BAB I
PENDAHULUAN

1.1 Latar Belakang

Di era 4.0 ini data atau informasi menjadi hal yang penting dan sangat dibutuhkan oleh masyarakat. Teknologi untuk menjaga keamanan data maupun informasi menjadi hal yang sangat penting bagi sebuah kalangan, baik yang berupa perusahaan, lembaga pemerintahan ataupun data pribadi.[1][2]

Keamanan digital merupakan hal privasi dan membutuhkan penanganan yang sangat besar, maka dari itu dibutuhkan sebuah mekanisme sistem keamanan yang dapat menyelesaikan masalah kerahasiaan sebuah data atau informasi. Untuk menjaga keamanan dan kerahasiaan sebuah data atau informasi dalam data pribadi maka diperlukan metode enkripsi untuk menjaga kerahasiaan data atau informasi tetap aman.[3] [4]

Metode enkripsi adalah proses mengacak data atau informasi agar tidak dapat dibaca oleh pihak lain atau pihak yang tidak berhak menerima data tersebut, kecuali pihak yang berhak menerimanya. Dengan adanya metode enkripsi ini diharapkan dapat mencegah campur tangan dari orang-orang yang tidak berhak melihat, merubah, ataupun menghapus data atau informasi yang telah diterima. Informasi dibagi menjadi dua yaitu informasi yang bersifat pribadi dan informasi yang bersifat umum. Informasi yang bersifat pribadi adalah informasi yang hanya boleh diketahui oleh orang-orang tertentu saja dan hanya Sebagian orang saja yang mengetahuinya, sedangkan informasi yang bersifat umum adalah informasi yang boleh diketahui oleh orang banyak atau sifatnya umum. Proses pengiriman sebuah data atau informasi tidak luput dari campur tangan pihak-pihak yang tidak berhak untuk menerima informasi tersebut. Salah satu teknik untuk mengamankan kerahasiaan data atau informasi adalah dengan menggunakan algoritma kriptografi.[5]

Algoritma kriptografi terdiri dari algoritma enkripsi dan algoritma deskripsi. Enkripsi adalah proses pengacakan data atau informasi agar tidak dapat

dibaca, dilihat, diubah atau dimanipulasi. Sedangkan deskripsi adalah proses pengembalian dari proses pengacakan ke bentuk yang semula.

Algoritma *One Time Pad* (OTP) merupakan kriptografi klasik yang menggunakan satu kunci untuk melakukan sebuah enkripsi dan deskripsi yang sama, penemunya adalah Major Joseph Mauborge pada tahun 1917. Kunci dari kriptografi algoritma *One Time Pad* adalah barisan acak yang Ketika disandikan akan menghasilkan *plain text* dengan barisan yang sepenuhnya acak. *One Time Pad* harus menggunakan kunci yang *random* untuk meningkatkan keamanan dari algoritma itu sendiri.[2]

Telegram merupakan aplikasi *cloud based* dan alat enkripsi. Telegram menyediakan enkripsi *end-to-end*. Selain itu telegram juga menyediakan wadah bagi pengembang yang ingin memanfaatkan Open API dan Protokol yang disediakan melalui Telegram Bot yang didokumentasikan pada *website* resminya. Telegram Bot merupakan telegram khusus yang didesain untuk menghandle pesan secara otomatis. Pengguna dapat berinteraksi dengan BOT dengan mengirimkan pesan perintah *(command)* melalui peran *private* maupun grup. Telegram Bot juga dapat dibangun sesuai dengan kebutuhan kita.[6]

Berdasarkan permasalahan tersebut dibutuhkan sebuah sistem keamanan enkripsi yang mana dapat mengamankan data atau informasi supaya tetap aman agar pihak-pihak yang tidak berhak menerima informasi tersebut tidak dapat melihat, ataupun mengubah data atau informasi tersebut. Dengan dasar tersebut, Penelitian ini menjadi acuan untuk perancangan Algoritma kriptografi baru, setelah melihat dalam penelitian tersebut terlihat bahwa suatu kriptografi juga memerlukan pembaharuan, supaya tingkat keamanan menjadi lebih baik. Dan latar belakang diatas penulis mencoba untuk membuat rancangan keamanan data dengan menggunakan algoritma kriptografi yang terintegrasi dengan api telegram dengan mengambil judul" Sistem Enkripsi Pesan Pada Bot Telegram Menggunakan Algoritma *One Time Pad*"

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah yang telah dibahas, terdapat beberapa masalah yang dirumuskan dalam penelitian ini, yaitu:.

1. Bagaimana Algoritma One Time Pad dapat terintegrasi dengan Bot Telegram ?
2. Bagaimana cara membuat program Enkripsi dan Deskripsi dalam sistem keamanan data atau informasi ?
3. Seberapa efisien Bot Telegram dalam mengenkripsi pesan dalam bentuk plain text ?

1.3 Batasan Masalah

Adapun batasan masalah dalam penelitian ini adalah:

1. Hanya dapat mengenkripsi pesan dalam bentuk text
2. Tingkat kedalaman algoritma yang digunakan dalam penelitian ini yang sudah terintegrasi dengan telegram bot belum mampu mengenkripsi file berupa document, audio, sticker dan foto.

1.4 Tujuan Penelitian

Pada penulisan tugas akhir ini, terdapat beberapa tujuan sebagai berikut:

1. Meningkatkan proses pengamanan data atau informasi untuk mencegah agar pihak-pihak yang tidak berhak menerimanya tidak dapat menyalahgunakan data atau informasi tersebut.
2. Membuat sistem enkripsi dan dekripsi yang efisien serta cepat dalam merespon dalam mengenkripsi dan dekripsikan pesan.
3. Meningkatkan kesadaran keamanan informasi pada setiap individu.

1.5 Manfaat Penelitian

A. Bagi Penulis

a. Mengaplikasikan ilmu – ilmu akademis yang didapat selama perkuliahan untuk merancang sistem enkripsi dan deskripsi pesan pada telegram bot menggunakan Alogirtma One Time Pad (OTP).

b. Memperluas wawasan khususnya dalam metode enkripsi dan deskripsi menggunakan telegram bot.

B. Bagi Universitas

a. Memberikan gambaran terhadap penerapan ilmu pengetahuan yang telah didapatkan selama kuliah

b. Menjadi sumbangan literatur karya ilmiah dalam ilmu teknologi khususnya dibidang *cyber security*.

1.6 Sistematika Penulisan

Sistematika penulisan dalam skipsi ini, disusun sebagai berikut:

BAB I PENDAHULUAN, Bab ini berisi latar belakang masalah, permasalahan, batasan masalah, tujuan dan manfaat penulisan , serta sistematika penulisan....

BAB II TINJAUAN PUSTAKA, Bab ini berisi tinjauan pustaka tentang kriptografi one time pad , serta dasar dasar teori dalam sistem enkripsi dan dekripsi pesan pada telegram bot.

BAB III METODE PENELITIAN, Bab ini menjelaskan tentang flowchart alur penelitian serta analisis kebutuhan *hardware* dan *software* pada penelitian ini.

BAB IV HASIL DAN PEMBAHASAN, Bagian ini berisi analisis dari hasil pengujian mengenai sistem enkripsi dan ekripsi pesan pada telegram bot.

BAB V PENUTUP, Pada bab ini berisikan beberapa kesimplan dari hasil penelitian ini.