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

Dengan ditemukannya teknologi internet, para pengguna komputer semakin dimudahkan untuk berkomunikasi antara satu komputer dengan komputer lainnya. Dengan internet, komunikasi yang tadinya jauh bisa menjadi lebih dekat, yang tadinya membutuhkan waktu yang lama jadi semakin lebih cepat, yang tadinya membutuhkan biaya yang mahal menjadi semakin murah. Komunikasi dengan internet bisa dilakukan oleh siapa saja, kapan saja dan di mana saja tanpa dibatasi oleh ruang, waktu, dan biaya. Seiring dengan berevolusinya teknologi internet, maka perubahan komunikasi semakin beragam, yang tadinya komunikasi hanya sekedar melalui suara dan pesan saja, sekarang bertambah dengan adanya teknologi *video call*, pesan suara, gambar dan teknologi lainnya.

Selain itu, penggunaan internet pun menjadi semakin berkembang dikarenakan adanya pembuatan berbagai macam-macam aplikasi seperti media social dan e-commerce. Menurut survey yang dilakukan oleh We are Social pada tahun 2017 (Kemp, 2017), ada 3811 miliar atau sekitar 51% pengguna internet diseluruh dunia dengan 2907 miliar atau sekitar 39% menggunakan media sosial. Adapun media sosial yang populer sampai dengan awal tahun 2017 adalah Facebook dengan total pengguna 1968 juta pengguna, Whatsapp dengan total pengguna 1200 juta pengguna, Facebook Messenger dengan total pengguna 1000 juta pengguna, Instagram dengan total pengguna 600 juta pengguna.

Pada tahun 2018, *statista.com* (“E-commerce worldwide - Statistics & Facts | Statista,” 2019) mencatat bahwa ada 1,8 miliar orang melakukan transaksi *e-commerce* diseluruh dunia. Pada tahun yang sama pula, pendapatan dari produk retail pada *e-commerce* mencapai 2.8 milyar dollar Amerika dan juga pada tahun 2021 pendapatan dari penjualan produk retail diprediksi mencapai 4.8 milyar

dollar Amerika. Pada quartal ke-4 tahun 2018, penggunaan PC masih mendominasi transaksi *online* akan tetapi transaksi yang menggunakan *smartphone* berada pada posisi pertama untuk kunjugan website ritel. Survey yang dilakukan selama tahun 2017 mencatat bahwa ada sekitar 11% dari penjualan yang dilakukan menggunakan *smartphone* setiap minggunya.

Dari data-data yang didapatkan dapat menunjukkan bahwa penggunaan internet saat ini sangat pesat pertumbuhnannya dan akan bertambah seiring berjalannya waktu. Penggunaan internet saat ini didominasi oleh aplikasi-aplikasi yang berabasiskan website dan Aplikasi *Mobile*. Untuk menggunakan aplikasi sepert sosial media dan *e-commerce* diperlukannya sebuah akun yang sesuai data pribadi dan telah didaftarkan sebelumnya. Tujuan dari pendaftaran akun tersebut untuk memudahkan pengiriman barang yang telah dibeli secara *online* dan memudahkan kita untuk terhubung dengan teman kita.

Untuk melindungi data pribadi kita dari penggunaan secara ilegal, maka diperlukan sebuah metode untuk melindungi data-data tersebut. Otentikasi adalah sebuah teknik untuk mengidentifikasi dan memverifikasi bahwa pengguna yang bersangkutan telah masuk kedalam sebuah aplikasi sesuai dengan legalitas data yang berlaku.

Metode yang paling umum digunakan untuk otentikasi adalah dengan memasukkan nama pengguna atau *email* serta dibarengi dengan kode password. Hal tersebut sangat rentan terhadap serangan seperti *Shoulder Surfing*, *guesing attack*, *dictionary attack*, serta serangan *Trojan*. Beberapa penelitian mengungkapkan bahwa banyak pengguna biasa yang menggunakan kode password yang pendek serta mempunyai keterkaitan dengan nama ataupun tanggal lahir. Sayangnya, kode password seperti ini sangat mudah dipecahkan dengan metode *Social Engineering*. Kode password yang panjang dapat membuat sistem menjadi lebih aman, akan tetapi akan sulit untuk diingat.

Selain dari serangan diatas, ada banyak serangan terhadap otentikasi seperti program mencurigakan yang merekam segala aktivitas yang dilakukan pada *keyboard* pada saat memasukan password untuk otentikasi kemudian informasi tersebut dapat dikirimkan kepada si penyerang (*Key Logging* dan *Pishing*). Untuk menghindari serangan tersebut, dibuatlah sebuah konsep *keyborad virtual* yang

dapat mencegah memasukkan inputan melalui *keyboard* digantikan dengan penggunaan *mouse*.

Keamanan dari data-data pribadi menjadi hal yang sangat diperlukan. Terlebih lagi pada era globalilasi sekarang ini, dimana setiap orang bisa melakukan transaksi jual-beli dimanapun, kapanpun dan oleh siapapun asalkan orang tersebut terhubung dengan jaringan internet atau biasa disebut dengan e-commerce (Chaffey, 2009). Salah satu bentuk e-commerce adalah pasar daring atau biasa disebut dengan online marketplace. Banyak sekali pelaku bisnis yang memanfaatkan metode online marketplace ini, salah satu contohnya adalah BukaLapak, Tokopedia, Shopee dan sebagainya. Sayangnya, data-data pribadi yang berada pada online marketplace, rentan untuk dicuri dan disalah gunakan oleh pihak yang tidap bertanggung jawab.

Seperti yang telah diberitakan oleh situs berita daring yakni detik.com, bahwa sepanjang tahun 2016 setidaknya ada beberapa kasus pencurian dan penyalahgunaaan akun pengguna di beberapa *online marketplace* oleh pihak yang tidak berwenang untuk melakukan transaksi pembelian pulsa dengan nominal yang relatif besar dan pembelian barang-barang lainnya (Rahman, 2016a, 2016b, 2016c). Kasus pencurian akun tersebut terjadi karena kelalaian pengguna dalam melakukan *login* dengan memasukan *email* dan kata sandi disembarang gawai tanpa melakukan *logout* setelahnya. Selain itu, penyebab lain dari pencurian akun milik pengguna disebabkan karena pengguna terkena serangan *phishing*, yakni sebuah teknik yang dilakukan oleh pihak yang tidak berwenang dengan membuat tiruan *website online marketplace* dengan tujuan untuk mendapatkan *email* dan kata sandi milik pengguna *online marketplace*. Lalu, *website* tiruan tersebut dikirimkan kepada pengguna dengan dalih untuk melakukan pemeliharaan sistem. Penyebab lainnya adalah, penggunan memberikan kode otentikasi kepada pihak yang tidak berwenang dengan alasan proses traksaksi baru dari sebuah *online marketplace*.

Untuk mencegah pencurian tersebut, hendaknya pihak *online marketplace* perlu untuk membangun sebuah mekanisme keamanan yang dapat melindungi data konsumen maupun data penjual. Salah satu mekanisme atau metode untuk melindungi data pribadi, adalah dengan menggunakan metode *One Time*

Password. Metode *One Time Password* ini dapat diterapkan pada saat konsumen atau penjual melakukan *Login* untuk memvalidasi ulang data-data pribadi miliknya. Penggunaan metode ini bertujuan untuk menghindari serangan atau pencurian yang dilakukan oleh pihak yang tidak bertanggung jawab pada saat *login* aplikasi.

Dengan bertambahnya aplikasi yang menggunakan teknik otentikasi dan berkembangnya serangan terhadap serangan otentikasi menyebabkan berkembangnya teknologi OTP. Ide dari penggunaan OTP sebagai teknik otentikasi pertama kali dikenalkan oleh Leslie Lamport (Lamport, 1981).

Secara umum, One Time Password adalah sistem otentikasi dimana kode tersebut hanya bisa digunakan satu kali dan pengguna harus menggunakan kode baru setiap kali melakukan otentikasi. Metode ini memberikan garansi keamanan meskipun penyerang mendapatkan kode pada jaringan internet atau dicuri dari pengguna. Selain itu, OTP memiliki beberapa fitur seperti kerahasiaan, mudah dibawa, dan memiliki cakupan yang sangat luas (Cho, Lee, Lee, & Lim, 2009).

Pengiriman kode otentikasi OTP, biasanya menggunakan layanan SMS dan *email*. Pengiriman kode otentikasi tersebut dilakukan dengan beberapa metode seperti *Self-updating OTP-based authentication* dan *time synchronized* OTP (Vinh, Bouzefrane, Farinone, Attar, & Kennedy, 2015).

Salah satu cara yang umum untuk mengirimkan kode OTP kepada pengguna adalah melalui layanan *Short Message Service* atau yang sering dikenal dengan SMS. Pengguna diharuskan untuk mengisi *username* dan *password* pada saat proses *login.* Kemudian, *username* dan *password* tersebut akan dikirmkan ke *server* dan server akang membangkitkan sebuah kode OTP. *Server* menghasilkan kode OTP menggunakan teknik tertentu. Setelah proses pembangkitan selasai, kode OTP dikirimkan kepada pengguna melalui layanan SMS. Pengguna diharuskan mengisi kode OTP yang tertera pada SMS ke aplikasi untuk nantinya dikirimkan kembali ke *server*. Otentikasi terjadi pada saat server mengenali bahwa pengguna memasukkan kode yang benar saat login. Setelah kode OTP diterima oleh *server*, kode tersebut dicocokan dengan kode OTP yang sebelumnya telah tersimpan dalam *database.* Dengan menggunakan layanan SMS ini dapat mengurangi biaya dari penggunaan perangkat keras tambahan. Selain itu, pada

penelitian yang dilakukan (Wu, Garfinkel, & Miller, 2004) menunjukkan bahwa layanan SMS ini memiliki keamanan yang lebih baik dibandingkan dengan jalur internet umumnya.

Untuk membangkitkan kode OTP, diperlukan sebuah metode matematis yang dapat membuat kode OTP tersebut. Metode matematis tersebut biasanya menggunakan algoritma khusus seperti halnya teknik kriptografi. Tujuan dari penggunaan teknik kriptografi dalam membangkitkan kode OTP adalah untuk menjamin keamanan pada saat verifikasi dengan menggunakan kode OTP. Pada penelitian (Sediyono, Santoso, & Suhartono, 2013) dikembangkan sebuah teknik pembangkitan kode OTP untuk sistem informasi akademik dengan memanfaatkan fungsi hash MD5. Penelitian tersebut menyimpulkan bahwa penggunaan fungsi hash MD5 untuk keperluan pembangkitan kode OTP memenuhi ke empat unsur kriptografi. Selain itu, proses pembangkitan kode OTP dengan menggunakan fungsi hash MD5 cukup cepat, yakni sekitar 0,744 detik.

Pada penelitian (Nugroho, Putra, & Ramadhan, 2016) yang memanfaatkan modifikasi algoritma *Advanced Encryption Standard* (AES) dan fungsi hash MD5 dapat disimpulkan bahwa penggunaan algoritma kriptografi dalam membangkitkan kode OTP sangat aman. Hal itu dibuktikan dengan hasil pengujian *Avalanche Effect* dengan nilai 50.39% dan hasil keseluruhan *Statistical Randomness Tess* yang menyatakan algoritma AES lolos uji keacakan. Selain itu, waktu yang diperlukan untuk melakukan proses enkripsi dari pembangkitan kode OTP cukup cepat, yakni sekitar 0.511 detik.

Kemudian, pada penelitian (Nursalman, Putra, & Lestari, 2017) yang menggabungkan antara modifikasi *Data Encryption Standar* (DES), *Linear Congruential Generator* (LCG) dan fungsi hash SHA1 yang menyatakan bahwa penggabungan agoritma kriptografi dengan pembangkit bilangan acak dan fungsi hash menghasilkan uji *Avalanche Effect* yakni 51.78% dan hasil keseluruhan dari *Statistical Randomness Tess* yang menyatakan bahwa kode OTP yang telah dibangkitkan lolos uji keacakan.

Dari ketiga penelitian tersebut dapat disimpulkan bahwa, penambahan teknik kriptografi, menimbulkan pengaruh yang signifikan untuk ketahanan dan keamanan dari serangan yang dilakukan oleh pihak yang tidak bertanggung

jawab. Akan tetapi, tidak semua algoritma kriptografi bisa ditambahkan untuk meningkatkan keamanan dan ketahan. Salah satu faktor yang dapat mendukung ketahanan dan keamanan proses otentikasi adalah kecepatan dari sebuah algoritma kriptografi. Algoritma kriptografi yang memiliki kecepatan yang cukup baik salah satunya adalah algoritma RC6. Pada penelitian (Verma & Singh, 2012), dilakukan penelitian terhadap *execution time* dari algoritma RC6, Twofish dan Rijndael. Hasil dari penelitian tersebut dapat dilihat pada tabel dan gambar berikut ini.

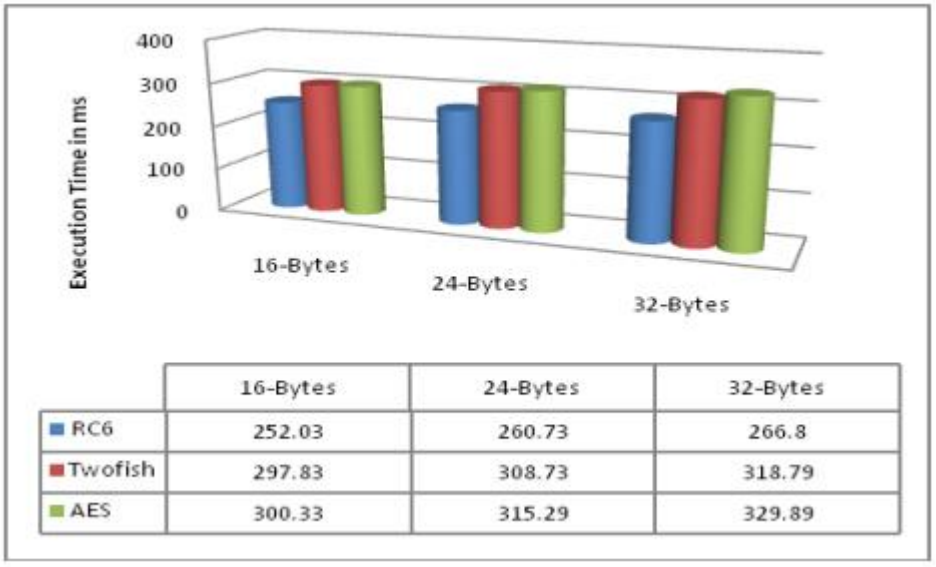
Dari gambar 1.1., didapatkan hasil bahwa *execution time* rata-rata dari algoritma RC6 dengan panjang kunci 16 bytes yaitu 252.03 *millisecond*, untuk panjang kunci 24 bytes yaitu 260.73 *millisecond*, dan untuk panjang kunci 32 bytes yaitu sebesar 266.8 *millisecond*. Dari data-data tersebut dapat disimpulkan bahwa algoritma RC6 memiliki rata-rata *execution time* yang lebih baik dibandingkan dengan algoritma Twofish dan Rijndael. Kemudian pada penelitian (Survey & Princy, 2015), algoritma RC6 memiliki keamanan yang cukup baik. Pada tahun 2015, Jindal dalam (Jindal & Singh, 2015) melakukan pengujian *Avalanche effect* terhadap finalis *Advanced Encryption Standard* dan didapatkan hasil bahwa algoritma RC6 memiliki nilai sebesar 49%. Selain itu pada penelitian *Randomness Test* yang dilakukan oleh Sulak dalam (Sulak, Douganaksoy, Ege, & Koçak, 2010) menunjukan bahwa keacakan chipertext dari algoritma RC6 muncul pada putaran ke 4. Hasil dari penelitian tersebut dapat dilihat dalam tabel 1.1.

Tabel 1.1. Hasil Randomness Test pada penelitian Sulak (Sulak et al., 2010)

Rnds	Freq.	B.Freq.	Run	L.Run	Ap.En.	C.Sum1	C.Sum2	Serial
3	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
4	0.2504	0.2245	0.0371	0.1145	0.1413	0.0755	0.9803	0.1453
5	0.6958	0.7972	0.9787	0.1823	0.6092	0.9830	0.5004	0.3810

Hasil dari penelitian-penelitian tersebut menunjukkan bahwa, algoritma RC6 bisa digunakan untuk menambah nilai ketahanan dan keamanan pada proses otentikasi dan akan digunakan dalam penelitian ini. Karena hasil ciphertext dari algoritma RC6 berupa karakter ASCII, maka pemanfaatan ciphertext sebagai kode OTP tidak dapat dilakukan karena pengguna tidak dapat membaca karakter tertentu dan akan menimbulkan kesalahan pada saat pengguna memasukan

karakter tersebut dalam proses aktivasi nantinya. Untuk mengatasi hal tersebut, pada penelitian ini digunakan metode HOTP.



	16-Bytes	24-Bytes	32-Bytes
RC6	252.03	260.73	266.8
Twofish	297.83	308.73	318.79
AES	300.33	315.29	329.89

Gambar 1.1. Perbandingan Execution Time antara algoritma RC6, Twofish dan Rijndael (Verma & Singh, 2012)

Dari hasil proses pembangkitan kode aktivasi dengan menggunakan HOTP, akan terbentuk 6 digit angka rahasia yang tidak boleh diberikan kepada siapapun.

Untuk mengetahui kerahasiaan dan integritas data dari pemanfaatan Algoritma RC6 dan metode HOTP maka akan dilakukan 2 buah pengujian yakni pengujian *Avalanche Effect* dan *Statistical Randomness Test*. Selain itu, untuk mengetahui tingkat kesesuaian terhadap fungsionalitas dari kebutuhan perangkat lunak, maka akan dilakukan *Black Box Testing*. Sedangkan, untuk mengetahui keamanan terhadap faktor otentikasi dan nir-penyangkalan, maka akan dilakukan pengujian dengan melakukan serangan *Man In The Middle* dan *Password Guessing Attack* terhadap perangkat lunak yang sudah dibuat.

1.2 Rumusan Masalah Penelitian

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

1. Bagaimana proses implementasi Algoritma RC6 dan metode *One Time Password* pada proses pembuatan kode otentikasi untuk *website online marketplace*?
2. Bagaimana hasil dari pemanfaatan Algoritma RC6 dan metode *One Time Password* pada proses otentikasi dapat mencegah pencurian akun pengguna *website online marketplace*?
3. Bagaimana keamanan dari sistem yang telah dibuat dengan memanfaatkan Algoritma RC6 dan metode *One Time Password* pada proses pembuatan kode otentikasi untuk *website online marketplace*?

1.3 Tujuan Penelitian

Tujuan dari penelitian ini adalah:

1. Mengimplementasi Algoritma RC6 dan metode *One Time Password* pada proses pembuatan kode otentikasi untuk *website online marketplace*.
2. Menganalisis hasil dari pemanfaatan Algoritma RC6 dan metode *One Time Password* pada proses otentikasi untuk *website online marketplace* dengan melakukan pengujian *Avalanche Effect* dan *Statistical Randomness Test.*
3. Menganalisis keamanan dari sistem yang telah dibuat dengan memanfaatkan Algoritma RC6 dan metode *One Time Password* pada proses pembuatan kode otentikasi untuk *website online marketplace* dengan melakukan pengujian serangan *Man In The Middle Attack* dan *Password Guessing Attack*?

1.4 Batasan Masalah

Batasan masalah pada penelitian ini adalah:

1. Penelitian dilakukan pada proses pengimplementasian RC6 pada proses otentikasi.
2. Pembangkitan kode otentikasi pada saat proses *login*.
3. Kode OTP yang dibuat hanya 6 digit angka.
4. RC6 yang dipakai hanya 128 bit.
5. HMAC yang digunakan adalah HMAC-SHA1.
6. Proses aktivasi dibatasi sampai 3 kali.
7. Waktu tunggu proses aktivasi dibatasi sampai 3 menit.

8. OTP yang dibangkitkan bertipe *Time-Event-Synchronized*.
9. Pengirima kode OTP dengan SMS menggunakan layanan dari pihak ketiga.

1.5 Sistematika Penulisan

Sistematika penulisan proposal skripsi adalah sebagai berikut

BAB I PENDAHULUAN

Bab ini berisi latar belakang penelitian yang mencakup masalah yang akan diselesaikan, penjelasan singkat tentang *One Time* Passwotd serta penelitian sebelumnya dari algoritma RC6 yang akan menjadi landasan dalam penelitian ini. Selanjutnya, bab ini berisi rumusan masalah penelitian, tujuan penelitian, batasan masalah dan sistematika penulisan.

BAB II KAJIAN PUSTAKA

Bab ini berisi teori dan konsep terkait dalam penelitian yang menunjang pada penelitian ini.

BAB III METODOLOGI

Bab ini berisi langkah-langkah penelitian yang diilustrasikan dengan skema desain penelitian, metode penelitian yang terdiri dari studi literatur dan proses pengembangan perangkat lunak, dan alat maupun bahan penelitian yang digunakan.

BAB IV HASIL DAN PEMBAHASAN PENELITIAN

Bab ini berisi hasil dan pembahasan yang telah didapatkan dan dilakukan selama penelitian.

BAB V KESIMPULAN DAN SARAN

Bab ini berisi kesimpulan dari seluruh penelitian yang telah dilakukan serta memberikan saran untuk penelitian selanjutnya.