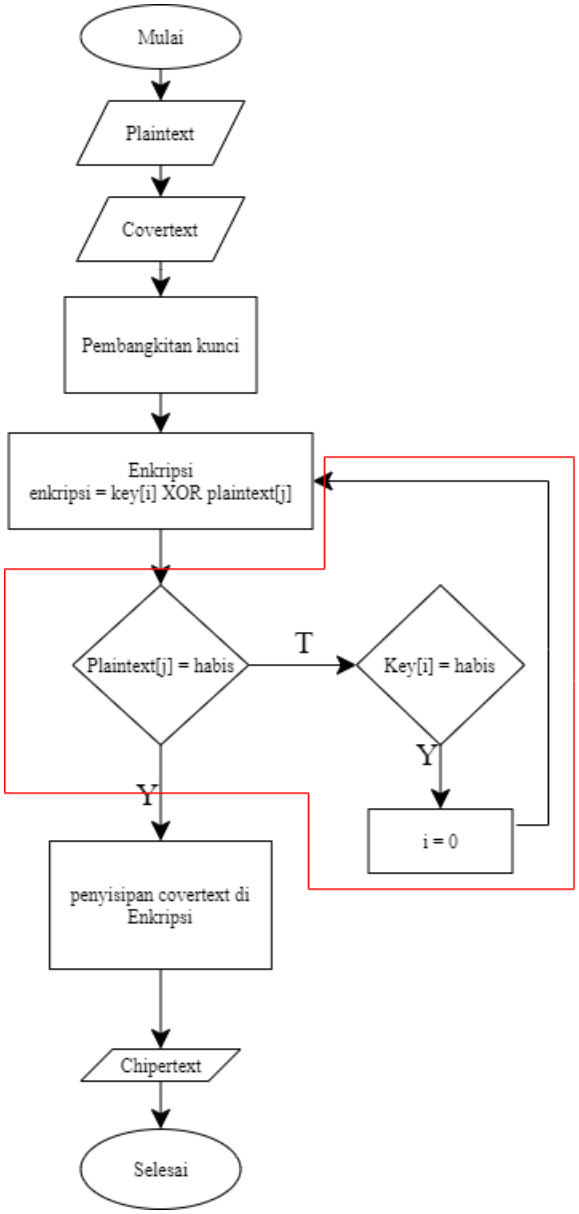
Celah pada proses enkripsi PDAC yang ditemukan yaitu Saat jumlah karakter covertext tidak memenuhi aturan jumlah karakter yang diperlukan. Gambar 1 menunjukkan ilustrasi proses enkripsi yang menggunakan jumlah covertext kurang dari n/4.



Gambar 1. Enkripsi PDAC dengan covertext kurang dari n/4

Dari gambar 1, dapat dijelaskan bahwa Jumlah Plaintext adalah 6 karakter, jumlah covertext seharusnya yang dibutuhkan adalah 6/4 = 1,5 karakter = 2 karakter. Dalam percobaan covertext hanya 1 karakter. Sehingga 2 karakter tidak terproses.

Dari celah permasalahan yang ditemukan, teknik pengulangan covertext diusulkan dilakukan secara berulang seperti penggunaan kunci pada algoritma enkripsi vigenere. Gambar 2 menunjukkan flowchart modifikasi PDAC dengan menggunakan proses pengulangan kunci.



Gambar 2. Enkripsi PDAC teknik pengulangan kunci

Dari gambar 2, terlihat area bergaris warna merah yang kedua yaitu mengadopsi teknik enkripsian dari Algoritma Vigenere dengan penggulangan kunci sesuai dengan jumlah karakter plaintext.

3. Hasil dan Pembahasan

Percobaan ini menggunakan 2 teks sebagai contoh yang berbeda sebagai plaintext dan menggunakan covertext yang sama untuk kedua plaintext untuk pengujian enkripsi modifikasi PDAC terlihat pada tabel 1. Eksperimen diimplementasikan dengan pemrograman PHP.

Table 1. Plainteks Pengujian

	Plainteks 1	***Plainteks 2***
Plaintext	BHARAT	BHARATUSESPORTALS
Covertext	QWE	QWE

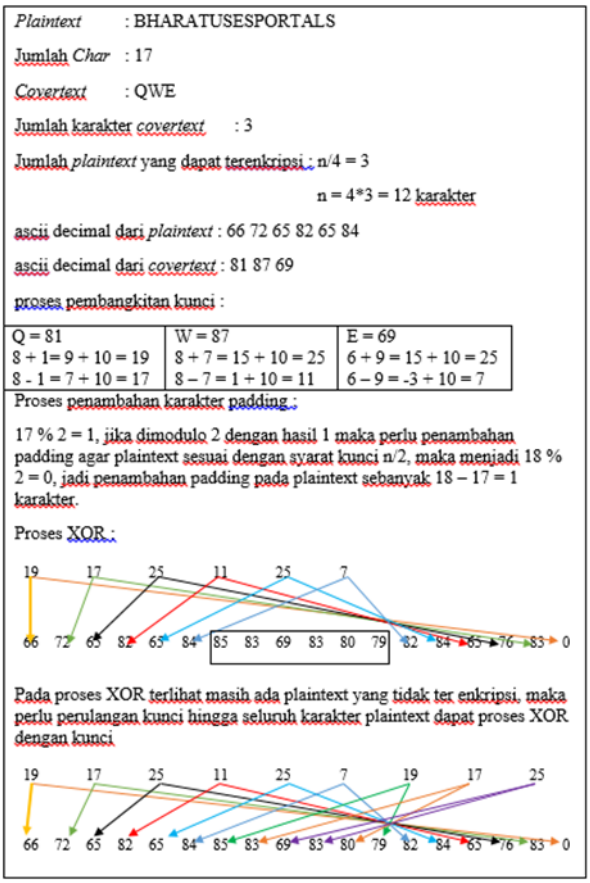
```
$enkripsi = array();
for ($x=0; $x < intval($a/2) ; ) {
   $sisapesan = $a-$x;
   for ($i=0; $i < count($key4); $i++) {
      $hurufdepan = $x+$i;
      if ($hurufdepan>=intval($a/2)) {
         break;      }
      $enkripsi[$hurufdepan] = $pesan3[$hurufdep
an] ^ $key4[$i];   }
   for ($j=0; $j < count($key4); $j++) {
      $hurufbelakang = $sisapesan-$j-1;
      if ($hurufbelakang<intval($a/2)) {
         break;      }
$enkripsi[$hurufbelakang] = $pesan3[$hurufbelak
ang] ^ $key4[$j];   }
   $x = $x + $i;    }
```

Gambar 3. Enkripsi PDAC dengan perulangan kunci

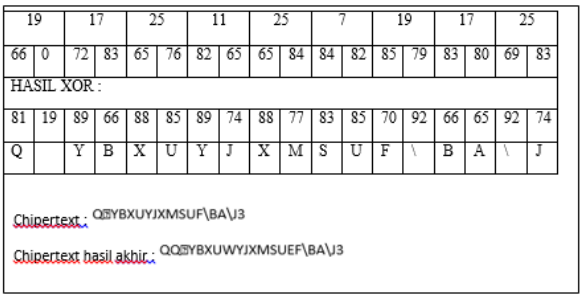
Proses enkripsi dengan memanfaatkan proses XOR antara karakter ascii plaintext dalam bentuk decimal dan karakter ascii covertext yang telah membangkitkan karakter kunci yang berupa decimal, proses perulangan berlangsung hingga separuh dari panjang karakter plaintext, karena untuk mempersingkat waktu mengenkripsi serta tanpa mengubah syarat dari enkripsi yaitu satu kunci dapat mengenkripsi dua karakter plaintext (n/2) yang dimana proses enkripsi karakter bagian depan dengan posisi 0 hingga separuh dari panjang karakter plaintext dan proses enkripsi karakter bagian belakang dengan posisi tengah atau separuh dari panjang karakter plaintext tersebut hingga posisi paling akhir, maka dari itu dilakukan perulangan dengan batas perulangan jika telah mencapai nominal yang sama dengan separuh panjang karakter plaintext maka selesai. Gambar 3 menunjukkan potongang sourcecode proses enkripsi PDAC yang dimodifikasi.

Pada source code perulangan kunci terdapat tiga sistem perulangan, 1) perulangan untuk keseluruhan proses, 2) untuk mengetahui posisi karakter plaintext yang belum terenkripsi, yang di gunakan untuk menghitung jumlah karakter yang

telah berjalan pada 1 putaran yang memanfaatkan hitungan dari hasil kode perulangan kedua dan ketiga tersebut, 3) menghitung urutan ke berapa karakter yang belum terenkripsi. Lalu untuk dua code perulangan selanjutnya yaitu proses XOR plaintext dengan kunci yang diulangi sesuai dengan jumlah karakter pada kunci. Gambar 4 memberikan ilustrasi proses perulangan kunci pada enkripsi PDAC. Gambar 5, menunjukkan hasil proses enkripsi PDAC dengan perulangan kunci.



Gambar 4. Proses manual Pengujian Enkripsi PDAC



Gambar 5. Ciphertext akhir PDAC dengan perulangan kunci

4. Kesimpulan

Hasil eksperimen menunjukkan bahwa bahwa untuk mengenkripsi karakter plaintext dengan jumlah yang tidak sesuai dengan ketentuan covertext yaitu n/4 dapat dilakukan dengan perulangan kunci untuk mengenkripsi seluruh plaintext, keuntungan lain yang didapatkan ialah memudahkan user untuk dapat secara langsung menggunakan proses enkripsi tanpa perlu menhitung terlebih dahulu banyaknya karakter covertext yang perlu dipakai untuk mengenkripsi, hal ini akan mempersingkat waktu.

References

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.

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.

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.

Selent, D., 2010, "*Advanced Encryption Standard*", InSight: Rivier Academic Journal, Volume 6, Number 2.

Saraf, K. R., Jagtap, V. P., Mishra, A. K., 2014, "*Text and Image Encryption Decryption Using Advanced Encryption Standard*", International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), INDIA.

Chengxia, L., 2012, "*Discussion of New Padding Method in DES Encryption*", Journal of Software Engineering and Applications, Computer Science and Technology Dept. , Beijing Information and Technology University, Beijing, China.

Handoko, W. T., Ardhianto, E., Supriyanto, E., 2020, "*Modifikasi New Pdac (Parallel Encryption With Digit Arithmetic Of Cover Text)*", Fakultas Teknologi Informasi. Universitas Stikubank (UNISBANK) Semarang.

Mohankumar, K. N., Jayaramu, H. S., Kurian, M. Z., Shiva kumar, K. B., 2014, "*FPGA Implementation of Vigenere Cipher Method Based on Colour Image Steganography*", International Journal of Advanced Research in

Electrical, Electronics and Instrumentation Engineering, INDIA.

Ayman, A., Sameh, F., 2015, "*The Effect Of Varying Key Length On A Vigenère Cipher*", IOSR Journal of Computer Engineering, Vol. 17.

Saputra, I., Hasibuan N. A., Mesran., Rahim, R., 2017, "*Vigenere Cipher Algorithm with Grayscale Image Key Generator for Secure Text File*", STMIK Budi Darma Medan, Indonesia