BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi yang begitu pesat saat ini memegang peranan penting dalam segala aspek kehidupan manusia. Teknologi informasi membuat masyarakat dapat membuat, mengubah, menyimpan dan menyebarkan informasi dengan mudah. Dengan kemajuan teknologi informasi data dapat dikelola dan bermanfaat bagi individu maupun kelompok sehingga menjadi informasi yang sangat berharga. Selain dapat bertukar informasi dengan mudah teknologi informasi juga membuka peluang bagi orang-orang yang ingin mencuri data dan informasi untuk digunakan dalam kepentingan tertentu. Pada tahun 2018 perusahaan keamanan Gemalto melaporkan ada 4,5 miliar data telah dicuri selama enam bulan pertama dan hanya 4 persen dari data tersebut yang terlindungi enkripsi oleh pemiliknya. Kasus tersebut menunjukkan bahwa perkembangan teknologi informasi belum sejalan dengan sistem keamanan yang diberikan.

Kriptografi sebagai ilmu untuk menjaga kerahasiaan pesan dapat digunakan dalam mengamankan informasi dan data. Teknik pengamanan informasi yang dilakukan yaitu dengan cara mengubah pesan menggunakan suatu metode enkripsi sehingga tidak dapat dibaca secara langsung oleh pihak yang tidak berhak. Dengan kriptografi informasi yang dapat dibaca dan dipahami dengan bahasa tertentu diubah ke dalam bentuk sandi tertentu yang susah dipahami dari segi bahasa apapun. Block cipher merupakan salah satu algoritma kriptografi yang menggunakan kumpulan bit dengan panjang tetap untuk mengenkripsi pesan. Teknik perancangan kriptografi block cipher dapat dilakukan dengan memodifikasi pola atau algoritma yang sudah ada sehingga dapat menunjukkan ciri khas dari pola tertentu.

Peta administrasi Kalimantan Barat adalah peta yang menginformasikan batas-batas administratif terkecil sampai terbesar wilayah Kalimantan Barat. Terletak di pulau kalimantan, provinsi Kalimantan Barat berbatasan langsung dengan Sarawak Malaysia di bagian utara, Laut Jawa di bagian selatan, Kalimantan

Tengah di sebelah timur, dan Laut Natuna serta Selat Karimata di sebelah barat. Sampai dengan saat ini provinsi Kalimantan Barat terbagi dalam 14 wilayah administratif kabupaten/kota yang kemudian kabupaten/kota tersebut terbagi lagi dalam kecamatan dan desa yang jumlahnya mencapai ratusan. Pembagian wilayah kabupaten/kota serta batas administrasi provinsi Kalimantan Barat memiliki bentuk yang abstrak sehingga peta administrasi Kalimantan Barat menarik untuk dijadikan pola dalam perancangan teknik kriptografi block cipher. Bentuk pola abstrak peta administrasi Kalimantan Barat akan membuat rancangan algoritma kriptografi unik dan berbeda dengan algoritma kriptografi yang sudah ada.

S-box merupakan teknik dasar yang diperlukan dalam merancang blok cipher yang telah ditetapkan oleh National Institute of Standard and Technology (NIST). S-box dapat menghasilkan hubungan nonlinier antara kunci dengan ciphertext dan memberikan efek confusion dari prinsip shannon. Algoritma block cipher yang telah ditetapkan sebagai standar pengamanan informasi dunia seperti DES (Data Encryption Standard) dan kemudian digantikan AES (Advanced Encryption Standard), keduanya menggunakan s-box yang bersifat statis. Kondisi statis yang dimaksud adalah nilai pada setiap entri selalu tetap dan secara fungsi bersifat satu-ke-satu. Hal ini dapat mempermudah cryptoanalyst untuk melihat pola dan kemudian dapat memprediksi perilaku dari pola berdasarkan masukan, sehingga kompleksitas waktu dan ruang untuk melakukan cryptoanalysis menjadi lebih pendek. Pada penelitian yang berjudul Dynamic AES-128 with Key-Dependent S-box, penelitian berhasil menghasilkan sebuah rancangan baru AES dinamis menggunakan key-dependent s-box yang lebih baik dibandingkan AES standard (Mahmoud dkk., 2013).

Penelitian ini merancang teknik kriptografi block cipher dengan pola dan algoritma yang memberikan ciri khas pola peta administrasi kalimantan barat di dalam proses pertukaran kode bitnya. Kalimantan Barat merupakan cakupan wilayah yang sangat luas sehingga untuk dapat merepresentasikannya secara utuh pola dalam teknik kriptografi yang dirancang menggunakan pertukaran kode dengan panjang 256 bit. Dengan dilakukan penelitian ini diharapkan dapat menghasilkan teknik kriptografi baru yang memiliki ciri khas berbeda dengan

teknik kriptografi yang sudah ada. Teknik kriptografi yang dirancang menggunakan S-box dinamis (Key Dependent S-box) yang diharapkan dapat menambah kompleksitas enkripsi yang dihasilkan. Penggunaan S-box dinamis diharapkan mampu menambah kekuatan dari teknik kriptografi yang dirancang sehingga sulit untuk dipecahkan oleh *cryptoanalysis*.

1.2 Perumusan Masalah

Setiap teknik kriptografi yang umum digunakan selalu berusaha dicari kelemahannya oleh *cryptoanalysis*. Begitu kelemahan dari teknik kriptografi ditemukan maka teknik tersebut sudah tidak dapat lagi digunakan untuk mencegah pencurian data. Penelitian ini akan membahas bagaimana merancang teknik kriptografi baru yang tahan terhadap serangan *cryptoanalysis*. Perancangan pola yang dapat merepresentasikan peta kalimantan barat sekaligus efektif untuk digunakan dalam pertukaran kode bit menjadi tantangan dalam penelitian ini. Penggunaan serta bagaimana pembangkitan s-box dinamis dalam teknik kriptografi yang akan dirancang membuat penelitian ini menarik untuk dilakukan.

1.3 Tujuan Penelitian

Penelitian ini bertujuan untuk menghasilkan teknik kriptografi block cipher baru yang tahan terhadap serangan *cryptoanalysis*. Teknik kriptografi diharapkan dapat merepresentasikan ciri khas pola peta administrasi kalimantan barat dalam pertukaran kode bitnya. Penelitian juga melihat pengaruh penggunaan s-box dinamis terhadap ketahanan teknik kriptografi yang dihasilkan.

1.4 Pembatasan Masalah

Agar tujuan dapat tercapai dan tidak keluar dari permasalahan semula, maka dilakukan pembatasan masalah, antara lain :

1. Peta administrasi kalimantan barat yang hendak direpresentasikan dalam penelitian ini berupa batas provinsi dan pembagian wilayah kabupaten/kota.

2. Teknik kriptografi block cipher yang hendak dirancang menggunakan panjang 256 bit dalam proses pertukaran kode bitnya.

3. Rancangan algoritma akan diimplementasikan dalam aplikasi surat elektronik (*email*) yang dibangun menggunakan bahasa pemrograman php.

4. Perancangan aplikasi surat elektronik (*email*) pada penelitian ini berfokus pada teknik pengamanan data sehingga tidak membahas analisa kebutuhan secara menyeluruh.

5. Aplikasi surat elektronik (*email*) yang dirancang memungkinkan pengguna untuk saling bertukar pesan hanya melalui aplikasi yang sama.

6. Distribusi kunci pada algoritma tidak dibahas dalam penelitian ini.

1.5 Sistematika Penulisan

Adapun sistematika penulisan dari tugas akhir ini disusun dalam lima bab yang terdiri dari :

1. Bab I Pendahuluan mencakup latar belakang, perumusan masalah, tujuan penelitian, pembatasan masalah, serta sistematika penulisan.

2. Bab II Tinjauan Pustaka berisi uraian penjelasan, meliputi Kriptografi, Block Chiper, Advance Encryption Standard (AES), serta Mode Operasi Block Chiper.

3. Bab III Metodologi Penelitian menjelaskan tentang langkah-langkah yang akan dilakukan dalam perancangan teknik kriptografi block chiper baru yang memiliki ciri khas pola peta administrasi Kalimantan Barat serta perancangan aplikasi email.

4. Bab IV Implementasi dan Hasil memaparkan mengenai implementasi teknik kriptografi yang telah dihasilkan ke dalam aplikasi email dan hasil yang telah diperoleh.

5. Bab V Kesimpulan dan Saran berisi uraian kesimpulan dan saran mengenai perancangan teknik kriptografi maupun aplikasi, serta penelitian yang telah dilakukan.