BAB I

PENDAHULUAN

1.1. Latar Belakang Penelitian

Keamanan suatu informasi merupakan hal terpenting untuk melindungi informasi tersebut dari pihak yang tidak berhak. Pengamanan suatu informasi dilakukan dengan cara mengenkripsi informasi tersebut agar keaslian isi dari informasi tetap terjaga dan dekripsi untuk mengembalikan informasi tersebut ke bentuk aslinya yang hanya dapat di akses oleh pihak yang berhak. (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)

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

Dalam NEW PDAC, sebuah karakter *covertext* mampu menerbitkan 3 buah kunci enkripsi. Sehingga satu *covertext* mampu mengenkripsi sebanyak 6 karakter. Untuk proses penerbitan karakter kunci sama seperti PDAC namun dengan 3 proses penghitungan matematika yaitu *SUM*, *SUB*, dan *MUL*. MUL merupakan proses perkalian antara 2 digit angka pada kode ASCII *covertext* lalu hasil perkalian tersebut ditambahkan 10 untuk menghasilkan kunci enkripsi. (Gaur, 2015)

Proses enkripsi PDAC dan NEW 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 yaitu PDAC dan NEW PDAC, pada kedua penelitian tersebut masih memiliki kekurangan yaitu, proses enkripsi akan tidak berjalan saat ukuran *covertext* yang dibutuhkan kurang dari n/4 karakter *plaintext* dan proses enkripsi akan tidak berjalan saat jumlah karakter *plaintext* adalah ganjil. Maka pada skripsi ini akan membahas tentang perbaikan untuk menutup celah tersebut pada PDAC.

1.2. Perumusan Masalah

Perumusan masalah yang akan diambil dari uraian latar belakang dalam pembuatan skripsi ini adalah :

1. Mekanisme seperti apa yang perlu dirancang untuk proses enkripsi PDAC jika ukuran *covertext* yang dibutuhkan berjumlah kurang dari n/4 karakter *plaintext* ?
2. Bagaimana penanganan proses enkripsi menggunakan PDAC saat jumlah karakter *plaintext* adalah ganjil ?

1.3. Tujuan dan Manfaat penelitian

1.3.1. Tujuan

1. Mendapatkan desain untuk mengatasi permasalahan kebutuhan jumlah karakter *covertext* yang berjumlah kurang dari n/4 karakter *plaintext*.
2. Mendapatkan desain untuk mengatasi permasalahan jika panjang dari *plaintext* berjumlah ganjil.

1.3.2. Manfaat

1. Memberikan manfaat dan sumbangsih pada bidang kriptografi.
2. Perbaikan yang dilakukan dalam penelitian ini akan memberikan dampak kemudahan penggunaan model enkripsi PDAC untuk menggamankan dokumen berbasis *text*.

1.4. Sistematika penulisan

Sistematika penulisan ini dibuat guna memberikan gambaran secara umum mengenai penelitian yang dijalankan. Berikut sistematika penulisan dalam penelitian ini :

BAB I PENDAHULUAN

Bab ini berisi tentang latar belakang penelitian, perumusan masalah, batasan masalah, tujuan dan manfaat penelitian, dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Tinjauan pustaka berisi uraian sistematis tentang informasi dari hasil penelitian sebelumnya yang telah dikumpulkan lalu dianalisa dan membandingkan dengan masalah dari penelitian yang sedang diteliti.

BAB III METODE PENELITIAN

Pada bagian ini akan dijelaskan mengenai jalan penelitian, usulan metode untuk menyelesaikan permasalahan, dan data pengujian yang digunakan.

BAB IV HASIL PENELITIAN DAN PEMBAHASAN

Hasil penelitian dan pembahasan berisi tentang keseluruhan hasil yang diteliti, hasil perhitungan pengujian, dan interprestasi hasil penelitian.

BAB V KESIMPULAN DAN SARAN

Kesimpulan dan saran berisi uraian tentang simpulan dari penelitian yang telah dibuat dan saran mengenai penelitian yang dilakukan.