# BAB I
# PENDAHULUAN

## I.1 Latar Belakang

Pada era digitalisasi saat ini penggunaan berkas tidak hanya berbentuk cetak, namun dapat berbentuk *file* digital yang dapat mengurangi penggunaan kertas, serta memudahkan data untuk diproduksi, diakses, dimodifikasi, dan disimpan. *File* digital dapat disimpan ke dalam perangkat penyimpanan *offline*, seperti komputer, *flashdrive*, ataupun aplikasi penyimpanan *file* digital secara *online*, seperti *Google Drive*, *Dropbox*, dan sebagainya sehingga mempermudah pengguna dalam mengakses *file* saat dibutuhkan kapanpun. Namun, menyimpan *file* digital yang belum diberi proteksi dapat mengancam keamanan terhadap kerahasiaan *file*, jika terjadi pencurian terhadap perangkat penyimpanan *file* digital *offline* atau akses terhadap akun yang digunakan untuk masuk ke dalam aplikasi penyimpanan *file* digital *online*. Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 20 Tahun 2016 Tentang Perlindungan Data Pribadi dalam Sistem Elektronik Bab II Perlindungan Bagian Keempat Penyimpanan Data Pribadi Pasal 15 Ayat 2 menjelaskan bahwa "Data Pribadi yang disimpan dalam Sistem Elektronik harus dalam bentuk data terenkripsi." (Indonesia, Peraturan Menkominfo, 2016).

Pada bulan Maret 2020 terjadi insiden pelanggaran data (*data breach*) sebanyak 91 juta data pengguna dari salah satu aplikasi *marketplace* Indonesia, yaitu Tokopedia yang disebar dalam forum yang berisikan transaksi ilegal tentang penjualan data-data hasil peretasan (CNN Indonesia, 2020). Sebagai akibat dari insiden tersebut beberapa masyarakat Indonesia, salah satunya penulis melakukan pengecekkan berdasarkan alamat *e-mail* yang digunakan pada akun *marketplace* tersebut melalui *website* haveibeenpwned.com. *Website* haveibeenpwned.com ini merupakan perangkat lunak yang dibangun oleh seorang Direktur Regional *Microsof*t, yaitu Troy Hunt, yang digunakan untuk mencari tahu apakah data pengguna

telah terekspos dan menjadi korban dari *data breach* berdasarkan alamat *e-mail* (Asih, 2020). Pada hasil dari pengecekkan alamat *e-mail* yang digunakan oleh penulis, diberitahu bahwa alamat *e-mail* tersebut telah terekspos datanya dan menjadi korban dari *data breach*. Alamat *e-mail* dan kata sandi penulis terdapat dalam suatu *file* teks berformat *.txt yang di dalamnya terdapat 4.788.657 akun pengguna Gmail. Tereksposnya informasi penting tersebut dapat disalahgunakan oleh oknum yang tidak berkuasa dalam mengakses semua aplikasi yang tersambung dengan alamat *e-mail*, terutama aplikasi penyimpanan *file* digital *online*. Hal ini dapat mengakibatkan *file* yang terdapat pada aplikasi penyimpanan *file* digital *online* dapat dibaca dan disalahgunakan.

Untuk mengantisipasi permasalahan keamanan pada kerahasiaan *file* digital di dalam perangkat penyimpanan *file* digital *offline* maupun *online*, maka diperlukan proteksi dengan teknik kompresi dan teknik kriptografi. Teknik kompresi dalam penelitian ini diterapkan sebelum *file* dienkripsi agar mengurangi redundansi pada isi *file*, sehingga kriptanalis tidak dapat memperkirakan kemungkinan makna dari *ciphertext*. Contoh kata "dan" pada Bahasa Indonesia redundansi, jika dalam *ciphertext* sering terdapat teks yang disandikan berupa "ftY" (3 huruf) maka berpeluang besar bahwa kata itu adalah kata "dan", semakin banyak redundansi, maka semakin gampang mengerjakan kriptanalisis (Munir, 2019). Teknik kriptografi dalam penelitian ini digunakan untuk melakukan perubahan terhadap informasi yang ada di dalam *file*, sehingga tidak berhasil dimengerti maknanya oleh oknum yang tidak berkuasa atas *file* tersebut (Rahardjo, 2017).

Algoritma kompresi yang digunakan pada penelitian ini adalah algoritma Lempel-Ziv-Welch (LZW). Pemilihan menggunakan algoritma kompresi LZW didasari dengan dua penelitian yang telah lalu dilaksanakan oleh peneliti sebelumnya. Penelitian pertama, yaitu membandingkan algoritma kompresi Huffman, LZW, dan kombinasi kedua algoritma tersebut dengan *file* yang digunakan ialah dokumen teks artikel teknologi Bahasa

Indonesia. Hasil penelitian berdasarkan nilai rasio kompresi terbaik yang dihasilkan oleh algoritma LZW sebesar 62% pada *file* *.doc. Hasil ini menunjukkan algoritma kompresi LZW lebih baik dalam melakukan pengecilan ukuran data dibandingkan dengan algoritma kompresi Huffman dan kombinasi dari kedua algoritma tersebut (Prasetyo, 2019). Penelitian kedua(Suharso, Zaelani dan Juardi, 2020), yaitu melakukan pengkajian kinerja algoritma LZW dengan memadankan hasil rasio kompresi seputar *file* teks, potret dan suara dengan aplikasi yang menggunakan algoritma Shannon Fano. Hasilnya menunjukkan bahwa kinerja algortima LZW lebih baik daripada Shannon Fano, terlebih pada *file* teks *.txt dengan menghasilkan rasio kompresi sebesar 65.95% dan 40.46% rasio kompresi yang dihasilkan oleh algoritma Shannon Fano (Suharso dkk., 2020).

Algoritma kriptografi yang dipakai dalam penelitian ini adalah algoritma *Twofish*, karena didasari dengan dua penelitian yang telah dilangsungkan oleh peneliti sebelumnya. Penelitian pertama, yaitu melakukan eksperimen untuk membandingkan kinerja dari kedua algoritma, yang hasilnya menyatakan bahwa algoritma *Twofish* lebih baik performanya karena durasi yang dibutuhkan untuk proses enkripsi dan dekripsi empat kali lebih unggul dibandingkan dengan algoritma 3DES (Sudirko dan Delimayanti, 2015). Penelitian kedua, yaitu penelitian ini menjelaskan bahwa hasil dari analisis pengujian terhadap kinerja algoritma *Twofish* bekerja lebih unggul daripada algoritma Serpent. Estimasi rata-rata waktu dari proses enkripsi *Twofish* bekerja 42% lebih cepat pada penggunaan semua ukuran kunci 128, 192, dan 256-bit daripada algoritma Serpent, serta pada rata-rata waktu proses dekripsi algoritma *Twofish* 48% lebih cepat daripada algoritma Serpent (Puji Sutan dkk., 2020).

Berdasarkan latar belakang yang telah dipaparkan di atas, maka penulis mengadakan penelitian dengan judul “Penerapan Algoritma Kompresi LZW dan Algoritma Kriptografi *Twofish* dalam Pengamanan *File* Digital”. Pada penelitian ini diharapkan dapat mengamankan kerahasiaan *file* digital yang

disimpan ke dalam perangkat atau aplikasi penyimpanan *file* digital agar tidak dapat dilihat dan dipahami oleh oknum yang tidak berkuasa.

## I.2 Rumusan Masalah

Berdasarkan dari penjelasan latar belakang penelitan di atas, maka dapat dirumuskan masalah yang diteliti, yaitu sebagai berikut:

a. Bagaimana mengamankan kerahasiaan dari *file* digital?
b. Bagaimana hasil dan kinerja dari algoritma kompresi LZW dan kriptografi *Twofish* terhadap *file* digital yang diamankan?

## I.3 Ruang Lingkup Penelitian

Adapun ruang lingkup penelitian yang akan ditelaah pada penelitian ini dengan sebagai berikut:

a. Algoritma yang digunakan untuk penelitian ini adalah algoritma kompresi LZW dan algoritma kriptografi *Twofish*.
b. Mode operasi *block cipher* yang digunakan adalah *Cipher Block Chaining* (CBC).
c. *File* digital yang akan digunakan dalam uji coba penelitian adalah *file* digital dalam bentuk *file* teks, *Word*, Excel, dan PDF.
d. Ukuran *file* digital tidak lebih dari 50 MB.
e. Kunci yang digunakan pada algoritma kriptografi *Twofish* maksimal adalah 256-bit atau 32 karakter.
f. Aplikasi yang dibangun berbasis *Windows* 64-bit.

## I.4 Tujuan Penelitian

Adapun tujuan yang akan dicapai dari pelaksanaan penelitian ini adalah sebagai berikut:

1. Mengamankan kerahasiaan *file* digital dari oknum yang tidak berwenang dengan menggunakan algoritma kompresi LZW dan algoritma kriptografi *Twofish*.
2. Mengetahui hasil dan kinerja dari algoritma kompresi LZW dan kriptografi *Twofish* terhadap *file* digital yang diamankan.

## I.5 Manfaat Penelitian

Adapun manfaat yang akan diperoleh dari pelaksanaan penelitian ini adalah sebagai berikut:

a. Menambah pengetahuan dan pemahaman mengenai pengamanan *file* digital dengan menerapkan algoritma kompresi LZW dan algoritma kriptografi *Twofish*.
b. Penelitian ini dapat diwujudkan sebagai suatu referensi atau rujukan dalam pengembangan penelitian berikutnya mengenai penerapan algoritma kompresi LZW dan algoritma kriptografi *Twofish* dalam mengamankan *file* digital.
c. Memberi alternatif solusi untuk menjaga keamanan terhadap kerahasiaan *file* digital yang disimpan pada perangkat atau aplikasi penyimpanan *file* digital.

## I.6 Luaran yang diharapkan

Luaran yang diharapkan dari penelitian ini adalah menyediakan aplikasi *desktop Windows* 64-bit dengan menerapkan algoritma kompresi LZW dan algoritma kriptografi *Twofish* yang dapat memberikan alternatif solusi pada permasalahan keamanan terhadap kerahasiaan *file* digital yang disimpan dalam perangkat atau aplikasi penyimpanan *file* digital, serta mengetahui bagaimana hasil dan kinerja dari algoritma kompresi LZW dan kriptografi *Twofish* terhadap *file* digital yang diamankan.

## I.7 Sistematika Penulisan

Adapun sistematika penulisan yang digunakan dalam penelitian ini yang bertujuan untuk memberikan informasi mengenai isi dari penulisan penelitian ini, yaitu sebagai berikut:

**BAB I PENDAHULUAN**

Pada bab ini menjelaskan latar belakang dari penelitian yang dilakukan oleh penulis, rumusan masalah yang terbentuk dari penjelasan latar belakang,

ruang lingkup penelitian, tujuan dan manfaat dari penelitian, luaran yang diharapkan dari penelitian, serta sistematika penulisan pada penelitian ini.

**BAB II LANDASAN TEORI**

Pada bab ini memaparkan teori, konsep, penelitian relevan yang menjadi landasan untuk menjunjung penelitian ini yang bertautan dengan topik dari penelitian.

**BAB III METODOLOGI PENELITIAN**

Pada bab ini menjelaskan metode penelitian yang digunakan oleh penulis secara bertahap-tahap dari awal hingga akhir pelaksanaan penelitian secara keseluruhan untuk mencapai tujuan penelitian.

**BAB IV HASIL DAN PEMBAHASAN**

Pada bab ini menjelaskan hasil dan pembahasan dari tahapan penelitian yang telah dijabarkan pada metode penelitian.

**BAB V PENUTUP**

Pada bab ini menjelaskan kesimpulan dan saran yang dihasilkan dari penelitian yang telah dilakukan.

**DAFTAR PUSTAKA**

**RIWAYAT HIDUP**

**LAMPIRAN**