BAB I
PENDAHULUAN

Bab ini akan menjelaskan mengenai latar belakang masalah dilaksanakannya penelitian, rumusan masalah, tujuan penelitian, batasan masalah, dan sistematika penulisan.

1.1. Latar Belakang

Sosial media merupakan alat komunikasi yang memberikan kemudahan agar masyarakat tetap terhubung satu sama lain. Masyarakat dapat melakukan berbagai kegiatan menggunakan sosial media, didalam sosial media pengguna dapat membagikan informasi umum bahkan informasi yang bersifat pribadi karena sosial media menyediakan fasilitas seperti membagikan status, foto, bahkan fasilitas untuk bisa mengirimkan pesan pribadi antar pengguna. *Electronic Commerce* atau sering disebut *e-commerce* juga banyak dimanfaatkan oleh masyarakat yang ingin memperkenalkan, menawarkan serta melakukan proses jual beli produk. Pada situs *e-commerce* pengguna diberi fasilitas untuk memberikan deskripsi serta foto barang yang akan dijual, fasilitas untuk melakukan transaksi pembayaran, hingga fasilitas *live chat* yang dapat berisikan informasi penting. *Electronic Commerce* merupakan contoh pemanfaataan lain dari sosial media yang digunakan sebagai alat untuk berorganisasi dan berbisnis.

Menurut Sherlyanita & Rakhmawati (2016) penggunaan internet diseluruh dunia mencapai 31,7 miliar dan disetiap tahunnya tumbuh hingga mencapai 7,6 persen. Penggunaan sosial media mencapai angka 2,2 miliar dengan pengguna *mobile* mencapai 3,7 miliar. Selain itu menurut KOMINFO di Indonesia sendiri pengguna sosial media mencapai 65 juta orang, sebanyak 33 juta orang aktif per harinya, 55 juta pengguna aktif yang memakai perangkat *mobile* dalam pengaksesan per bulan, dan sekitar 28 juta pengguna aktif yang menggunakan perangkat *mobile* per hari. Hal ini menunjukan bahwa sosial media ataupun *e-commerce* memiliki peranan penting dalam kehiduapan masyarakat saat ini.

Cara untuk dapat memiliki akun sosial media atau akun *e-commerce* tidak sulit, masyarakat selaku pengguna diberikan kemudahan dalam melakukan registrasi yaitu dengan mengisi *form* registrasi kemudian data tersebut akan langsung disimpan dan dijadikan data pribadi dari pengguna itu sendiri, dengan adanya

kemudahan dalam melakuan pendaftaran akun tersebut, menyebabkan banyak masyarakat membuat akun diberbagai sosial media dan *e-commerce* seperti *Facebook, Twitter, Instagram, Google, Whatsapp*, Lazada, Tokopedia dan lain sebagainya. Dalam pendaftaran suatu akun sosial media selain data pribadi, pengguna diharuskan membuat *username* dan *password* untuk dapat melakukan login. Data login merupakan data yang harus dilindungi karena dapat memicu terjadinya penyalahgunaaan akun oleh orang yang tidak bertanggung jawab.

Password cracking merupakan program yang dibuat untuk membongkar sebuah *password* yang telah terenkripsi dengan menggunakan algoritma tertentu dengan cara mencoba semua kemungkinan (Pramudita, 2010). E*xhautive attack* atau *bruteforce attack* merupakan contoh penyerangan untuk mendapatkan akun seseorang secara tidak sah dengan mencoba semua kemungkinan kunci yang ada, serangan ini sering dilakukan *hacker* untuk mendapatkan data dari seorang pengguna dengan memanfaatkan pemrosesan komputer. Selain itu terdapat penyerangan lain seperti penyebaran *malware* dengan tujuan untuk menguasai data pengguna, penyerangan menggunakan situs palsu yang digunakan untuk mengelabui pengguna sehingga berhasil mendapatkan *username* dan *password.* Kerugian yang ditimbulkan apabila *hacker* berhasil melakukan serangan yaitu terjadinya pencurian data penting dari pengguna yang kemudian digunakan untuk hal yang tidak baik seperti pembuatan akun palsu, biasanya akun palsu ini dibuat untuk menjatuhkan seseorang, kemudian akun palsu dapat digunakan untuk penipuan, penyalahgunaan akun untuk menyebarkan pornografi, penyalahgunaan akun untuk dijadikan sebagai media provokasi, bahkan dalam kasus *e-commece* pencurian data ini dapat menyebabkan kerugian materil yang tentunya akan merugikan pengguna.

Salah satu cara yang dapat dilakukan untuk mengantisipasi adanya penyalahgunaan akun sosial media dan *e-commerce* adalah dengan menggunakan dua faktor otentikasi sebagai keamanan tambahan dalam melakukkan registrasi. Dengan adanya tambahan keamanan ini dapat mengurangi resiko pembuatan akun palsu dan kerugian yang akan ditimbulkan. Pembangkitan kode otentikasi bertujuan untuk verifikasi akun, sehingga pada saat registrasi pengguna harus melakukan verifikasi untuk dapat menggunakan layanan sosial media maupun *e-commerce*.

Pada tahun 2013, penelitian Sediyono, Santoso, & Suhartono (2013) menerapakan OTP dengan menggunakan MD5, hasil penelitian menunjukan bahwa OTP yang dihasilkan pada penelitian ini selalu berbeda, waktu penggunaan OTP dibatasi selama 3 menit sehingga kode susah untuk dipecahkan oleh kriptanalis. Kemudian pada tahun yang sama, Santoso (2013) menerapkan OTP dengan menggunakan SHA, kode yang dibangkitkan dari SHA sulit ditebak oleh kriptanalis dan lebih baik dibandingakan dengan *hash* MD5. Pada penelitian Nugroho, Judie Putra, & Ramadhan (2016) melakukan penelitian dalam pembangkitan kode otentikasi yang menerapkan OTP dan algoritma AES. Hasil penelitian menyatakan bahwa penggunaan algoritma kriptografi dapat digunakan untuk pembangkitan kode otentikasi dan juga sebagai tambahan keamanan.

Melihat dari penelitian terdahulu dalam kasus verifikasi akun dapat dilakukan implementasi dari algoritma kriptografi dan fungsi *hash* untuk pembangkitan kode otentikasinya kemudian kode yang telah didapat akan dikirimkan dengan SMS kepada nomor telepon dari pengguna akun sebagai syarat untuk mengecek apakah yang melakukan login merupakan mesin, pemilik asli atau orang lain. Waktu pemasukan kode otentikasi dibatasi selama beberapa waktu, jika dapat memasukan kode otentikasi maka pengguna dapat menggunakan layanan sosial media dan jika tidak, maka tidak dapat login dan harus meminta kode otentikasi kembali agar dapat menggunakan layanan sosial media.

Pada penelitian ini algoritma yang diimplementasikan untuk membangkitkan kode otentikasi adalah algoritma kriptografi *Data Encryption Standard* (DES) karena algoritma DES menggunakan kunci simetris yang berbasis cipher blok sehingga dapat melakukan proses dengan cepat, selain itu pemilihan algoritma DES dapat memberikan nilai *avalanche effect* yang baik. Menurut Sadikin (2012), algoritma DES memberikan efek *avalanche* yang kuat terhadap perubahan kunci karena dari dua percobaan yang pernah dilakukan didapatkan perbedaan nilai bit antara hasil enkripsi yang satu dengan yang lainnya yang menunjukan bahwa terdapat efek *avalanche* yang baik pada plainteks yang diuji.

Pada penelitian tahun 2011, Algoritma DES telah digunakan untuk enkripsi dan dekripsi pesan, pada penelitian ini implementasi dari algoritma DES dikembangkan dalam bahasa pemrograman Java hasil dari penelitian menyebutkan bahwa waktu

untuk melakukan enkripsi dan dekripsi relatif sama pada setiap prosesnya (Primartha, 2011).

Penelitian tahun 2012, Algoritma DES digunakan dalam enkripsi dan dekripsi SMS penelitian ini membahas mengenai pengamanan terhadap pesan singkat yang akan dikirimkan kepada orang lain dengan menerapkan algoritma DES, program aplikasi yang dibuat dinamakan SMSCrypt yang kemudian diuji coba pada *emulator* android, hasil dari uji coba program aplikasi tersebut dapat membantu keamanan pesan yang dikirim (Hendrayanto & Nilawati, 2012).

Tahun 2013, penelitian mengenai perbandingan algoritma DES dan Baker Map yang diimplementasikan pada citra digital menunjukan bahwa algoritma DES memiliki waktu ketahanan $1.28x10^{12}$ tahun terhadap serangan *brute force* karena memiliki kemungkinan kunci yang jauh lebih sedikit dibandingkan dengan algoritma Baker Map. Pada penelitian disebutkan pula bahwa algoritma DES memiliki nilai *avalanche effect* yang lebih baik dibandingkan dengan algoritma Baker Map, algoritma DES benar-benar mengacak bit karena memiliki sifat subtitusi dan permutasi (Nurdinta, Usman, & Aulia, 2013).

Pada tahun 2016, terdapat penelitian yang membandingkan algoritma DES dan algoritma AES pada teknologi QR-Code hasil dari penelitian menyebutkan bahwa algoritma DES memiliki waktu yang lebih cepat, dan memiliki ukuran file lebih kecil dibandingkan algoritma AES, tetapi memiliki tingkat keakuratan yang sama dalam pembacaan QR-Codenya (Depayusa, Diana, & Halim, 2016). Ditahun yang sama, dilakukan penelitian terhadap sistem listrik prabayar dengan mengkombinasikan algoritma DES dan algoritma RSA untuk membangkitkan kode voucher listrik prabayar dengan merangkai 16 digit bilangan heksadesimal dari hasil enkripsi algoritma DES dan RSA (Kusmiati, Faruk, & Dewi, 2016).

Berdasarkan penelitian terdahulu masih didapati kekurangan pada algoritma DES seperti penggunaan kunci yang sedikit sehingga memicu *haker* untuk melakukan serangan, oleh karena itu pada pembangkitan kode otentikasi ini algoritma DES akan dimodifikasi. Modifikasi berdasarkan pada penelitian Santosa, Bayu, & Wowor (2014) yang melakukan modifikasi dengan menambahkan proses xor dan *concatenate* pada pembangkitan kunci internal. Berdasarkan penelitian yang telah dilakukan tersebut, maka pada penelitian ini modifikasi akan dilakukkan

pada bagian permutasi kompresi (PC-1) dan bagian S-box, Modifikasi yang dilakukan mengacu pada prinsip *Shannon* yaitu *Confusion* dan *Difusion*. Penelitian diharapkan dapat memberikan hasil pengujian yang baik karena suatu algoritma yang bagus harus memiliki dua sifat operasi yaitu *Confusion* dan *Difusion* (Shannon, 1949). Setelah algoritma DES dimodifikasi kemudian hasil enkripsinya akan melalui proses *hashing* dengan menggunakan SHA-1. Penggunaan fungsi *hash* pada penelitian ini adalah untuk memberikan pilihan pada kode otentikasi yang dirandom, karena fungsi hash memberikan keluaran yang lebih panjang. Untuk menghasilkan kode otentikasi yang memiliki kekuatan yang baik, dalam pembangkitan kode otentikasinya akan menerapkan metode *One Time Password* (OTP) karena untuk saat ini penggunaan OTP masih menjadi keamanan tambahan yang baik digunakan pada saat melakukan verifikasi. OTP berfungsi untuk kontrol akses terhadap login yang tidak sah, dalam penelitian ini OTP bertujuan untuk memberikan batasan waktu validasi terhadap kode otentikasi yang didapatkan, sehingga kode otentikasi hanya dapat digunakan sekali dan memiliki batas waktu kadaluarsa.

Untuk mengetahui dan dapat membandingkan, pengujian *avalanche effects* dan *randomness test* akan dilakukan terhadap algoritma DES standar maupun pada algoritma DES yang dimodifikasi pada bagian permutasi kompresi (PC-1) dan bagian S-box. Peningkatan nilai *avalanche effects* akan berdampak pada kompleksitas hasil enkripsi sehingga dalam pembangkitan kode otentikasi dengan menggunakan algoritma DES, SHA-1, dan metode OTP ini diharapkan dapat menghasilkan kode yang sangat acak sehingga tidak mudah untuk diprediksi.

1.2. Rumusan Masalah

Berdasarkan uraian latar belakang yang telah dijelaskan, dapat dirumuskan permasalahan pada penelitian ini adalah sebagai berikut:

1. Bagaimana melakukan proses modifikasi algoritma *Data Encryption Standard* (DES)?
2. Bagaimana mengimplementasikan algoritma *Data Encryption Standard* (DES) yang telah dimodifikasi, fungsi *hash* SHA-1 dan metode OTP pada proses pembuatan kode otentikasi?

3. Bagaimana hasil pengujian *Data Encryption Standard* (DES) yang telah dimodifikasi?
4. Bagaimana membuktikan kode otentikasi dapat digunakan sebagai tambahan keamanan?

1.3. Tujuan Penelitian

Tujuan dari penelitian ini adalah:

1. Melakukan modifikasi algoritma *Data Encryption Standard* (DES).
2. Memberikan hasil implementasi algoritma *Data Encryption Standard* (DES) yang telah dimodifikasi, fungsi *hash* SHA-1 dan metode OTP pada proses pembuatan kode otentikasi untuk registrasi *online*.
3. Memberikan hasil pengujian terhadap algoritma *Data Encryption Standard* (DES) yang telah dimodifikasi.
4. Melakukan analisis hasil kode otentikasi terhadap percobaan *exhautive attack*.

1.4. Batasan Masalah

Batasan masalah pada penelitian ini adalah:

1. Modifikasi algoritma DES hanya dilakukan pada bagian PC-1 dan S-box.
2. Penelitian dilakukan pada proses pembuatan kode otentikasi.
3. Kode otentikasi dibangkitkan dari 64 bit pesan dan 64 bit kunci.
4. Kode otentikasi berbasis heksadesimal.
5. Pembangkitan kode otentikasi hanya dilakukan pada saat registrasi.
6. OTP digunakan pada saat login pertama kali.
7. Pengujian modifikasi algoritma *Data Encryption Standard* (DES) dilakukan menggunakan tes *avalanche effects* dan *randomness test*.

1.5. Sistematika Penulisan

Pada bagian sistematika penulisan ini akan diuraikan mengenai penjelasan tiap bab.

BAB I PENDAHULUAN

Bab ini menjelaskan bagaimana penelitian itu bisa muncul dan isinya mengenai konteks penelitian yang dilakukan, diawali dengan latar belakang masalah, rumusan masalah, tujuan penelitian, manfaat penelitian, batasan masalah, dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Bab ini menjelaskan mengenai teori-teori yang digunakan dan menunjang dalam melakukan penelitian.

BAB III METODOLOGI PENELITIAN

Bab ini menjelaskan langkah-langkah penelitian yang akan dilakukan, dimulai dari desain penelitian, fokus penelitian, kemudian alat dan bahan yang digunakan untuk penelitian dan yang terkahir adalah metode penelitian.

BAB IV HASIL DAN PEMBAHASAN

Bab ini menjabarkan hasil penelitian yang telah dilakukan dan analisisnya. Semua pertanyaan mengenai masalah yang diangkat dalam tema skripsi dibahas di sini. Yaitu tentang proses pengumpulan data, pengembangan model, implementasi sistem, studi kasus, desain eksperimen, dan analisa.

BAB V KESIMPULAN DAN SARAN

Bab ini berisi kesimpulan dan saran bagi peneliti selanjutnya dari hasil penelitian yang telah dilakukan.