BAB I
PENDAHULUAN

1.1 Latar Belakang

Teknologi informasi pada masa kini sudah menjadi bagian penting dikalangan banyak orang, baik itu kalangan anak-anak maupun kalangan dewasa. Pada dasarnya teknologi diciptakan untuk mempermudah pekerjaan manusia pada bidang-bidang tertentu yang mengharuskan pekerjaan tersebut terselesaikan dengan tepat dan efisien. Banyak contohnya dalam kehidupan sehari-hari antara lain dalam hal berkomunikasi, baik itu dengan media *handphone* maupun *website.*

Pada bidang komunikasi pun terdapat layanan Pengaduan yang berfungsi sebagai sarana pelayanan masyarakat. Layanan ini berguna untuk memudahkan atau mempercepat tindakan masyarakat dalam melaporkan dan tindakan terhadap keadaan darurat kepada pihak yang berwajib. Bentuk dari layanan bantuan berorientasi pada pengaduan masyarakat pada kegawatdaruratan, diantaranya seperti: Medis, kebakaran, keamanan, kecelakaan, dan bencana alam. Pada penelitian kali ini akan berkaitan dengan instansi kantor polisi, misalnya seseorang melaporkan suatu kejadian atau masalah dan ingin melaporkan ke kantor polisi yang terdekat dengan kejadian, maka pelapor tersebut tidak perlu sulit mencari atau menanyakan kepada masyarakat sekitar dimana kantor polisi terdekat. Maka dari itu dibentuklah aplikasi untuk menangani kasus tersebut dengan bantuan *google map*.

Namun pada dasarnya pertukaran informasi dan data merupakan hal yang sangat rentan akan kebenaran dan keaslian data tersebut, dengan adanya layanan bantuan masyarakat ini juga dapat menimbulkan dampak buruk dan kerugian bagi salah satu pihak, dampak tersebut biasanya dilakukan oleh oknum-oknum masyarakat yang tidak bertanggung jawab yang menjadikan data atau informasi tersebut palsu dan tidak benar adanya (*Hoax*) dengan alasan hanya iseng atau main-main dan merubah atau menggunakan data orang lain untuk kepentingan dirinya sendiri.

Sebagai contoh adalah yang dikatakan oleh Arman Haizarin *Contact Center & Outsourcing Services Director Infomedia*, dalam halaman website berita

KOMPAS dengan judul berita Di 110 Masih Banyak Telepon Iseng https://tekno.kompas.com/read/2013/02/14/13285864/Di.110.Masih.Banyak.Telepon.Iseng, hingga pertengahan 2013 ada 18 ribu telepon per hari yang masuk ke 110. Namun, masyarakat yang memberi laporan sungguhan hanya 101 laporan per hari. Berdasarkan kategori, 30 % laporan yang masuk ke 110 adalah aduan tindak kriminalitas, 19 % info lalu lintas, dan kecelakaan sebesar 18 % Kompas.com – 14/02/2013 13:28 WIB.

Penggunaan OTP dan *Two Central Facilities Protocol* yang diterapkan pada sistem layanan pengaduan mendapatkan hasil, dimana pelapor tidak akan berani membuat laporan paslu karena data pelapor tersebut didapat dari data asli yang di simpan di CLA, CLA ini merupakan badan yang menyimpan KTP asli pelapor juga sebagai badan yang memberikan nomer validasi atau OTP kepada pelapor. Sehingga jika pelapor tersebut menggunakan nomer NIK palsu atau yang tidak terdaftar di CLA sistem akan menolak data masukan tersebut dan jika OTP tersebut tidak sesuai dengan yang dikirimkan oleh CLA maka sistem juga akan menolak pelapor tersebut selain itu OTP tersebut dihashing menggunakan MD5 dengan begitu *hacker* akan sulit untuk menentukan nomer OTP tersebut, namun jika isi dari laporan tersebut terbukti palsu maka polisi dapat melacak keberadaan dari pelapor tersebut karena harus menggunakan data asli yang didapat dari KTP pelapor dan sanksi jika melanggar yaitu yang diatur dalam Bab IX tentang sumpah dan keterangan palsu, pasal 242 ayat (1) kitab Undang-Undang Hukum Pidana (KUHP) dan Undang-Undang No. 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (ITE).

Perbedaan dari sistem ini dan sistem dengan panggilan terlepon yaitu data pelapor yang melaporkan akan lebih spesifik karena data yang didapat adalah dari KTP jika dibandingkan dengan melakukan panggilan dengan telepon seperti yang didapat dari berita Kompas.com – 30/01/2013 dengan judul Hati-hati, Ada Sanksi Untuk yang Iseng Telepon 110. Polisi hanya merekam data dari nomor penelponnya saja maka belum terjamin jika pelapor tersebut akan membuat laporan asli dan mendapat sanksi jika pelapor tersebut hanya main-main atau membuat laporan palsu.

Pada penelitian Muhammad Ilyas Sikki (2014) dengan bantuan *fingerprint* sebagai otentikasi *voter* atau pemilih. Terlebih, Muhammad Ilyas sikki menyebutkan bahwa protokol tersebut dapat dikembangkan dan diimplementasikan lebih lanjut. Penelitian lebih lanjut dikembangkan dan diimplementasikan oleh Caesar Firdaus (2017). Penggunaan *Two Central Facilities Protocol* juga harus memenuhi kebijakan *Secure Voting,* dimana *secure voting* sendiri memiliki arti protokol yang menjamin privasi individu dan mencegah segala bentuk kecurangan serta memiliki tingkat keamanan yang cukup baik, dimana terdiri dari *Central Legitimazation Agency* (CLA) untuk pengesahan pemilih dan *Central Tabulating Facility* (CTF) untuk perhitungan suara (Schneier, 1996).

Penggunaan *Two Central Facilities Protocol* pada penelitian tersebut diimplementasikan untuk sistem monitoring kontrak kerjasama, namun pada penelitian Caesar Firdaus tidak ada sistem otentikasi, maka dari itu penelitian kali ini penggunaan *Two Central Facilities Protocol* diimplementasikan pada sistem layanan pengaduan dengan bantuan OTP untuk otentikasi pelapor.

Dalam penelitian sistem layanan pengaduan kali ini pun, masalah keamanan dan validasi juga merupakan masalah yang paling penting untuk didiskusikan pertumbuhan pengguna internet juga terdapat *trend* meningkatnya kejahatan internet (*Cybercrime*) di Indonesia bahkan masuk 2 besar asal serangan kejahatan internet dunia dan dianggap sebagai negara paling beresiko terhadap serangan keamanan teknologi informasi (Danuri, 2017). Selain karena hal keamanan dan validasi yang tidak bisa dijamin data tersebut akan aman dan keasliannya, penerapan layanan bantuan masyarakat masih sangat sulit untuk diterapkan di Indonesia, yaitu pada pemahaman masyarakat yang belum mengerti benar akan layanan tersebut dan karena adanya beberapa kalangan masyarakat Indonesia yang kurang mengerti akan perkembangan teknologi.

Oleh karena itu diperlukan metode yang dapat menjaga keamanan dan validasi informasi atau data tersebut, metode yang dimaksud adalah Kriptografi. Dimana kriptografi memiliki arti sebuah metode algoritma untuk mengamankan data. Dalam kriptografi ada beberapa istilah penting atau utama yaitu enkripsi dan dekripsi. Dimana enkripsi adalah suatu proses mengubah *plaintext* (teks asli) menjadi *chipertext* (teks yang sudah disandikan). Sedangkan dekripsi adalah

kebalikannya yaitu mengubah *chipertext* menjadi *plaintext* (Hendrayanto, 2012). Pada sistem keamanan dalam layanan pengaduan ini menggunakan protokol yaitu *Two Central Facilities* dan penggunaan *One Time Password* (OTP). Penelitian kali ini juga menambahkan penggunaan algoritma kriptografi sebagai keamanan dari sistem pelayanan pengaduan yaitu algoritma RC6.

One Time Password (OTP) adalah sebuah *password* yang hanya berlaku untuk sesi *login* tunggal atau transaksi tunggal. Berbeda dengan penggunaan *password* statis, OTP tidak menggunakan *password* yang sama untuk setiap *login* atau transaksi, sehingga jika pihak yang tidak berkepentingan berhasil merekam *password* OTP yang sudah digunakan maka dia tidak akan dapat menyalahgunakan *password* tersebut karena sudah tidak berlaku lagi. Untuk dapat membuat sebuah *password* OTP, digunakan salah satu metode kriptografi, yaitu fungsi hash, dan untuk pemilihan karakternya dipilih secara acak dengan *Pseudo Random Number Generator* (Sakti, 2015). Penggunaan OTP menurut Kim (2009) untuk meningkatkan kesulitan dalam mengakses sistem dengan terbatas, dimana kondisi ini nilai OTP akan dienkripsi menggunakan *hashing* maka akan membuat *hacker* sulit untuk masuk kedalam sistem.

Kelebihan dari algoritma RC6 yaitu kode untuk RC6 lebih sederhana dibandingkan dengan Rijndael, namun performa Rijndael pada *smart card* masih melebihi performa RC6 (Panggabean, 2007). Selain itu jika diimplementasikan pada sistem layanan pengaduan, karena isi dari laporan tersebut banyak lalu jika pada penelitian selanjutnya ditambah dengan bukti pelaporan maka algoritma RC6 sangat cocok dengan hal tersebut karena jika menggunakan algoritma lain ukuran *file* akan semakin membesar dan membutuhkan waktu yang lama untuk proses enkripsi dan dekripsinya. Pada penelitian Caesar Firdasus memakai algoritma AES menghasilkan beberapa kali peningkatan ukuran *file* dari aslinya.

Penelitian mengenai penerapan *Two Central Facilities Protocol* selain pada sistem *e-voting* yaitu oleh Caesar Firdaus (2017) ditemukan penemuan dalam penelitiannya yaitu, waktu untuk proses enkripsi dan dekripsinya akan bertambah sesuai dengan ukuran *file* meningkat 3,785 menjadi 4,095 kali. Dapat disimpulkan bahwa itu terjadi karena file pdf diubah menjadi heksadesimal menghasilkan dua kali peningkatan ukuran dari *file* aslinya, lalu penelitian yang dilakukan adalah

mengenai *monitoring system* di perusahaan dan oleh Igor Bony Tua Panggabean (2007) mengenai perbandingan algoritma RC6 dengan Rijndael pada AES. Sedangkan penelitian kali ini, penelitian akan dilakukan pada sistem layanan pengaduan dengan algoritma RC6 yang akan mengenkripsi dan mendekripsi string. Oleh karena itu pembentukan sistem layanan pengaduan ini dibentuk untuk menghindari pelapor palsu dan laporan yang palsu maka perlu adanya sistem verifikasi untuk dimintai pertanggung jawaban selain itu sistem ini juga diharapkan dapat membantu masyarakat dalam melaporkan suatu kejadian ke kantor polisi tanpa perlu datang langsung menuju kantor polisi.

1.2 Rumusan Masalah

Berdasarkan latar belakang diatas, rumusan masalah dalam penelitian ini yaitu:

1. Bagaimana pelapor membuat laporan pada aplikasi layanan pengaduan jika terjadi suatu kejadian dan ingin melaporkannya ke kantor polisi?
2. Bagaimana peran *One Time Password* (OTP) untuk proses otentikasi pada *user login* hingga *user* menerima hasil laporan tersebut?
3. Bagaimana peran algoritma RC6 untuk mengamankan data pada proses enkripsi dan dekripsi data pelapor?

1.3 Tujuan Penelitian

Sesuai dengan rumusan masalah yang ada, maka tujuan penelitian ini yaitu:

1. Membangun sistem layanan pengaduan menggunakan *Two Central Facilities Protocol* dan mengamankan data pelapor.
2. Mengimplementasikan *One Time Password* (OTP) sehingga jika pihak yang tidak berkepentingan berhasil merekam nomer OTP yang sudah digunakan maka dia tidak akan dapat menyalahgunakan nomer tersebut karena sudah tidak berlaku lagi.
3. Mengimplementasikan keamanan data dengan menggunakan algoritma RC6 pada sistem layanan pengaduan dengan *Two Central Facilities Protocol.*

1.4 Manfaat Penelitian

1 Bagi peneliti, hasil penelitian ini diharapkan dapat dijadikan bahan untuk menambah wawasan dalam bidang kriptografi khususnya keamanan data.

2 Bagi masyarakat, sistem ini dapat memberikan pelayanan kemudahan dalam melakukan pelaporan dan memilih kantor polisi yang dekat dengan tempat kejadian agar dapat penanganan yang cepat.

3 Bagi Polisi, memberikan kemudahan penyortiran data laporan sesuai dengan data yang dimasukan oleh pelapor agar data laporan tersebut tidak bercampur dengan kantor polisi lain dan polisi bisa langsung melakukan tindakan.

1.5 Batasan Masalah

Adapun batasan masalah dalam penelitian ini adalah sebagai berikut:

1. Instansi yang terkait hanya dengan kantor polisi.
2. Sistem hanya dapat digunakan oleh NIK yang sudah terdaftar disistem saja.
3. Penelitian ini belum bisa memilih kantor polisi yang paling dekat dengan kejadian atau dengan kata lain *shortestpath*.
4. Karena penelitian ini bukan termasuk dalan penelitian *mobile android* maka pada saat menunjukan lokasi tempat kejadian perlu adanya koordinat karena tidak adanya GPS.
5. Pengiriman otentikasi melalui *email*.
6. Sistem ini hanya mencakup Bandung Timur saja.
7. Jenis laporan yang akan diberikan hanya jenis laporan yang dapat ditinjak lanjuti oleh Polsek saja.