BAB I

PENDAHULUAN

Dalam bab ini akan dibahas latar belakang dilaksanakannya penelitian, rumusan masalah, batasan masalah, tujuan penelitian, dan sistematika penulisan.

1.1 Latar Belakang

Penggunaan internet untuk berinteraksi sosial atau berbelanja secara *online* tiap tahun semakin banyak manusia yang memanfaatkannya, manusia dapat mendaftarkan diri pada jejaring media sosial atau situs jual beli *online* yang ada. Dan jejaring media sosial yang populer dikalangan masyarakat menurut *survey* We Are Social (Kemp, 2015) sampai pada Januari 2015 diantaranya adalah Facebook, Whatsapp, Twitter, dan Instagram, kemudian untuk situs belanja *online* atau *marketplace* yang populer di Indonesia diantaranya adalah Bukalapak, Kaskus, Lazada, OLX, Tokopedia dan lain sebagainya.

Agar terdaftar pada jejaring media sosial atau situs jual beli *online* pun tidak begitu sulit dan tidak dipersulit oleh birokrasi, apabila di dunia nyata untuk melakukan pendaftaran biasanya harus menuliskan data diri pada sebuah *form* kertas kemudian ada beberapa yang meminta untuk mencantumkan foto kopi identitas diri serta foto diri, maka berbeda ketika semuanya terintegrasi secara *online*. Pendaftar dapat langsung meng-*input*-kan data dirinya pada *form* registrasi yang sudah disediakan secara *online*, kemudian Pendaftar dapat langsung mengunggah foto diri yang akan ditampilkan atau disimpan sebagai informasi dasar milik Pendaftar.

Selanjutnya pada sisi pemilik jejaring sosial atau situs jual beli *online*, tentu ingin semua pengguna jejaring sosial atau situs jual beli *online*-nya menggunakan jejaring sosial atau situs jual beli *online*-nya dengan baik dan benar,

Iman Muhamad Ramadhan, 2016
IMPLEMENTASI KRIPTOGRAFI AES DAN OTP DALAM MEMBANGKITKAN KODE OTENTIKASI UNTUK AKTIVASI ONLINE MEMBER BARU YANG DIKIRIM MELALUI SMS
Universitas Pendidikan Indonesia | repository.upi.edu | perpustakaan.upi.edu

serta penggunanya diisi oleh manusia tanpa akun robot. Karena akun robot atau akun palsu dapat merugikan pemilik jejaring sosial atau situs jual beli online,

sebagai contoh berita yang dilansir Okezone.com Kasus Lazada dapat memberikan dampak buruk bagi *e-Commerce*, dimana Lazada terkait kasus penipuan pembelian iPhone tapi yang dikirimkan ke konsumen adalah sabun mandi, kemudian Pengelola Lazada Indonesia memastikan pembelian Apple iPhone 6 Plus oleh Danish Darusman yang mengaku hanya menerima barang sabun mandi padat, dilakukan melalui *merchant* atau pedagang yang memanfaatkan *platform* Lazada (Panji, 2015), Muhammad Jumadi Sekjen Indonesia Telecommunications Users Group menerangkan (dalam Wiratri, 2015) "UU No. 8 perlindungan konsumen bisa digunakan oleh konsumen untuk mengklaim hal tersebut. Peristiwa terkait Lazada dapat menjadi preseden buruk bagi *e-commerce* kalau sampai terjadi salah kirim barang bisa jadi bumerang untuk *e-commerce* lain di Indonesia". Kasus penipuan melalui *e-commerce* kembali terjadi pada saat Hari Belanja *Online* Nasional (Harbolnas) tahun 2015, pada saat Harbolnas ada penjual yang dengan sengaja menaikan harga berkali-kali lipat, kemudian memberikan diskon yang sangat besar, tentu ini adalah tindakan penipuan terhadap konsumen yang pada akhirnya merugikan dan mencoreng nama baik *e-Commerce* dengan berita-berita yang tersebar, Bachtiar Rifai, *Co-founder* Kofera.com (dalam Damar, 2015), menurutnya kasus ini lebih menyorot pada beberapa oknum penjual yang nakal dan bukannya bisnis *e-Commerce* sendiri, "Dari sisi analisis, sebenarnya dalam kasus ini bukan e-Commerce yang nakal tapi beberapa oknum penjual yang menaikkan harga dengan besar-besaran lalu memberikan diskon", ujar Bachiar. Dilihat dari beberapa kasus diatas oleh karena itu pemilik jejaring sosial baru atau situs jual beli *online* baru perlu melakukan tindakan preventif untuk menghindari pembuatan akun-akun robot, akun-akun palsu atau akun-akun nakal, tindakan preventif yang dapat dilakukan oleh pemilik jejaring sosial baru atau situs jual beli *online* baru adalah

Iman Muhamad Ramadhan, 2016
IMPLEMENTASI KRIPTOGRAFI AES DAN OTP DALAM MEMBANGKITKAN KODE OTENTIKASI UNTUK AKTIVASI ONLINE MEMBER BARU YANG DIKIRIM MELALUI SMS
Universitas Pendidikan Indonesia | repository.upi.edu | perpustakaan.upi.edu

mengimplementasikan langkah-langkah keamanan untuk menghindari pembuatan akun palsu atau akun nakal

Karena semakin banyaknya media sosial dan situs jual beli *online* di dunia maya, ada saja pihak-pihak yang memanfaatkannya untuk menguntungkan dirinya atau merugikan orang lain, dengan mendaftarkan akun palsu atau akun robot pihak-pihak yang tidak bertanggungjawab dapat melakukan tindakan-tindakan tidak terpuji, seperti menipu, menghina orang, menyebarkan fitnah, atau memalsukan dukungan. Sebagai contoh menjelang pemilihan kepala daerah Kabupaten Pangkajene Kepulauan, Sulawesi Selatan, sejumlah akun palsu di media jejaring sosial bermunculan (Badauni, 2015) selain itu kembali ke masa kampanye Pemilihan Umum Presiden tahun 2014 beberapa media massa *online* melansir beberapa berita tentang akun robot yang ikut meramaikan kampanye Pilpres 2014 diantaranya Viva.co.id (Setiawan & Sukmawati, 2014) Puluhan ribu akun palsu atau biasa disebut akun robot bermunculan di media sosial pada masa kampanye Pemilu Presiden 2014. Dan media massa *online* lainnya yaitu Detik.com (Suryadhi, 2014) Debat capras babak ketiga Minggu malam memang juga berlangsung seru di dunia maya. Tentu maraknya akun palsu yang memprovokasi untuk menyerang atau memalsukan dukungan melalui media sosial agar menarik perhatian kepada salah satu calon kepala dareah dapat mengganggu jalannya pemilihan umum.

Salah satu cara yang dilakukan untuk menjaga keamanan situs jejaring sosial baru atau situs jual beli *online* baru agar tidak membuat akun robot atau akun palsu adalah dengan membangkitkan kode otentikasi sebagai salah satu cara verifikasi akun, agar akun yang telah didaftarkan dan diverifikasi dapat diaktifkan. Dan untuk kasus aktivasi akun dapat mengimplementasikan algoritma kriptografi dalam pesan aktivasi pada kode otentikasi yang dikirim melalui SMS yang ditujukan ke nomor telepon genggam pribadi milik pendaftar sebagai metode untuk mengecek apakah pendaftar robot atau bukan, dimana kode otentikasi ini

berupa kode hasil enkripsi pesan aktivasi sekali pakai dan memiliki umur yang singkat.

Kode dibangkitkan dengan mengimplementasikan algoritma kriptografi *Advance Encryption Standard*, *Advanche Encryption Standard* dipilih untuk membangkitkan kode otentikasi karena AES adalah salah satu algoritma kriptografi dengan kunci simetris dimana algoritma dengan kunci simetris prosesnya lebih cepat dibandingkan dengan algoritma kriptografi dengan kunci asimetris, AES juga merupakan salah satu kriptografi *block cipher* yang menjadikannya mudah untuk diimplementasikan dan *Error Propagation* yang terjadi tidak akan merambat ke ciphertext lainnya karena enkripsi masing-masing bloknya independen (Pahlevi, 2012). Dan AES telah melalui serangkaian evaluasi yang dilakukan oleh National Institute of Standards and Technology, dimana AES ini merupakan pemenang dari kompetisi yang diadakan oleh NIST sebagai pengganti Algoritma kriptografi *Data Encryption Standard*, setelah diketahui jika DES memiliki kelemahan dan terkadang sering menghasilkan kunci lemah, walaupun dikembangkan dan ditingkatkan 3 kali menjadi *Triple*-DES tetap saja terkadang membangkitkan kunci lemah. Selain pertimbangan diatas AES juga di pilih karena menurut Naik dan Wei (dalam Ellminaam, Kader, & Hadhoud, 2009) "enkripsi AES itu cepat dan fleksibel, AES dapat diimplementasikan ke berbagai macam jenis *platform* khususnya *devices* berukuran kecil". Dan juga Daemen dan Rijmen mengemukakan (dalam Ellminaam, Kader, & Hadhoud, 2009) "AES telah melalui tes yang dilakukan secara hati-hati pada berbagai macam aplikasi keamanan". Kemudian menurut Wali dan Rehan (2005, hlm. 6) "Dengan menggunakan mesin komputasi yang lambat tentu menjadi sangat sulit untuk membongkar AES. Dimana AES telah diimplementasikan ke dalam berbagai macam bahasa dan *software tools*. Beberapa kode dioptimasikan untuk menciptakan *S-box* dan *inverse mix columns transformation*. Hal tersebut memudahkan transformasi dari AES sehingga dapat diimpelemtasikan kedalam berbagai macam bahasa tingkat tinggi atau tingkat rendah dan *software tools*".

Dengan demikian Kumar dan Karthikeyan (2012, hlm. 27) menyatakan "Dengan demikian dapat dinyatakan jika AES bisa digunakan pada situasi yang membutuhkan tingkat keamanan yang tinggi".

Namun pada tahun 2011 tiga orang peneliti dari beberapa universitas dan Microsoft, Andrey Bogdanov dari K.U. Leuven, Dimitri Khovratovich Peneliti dari Microsoft dan Christian Reachberger dari ENS Paris menemukan adanya celah pada enkripsi AES seperti yang diberitakan oleh The INQUIRER (dalam Neal, 2011) yang memungkinkan untuk memecahkan kunci rahasia lebih cepat dari sebelumnya. Walaupun AES dinyatakan telah melalui berbagai macam tes seperti yang dikemukakan Daemen dan Rijndael sebelumnya dan berita ditemukannya celah untuk mempercepat memecahkan kunci AES. Peneliti akan melakukan modifikasi pada AES yang sudah ada. Dan panjang kunci AES yang dipilih adalah AES dengan panjang kunci 256 *bits,* AES 256 *bits* dipilih karena memiliki ekspansi lebih banyak yaitu 14 putaran dan tentunya memiliki tingkat kompleksitas lebih tinggi dibandingkan dengan AES lainnya. Untuk menambahkan kompleksitas Peneliti akan memodifikasi AES yang mengacu pada prinsip Shannon yaitu *Confusion* dan *Diffusion*. Penelitian sejenis untuk meningkatkan *Confusion* dan *Diffusion* pernah dilakukan oleh Salasiah dkk (2012) untuk memodifikasi ekspansi kunci pada AES, untuk *confusion* dan *diffusion* Salasiah dkk menambahkan fungsi baru berupa *ShiftColumn* dalam membangkitkan ekspansi kunci, dimana dengan menambahkan fungsi baru tersebut hasil pengujian yang dilakukan Salasiah dkk memberikan hasil yang baik. Karena menurut Claude Shannon (1949), algoritma enkripsi yang baik harus memiliki dua sifat operasi yaitu *Confusion* dan *Diffusion.*

Selanjutnya kode otentikasi dibuat untuk melakukan kontrol akses yang ada untuk mencegah akses yang tidak sah. Karena perusahaan harus memastikan bahwa akses yang illegal tidak diperbolehkan dan pengguna yang tidak memiliki hak akses pada bagian tertentu tidak dapat memodifikasi yang tidak perlu. Kontrol tersebut ada dalam berbagai bentuk, mulai dari Identifikasi *badge* dan *password*

untuk mengakses protokol otentikasi dan langkah-langkah keamanan (Parmar, Nainan, & Thaseen, 2012). Agar memberikan imunitas atau kekebalan untuk kode otentikasi yang dibangkitkan AES maka perlu ditambahkan metode untuk itu. Dan metode yang akan digunakan untuk memberikan imunitas pada kode otentikasi yang dibangkikan AES adalah *One-time Password*. Metode ini memungkinkan untuk memberikan umur dan validasi pada setiap kode otentikasinya, yang nantinya setiap kode otentikasi hanya dapat digunakan satu kali dan memiliki batas kadaluarsa. Metode *One-time Password* dipilih karena menurut Kim dkk (2009, hlm. 29) "tujuan dari *One-time Password* adalah untuk meningkatkan kesulitan mengkases *restricted resource* secara illegal." . Selain itu menurut Sediyono dkk (2013, hlm. 1607) "membandingkan kode yang dibangkitkan oleh OTP dengan *Pseudo Random Number Generator* (PNRG) mungkin akan membuat kode yang sama. Pada kondisi ini, itu membuat hacker tidak mudah untuk membongkar kode dan menembus kedalam sistem", selain itu menurut Parmar dkk (2012, hlm. 195) "algoritma ini sangat ekonomis untuk diimplementasikan agar tersedia ketika disingkronkan dengan pengguna"

Analisis statistik seperti *Avalanch Effect, Hamming Weight,* dan *Randomness Test* akan dilakukan pada modifikasi AES 256 bit dan hHasil dari penelitian ini akan diimplementasikan pada registrasi Saungkode.com yang sedang dikembangkan oleh teman-teman dari Toprak DG sebagai contoh untuk jejarning sosial bertipe Question & Answer.

1.2 Rumusan Masalah

Berdasarkan Latar Belakang masalah diatas, maka dapat diidentifikasikan masalah sebagai berikut :

1. Bagaimana pembuatan kode otentikasi berbasis heksadesimal dengan algoritma kriptografi *Advance Encryption Standard* dan *One-time Password*?

2. Bagaimana proses aktivasi dengan kode otentikasi yang mengimplementasikan algoritma kriptografi *Advance Encryption Standard* yang telah dimodifikasi dan *One-time Password*?
3. Bagaimana pengujian kompleksitas *Advance Encryption Standard* yang telah dimodifikasi?

1.3 Batasan Masalah

Untuk memfokuskan penelitian, ditetapkan beberapa batasan masalah, yaitu sebagai berikut:

1. Penelitian dilakukan pada kode otentikasi dengan mengimplementasikan algoritma kriptografi *Advance Encryption Standard* dan *One-time Password* dalam mengenkripsi pesan aktivasi *member* baru.
2. Kode otentikasi berbasis heksadesimal.
3. Proses dipakai pada saat pendaftaran *member* baru.
4. Diimplementasikan pada jejaring media sosial baru atau pada situs jual beli *online* baru.
5. Modifikasi *Advance Encryption Standard* hanya dilakukan pada AES-256, pada bagian *S-Box* dan *ShiftRow.*
6. Pengiriman SMS kode otentikasi pada pendaftar baru menggunakan SMS API dari zenziva.net
7. Pengujian *randomness* algoritma AES-256 dilakukan dengan bantuan software Cryptool 1.4.3

1.4 Tujuan Penelitian

Sesuai dengan permasalahan yang telah dirumuskan, maka tujuan yang ingin dicapai pada penelitian ini adalah :

1. Menghasilkan kode otentikasi berbasis heksadesimal dengan algoritma kriptografi *Advance Encryption Standard* dan *One-time Password.*

2. Menghasilkan protokol baru untuk aktivasi akun dengan kode otentikasi yang dibangkitkan dengan algoritma *Advance Encryption Standard* dan *One-time Password.*

3. Mendapatkan hasil pengujian kompleksitas dengan menggunakan *Avalanche Effect* dan *Randomness Test.*

1.5 Sistematika Penulisan

Sistematika penulisan skripsi ini adalah sebagai berikut.

BAB I PENDAHULUAN

Bab ini berisi latar belakang, rumusan masalah, batasan masalah, tujuan penelitian yang akan dilakukan, dan sistematikan penulisan.

BAB II TINJAUAN PUSTAKA

Bab ini berisi penjelasan tentang teori-teori dan konsep algoritma yang digunakan dalam penelitian.

BAB III METODOLOGI PENELITIAN

Bab ini berisi penjelasan langkah-langkah yang akan dilakukan dalam penelitian.

BAB IV HASIL PENELITIAN DAN PEMBAHASAN

Bab ini berisi uraian tentang hasil penelitian dan pembahasan terhadap hasil penelitian yang dilakukan

BAB V KESIMPULAN DAN SARAN

Bab ini berisi kesimpulan dari keseluruhan penelitian yang telah dilakukan, serta saran dari penulis untuk kegiatan penelitian selanjutnya terkait dengan topik yang sedang dibahas.