BAB I
PENDAHULUAN

1.1 Latar Belakang

Pengiriman atau pertukaran data adalah hal yang sering terjadi dalam dunia teknologi informasi. Data yang sering dikirim kadang berisi data informasi yang sangat penting dan sangat rahasia sehingga harus terjaga keamanannya. Apalagi pengiriman data dilakukan melalui dunia maya, ancaman kejahatan sangat banyak di dalamnya. Dengan adanya kejahatan seperti pencurian data, akibatnya data tersebut bisa jatuh pada orang yang tidak berhak bahkan data tersebut disalahgunakan oleh pihak tidak berwenang. Salah satu dari sisi buruk tersebut adalah rawannya keamanan data sehingga menimbulkan tantangan dan tuntutan akan tersedianya suatu sistem kemanan data yang sama canggihnya dengan kemajuan teknologi komputer tersebut. Hal inilah yang menjadi latar belakang berkembangnya sistem keamanan untuk melindungi data yang ditransmisikan melalui suatu jaringan komunikasi (Ariyus, 2006).

Pada era serba digital banyak orang yang melakukan pengiriman data melalui teknologi informasi, ditambah dengan adanya hacker dan cracker, data yang dikirim dan disimpan harus mempunyai keamanan yang kuat agar data yang dikirim bisa sampai kepada penerima atau disimpan dengan aman. Untuk menjaga keamanan data dilakukan dengan Teknik kriptografi.

Keamanan yang terjamin dari suatu sistem sangat diperlukan dalam kegiatan bisnis, sistem yang aman mampu memberikan tingkat kepercayaan yang tinggi bagi pengguna sistem tersebut, sehingga dapat memberi nilai tambah dan daya guna bagi sistem tersebut. Pengguna akan merasa nyaman dan aman ketika menggunakan sistem yang mampu mengamankan data pengguna dari penyerang (Ariyus, 2006).

Ada beberapa teknik pengamanan data yang melalui saluran, salah satu diantaranya adalah kriptografi. Dalam kriptografi, data yang sangat rahasia disandikan sedemikian rupa sehingga jika data tersebut dicuri oleh pihak yang tidak berhak, mereka tidak dapat mengetahui data yang sebenarnya, karena data

Yuda Wijaya Prawira, 2018
IMPLEMENTASI ALGORITMA SYMETRIC KEY ADVANCED ENCRYPTION STANDARD (AES) DAN BLOWFISH MENGGUNAKAN OTENTIKASI GENERATE ONE TIME PASSWORD (OTP) PADA KEAMANAN DATA FILE
Universitas Pendidikan Indonesia | repository.upi.edu | perpustakaan.upi.edu

yang mereka curi merupakan data yang sudah disandikan, dan data yang telah disandikan tersebut sebagai ciphertext (Munir, 2006).

Yuda Wijaya Prawira, 2018
IMPLEMENTASI ALGORITMA SYMETRIC KEY ADVANCED ENCRYPTION STANDARD (AES) DAN BLOWFISH MENGGUNAKAN OTENTIKASI GENERATE ONE TIME PASSWORD (OTP) PADA KEAMANAN DATA FILE
Universitas Pendidikan Indonesia | repository.upi.edu | perpustakaan.upi.edu

Dalam hal keamanan data, ada 4 aspek layanan keamanan yaitu kerahasiaan, keutuhan, otentikasi dan penyangkalan (Munir, 2006). Banyak algoritma kriptografi yang digunakan untuk melakukan pengamanan data, tetapi kekuatan dari keamanan pesan tersebut masih terhitung lemah. AES adalah algoritma yang terbaik dari teknologi enkripsi simetri. Algoritma AES termasuk *Cipher Block* dimana rangkaian bit-bit plainteks menjadi blok-blok bit dengan panjang kunci yang sama (Saikh & Kaul, 2014). Blok plainteks yang sama akan dienkripsi menjadi cipherteks yang sama apabila menggunakan kunci yang sama. Begitu pula dengan algoritma *Blowfish* yang dibuat oleh Scheiner merupakan salah satu algoritma terbaik dan termasuk *Cipher Block* yang menggantikan algoritma DES. Sesuai dengan pernyataan Scheiner *Blowfish* telah mendapatkan tempat di dunia kriptografi, khususnya bagi masyarakat yang membutuhkan algoritma yang cepat, kuat dan tidak terhalang oleh lisensi.

AES adalah proses mengenkripsi dan mendekripsi blok data sepanjang 128 bit dengan panjang kunci 128 bit, 192 bit, dan 256 bit. Proses enkripsi pada algoritma ini terdiridari 4 jenis transformasi bytes, yaitu SubBytes, ShiftRows, MixColumns, dan AddRoundKey (Katkade & Phade, 2016). Sedangkan pada algoritma *Blowfish* memiliki panjang kunci dari 32 bit sampai 448 bit dan ukuran blok 64 bit (Bruce, 1996).

One Time Password (OTP) Kata kunci yang dihasilkan tidak dapat digunakan kembali (tidak dapat digunakan kembali), jadi tidak ada gunanya jika seseorang menemukan kata sandinya, karena kata sandinya akan kedaluwarsa. Setiap password hanya digunakan satu kali (Menezes, Van Oorschot, & Vanstone, 1996). OTP menyediakan kekebalan dan keamanan dari kemungkinan serangan sniffing password, bahkan jika seseorang mengintip kata sandi Anda, mereka tetap tidak dapat mengakses akun Anda.

Salah satu contoh kasus pada bidang kriptografi adalah pencurian data oleh hacker pada server di gawker media, gawker media adalah salah satu perusahaan media yang membawahi beberapa situs di amerika serikat (CSO ONLINE, 2010), pada kasus ini perusahaan tersebut telah kehilangan 500 MB *file* yang berisikan data pribadi anggotanya berupa cv untuk melamar pekerjaan. Perusahaan gawker

merekomendasikan agar siapa pun yang memiliki akun yang terdaftar harus mengganti kata sandi mereka. Apabila seseorang menggunakan kata sandi yang sama dengan situs lain, maka kata sandi tersebut harus diganti juga. Tidak disebutkan sebelumnya apakah perusahaan tersebut memakai kriptografi atau tidak.

Pada penelitian sebelumnya dalam jurnal *Performance Analysis of Encryption Algorithms for Security* membahas tentang perbandingan algoritma AES, DES, Blowfish dan RSA. Dalam makalah tersebut melakukan uji coba enkripsi dan dekripsi data berupa teks *file* enkripsi dan dekripsi, pada proses dekripsi algoritma AES menduduki peringkat pertama yang tercepat dalam enkripsi teks *file* tersebut (Panda, 2016). Sedangkan untuk proses dekripsi teks *file* algoritma RSA mendapatkan hasil tercepat. Pada jurnal lain yang berjudul *Performance Analysis of Encryption Algorithms for Information Security* melakukan penelitian untuk mempertimbangkan metrik kinerja dari algoritma AES, DES dan Blowfish dalam hal waktu eksekusi, memori yang dibutuhkan dan *throughtput*. Hasilnya Algoritma Blowfish memiliki waktu lebih cepat dalam waktu eksekusi dibandingkan dengan algoritma AES dan DES. Pada uji coba memori yang dibutuhkan algoritma Blowfish mengkonsumsi memori lebih sedikit dibandingkan dengan algoritma lain yaitu 25,2 Kb. Untuk uji coba *throughtput* algoritma Blowfish berkinerja 4 kali lebih cepat dari kinerja AES dan 2 kali lebih cepat dibandingkan kinerja DES (A.Ramesh & A.Suruliandi, 2013). Algoritma AES dapat menjaga kerahasiaan data yang ditransmisikan dengan memprosesnya ke bentuk terenkripsi (Firdaus, Wahyudin, & Nugroho, 2017). Pada Jurnal "penerapan algoritma DES dan RC6 pada aplikasi enkripsi berbasis android" menjelaskan tentang kecepatan waktu enkripsi dan dekripsi teks sms berbasis android. hasilnya bahwa semakin panjang *plainteks, ciphertext,* dan *key* maka semakin lama proses enkripsi dan dekripsinya, serta ukuran RAM dari hardware mempengaruhi kecepatan proses enkripsi dan dekripsi (Anwar & Hastuti, n.d.). Pada Skripsi "aplikasi kemanan data *multimedia message service* (MMS) pada *Microsoft Office file* memanfaatkan algoritma *Rivest-Shamir Adleman* (RSA) dan Blowfish berbasis android" menjelaskan kecepatan hasil enkipsi dari kombinasi

algoritma RSA dan Blowfish terhadap *file* berekstensi *Microsoft Office*. Hasil dari penelitian tersebut bahwa algoritma blowfish menunjukan estimasi waktu yang tidak beraturan, hal ini menunjukan bahwa besarnya ukuran *file* yang akan dienkripsi berpengaruh terhadap estimasi waktu yang dicapai (Subroto, 2017).

Masalah dari perusahaan gawker media dapat diatasi dengan kombinasi algoritma AES dan *Blowfish* yang merupakan algoritma simetri, dari hasil penelitian sebelumnya bahwa algoritma AES mengkonsumsi panjang kunci sampai dengan 256 bit, sedangkan algoritma Blowfish mengkonsumsi kunci sampai 448 bit. Kelemahan dari kunci simetri adalah proses enkripsi dan dekripsi menggunakan kunci yang sama. Apabila kunci enkripsi diketahui oleh orang lain, maka orang tersebut dapat mendekripsikannya sehingga data menjadi tidak rahasia lagi. Kekuatan kriptografi sangat ditentukan oleh kunci yang digunakan dan kedua algoritma ini menggunakan operasi XOR dalam melakukan enkripsi, sehingga penyerang mudah untuk menyandikan kembali ciphertext menjadi plaintext, hanya dengan melakukan kembali operasi XOR. Misalnya diasumsikan A berhasil menyadap dua buah ciphertext yang berbeda menggunakan kunci yang sama, kemudian A melakukan operasi XOR terhadap kedua ciphertext yang berhasil disadapnya. Jika A berhasil mengetahui plaintext dari salah satu ciphertext tersebut, maka A akan mudah menemukan plaintext yang lain tanpa mengetahui rangkaian kuncinya (Munir, 2006).

Peningkatan keamanan pesan dari kunci dilakukan dengan mengkombinasikan beberapa algoritma baik algoritma simetri maupun asimetri akan menambah keamanan sehingga menjadi lebih aman dan powerful (Jain & Agrawal, 2014). Pada proses pengambilan *file* pengguna akan melakukan otentikasi menggunakan OTP yang akan dikirimkan melalui email, OTP hanya bisa dilakukan satu kali setiap akan mengambil *file*. Kode otentikasi ini dihasilkan menggunakan One-time Password. Kemudian, akan dienkripsi menggunakan algoritma kriptografi *Advanced Encryption Standard*, kode otentikasi yang dihasilkan hanya dapat digunakan sekali dalam waktu yang terbatas (Nugroho, Judhie Putra, & Ramadhan, 2016).

Untuk memenuhi aspek-aspek layanan keamanan serta meningkatkan keamanan data maka pada penelitian ini akan dilakukan metode *simetric-key* yaitu dengan mengkombinasikan algoritma AES dan *Blowfish* dimana algoritma *Blowfish* sebagai enkripsi dan dekripsi data, sedangkan pada saat pengambilan *file* yang original akan dilakukan otentikasi terhadap pengguna dengan metode generate OTP menggunakan algoritma sha1 yang di enkripsi oleh algoritma AES yang ekspansi kuncinya menggunakan *hashing* SHA-256 agar mengetahui bahwa yang akan mengambil *file* adalah orang yang berwenang. Analisis statistik *Randomness Test* akan dilakukan pada hasil enkripsi data menggunakan algoritma blowfish dan tes kerahasaiaan terhadap data yang dihasilkan oleh algoritma blowfish.

1.2 Rumusan Masalah

Rumusan masalah dalam penelitian ini adalah:

1. Bagaimana pengimplementasian algoritma AES dan Blowfish dengan menggunakan verifikasi OTP dalam keamanan data?
2. Bagaimana proses pengambilan data dengan otentikasi yang mengimplementasikan algoritma *Advanced Encryption Standard* dan *One-time Password*?
3. Bagaimana hasil penerapan algoritma AES-256 yang dikombinasikan SHA-256 sebagai otentikasi pengambilan data?
4. Bagaimana hasil pengujian algoritma Blowfish terhadap kerahasiaan data dan pengujian keacakan terhadap *ciphertext* hasil enkripsi?

1.3 Tujuan Penelitian

Adapapun tujuan dari penelitian ini adalah:

1. Untuk mengetahui pengimplementasian algoritma AES dan Blowfish dengan menggunakan verifikasi OTP dalam keamanan data.
2. Untuk mengetahui proses pengambilan data dengan otentikasi yang mengimplementasikan algoritma *Advanced Encryption Standard* dan *One-time Password*.
3. Untuk mengetahui hasil penerapan algoritma AES-256 yang dikombinasikan SHA-256 sebagai otentikasi pengambilan data.

4. Untuk mendapatkan hasil pengujian algoritma blowfish terhadap kerahasiaan data dan pengujian keacakan terhadap *ciphertext* hasil enkripsi.

1.4 Manfaat Penelitian

Manfaat dari penelitian ini adalah memberikan model kombinasi antara AES dan *Blowfish* untuk enkripsi dan dekripsi yang akan di verifikasi oleh OTP sehingga data yang dikirimkan atau disimpan menjadi lebih aman.

1.5 Batasan Masalah

Adapun Batasan masalah dalam penelitian ini adalah:

1. Algoritma AES yang digunakan adalah AES-256.
2. Poses enkripsi dan dekripsi data menggunakan algoritma *Blowfish*.
3. Pengenkripsian string terhadap nama file yang dilakukan pada penelitian ini berekstensi .docx dan .pdf.
4. Pengujian *randomness test* terhadap kerahasiaan data algoritma blowfish dilakukan dengan bantuan software Cryptool 1.4.3
5. Proses kombinasi *Advanced Encryption Standard* dan *One-Time-Password* dipakai pada saat pengambilan data.

Pengiriman otentikasi pada user menggunakan E-mail.